Del riesgo cuántico al deber jurídico de anticipación: retos de la criptografía postcuántica para la ciberseguridad pública

por

Prof. Dr. Carlos M. Galán Pascual **Doctor en Informática** **Abogado** **Profesor del Departamento de Derecho Público del Estado – Área de Derecho Administrativo** **Universidad Carlos III de Madrid** **Agencia de Tecnología Legal**	**Prof. Dr. Carlos Galán Cordero** **Doctor en Derecho – Máster en Relaciones Internacionales y Comunicación** **Director del Máster en Análisis de Inteligencia y Ciberinteligencia** **Departamento de Seguridad y Defensa** **Universidad Nebrija** **Agencia de Tecnología Legal**

Resumen

La transición a la criptografía postcuántica suele presentarse como una cuestión eminentemente técnica: la sustitución progresiva de mecanismos criptográficos vulnerables frente a un futuro computador cuántico criptográficamente relevante por otros diseñados para resistir adversarios cuánticos. Sin embargo, esa transición plantea problemas jurídicos de primer orden. El presente trabajo analiza, desde la perspectiva del Esquema Nacional de Seguridad (ENS), los efectos del riesgo cuántico y de la propia migración postcuántica sobre las cinco dimensiones que el Real Decreto 311/2022 utiliza para categorizar los sistemas de información: disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad. El artículo distingue dos planos: el riesgo cuántico de origen, derivado de la futura pérdida de seguridad de determinados mecanismos de clave pública, y el riesgo de transición, asociado a la implantación de nuevas soluciones, a la interoperabilidad, a la conservación de evidencias, a la continuidad de los servicios y a la cadena de suministro. Se sostiene que el riesgo cuántico está pasando de ser una amenaza hipotética a constituir un riesgo jurídicamente previsible. La Recomendación (UE) 2024/1101 y la hoja de ruta del Grupo de Cooperación NIS de 2025 no crean, por sí solas, obligaciones directamente exigibles a cada entidad española, pero contribuyen a concretar el estado de conocimiento, la previsibilidad del riesgo y las expectativas de diligencia en ámbitos sometidos a obligaciones dinámicas de gestión del riesgo. Sobre esta base se proponen líneas generales de mitigación compatibles con el enfoque del ENS, sin formular todavía reformas normativas concretas.

Palabras clave: computación cuántica; criptografía postcuántica; Esquema Nacional de Seguridad; riesgo jurídico; confidencialidad; integridad; autenticidad; trazabilidad; disponibilidad; criptoagilidad.

Abstract

The transition to post-quantum cryptography is often framed as a predominantly technical matter: the progressive replacement of cryptographic mechanisms vulnerable to a future cryptographically relevant quantum computer with mechanisms designed to withstand quantum adversaries. Yet the transition already raises significant legal issues. This article examines, from the perspective of Spain's National

Security Framework (Esquema Nacional de Seguridad, ENS), the effects of quantum risk and of the post-quantum migration itself on the five security dimensions used by Royal Decree 311/2022 to categorize information systems: availability, confidentiality, integrity, authenticity and traceability. The analysis distinguishes between origin quantum risk, arising from the future loss of security of certain public-key mechanisms, and transition risk, associated with deployment, interoperability, long-term evidence preservation, service continuity and supply-chain dependencies. It argues that quantum risk is moving from a merely hypothetical threat towards a legally foreseeable risk. Commission Recommendation (EU) 2024/1101 and the 2025 NIS Cooperation Group roadmap do not, by themselves, impose directly enforceable deadlines on each Spanish entity, but they contribute to defining the state of knowledge, foreseeability and reasonable diligence in regulatory frameworks based on dynamic risk management. The article therefore outlines general mitigation strategies consistent with the logic of the ENS, while deliberately avoiding concrete proposals for regulatory amendment at this stage.

Keywords: quantum computing; post-quantum cryptography; National Security Framework; legal risk; confidentiality; integrity; authenticity; traceability; availability; crypto-agility.

1. Introducción: de una amenaza criptográfica futura a un problema jurídico presente

La computación cuántica no constituye todavía, en el sentido que interesa a este trabajo, una capacidad operativa capaz de quebrar de manera generalizada los principales sistemas criptográficos de clave pública desplegados en las administraciones y en las empresas. Esta constatación, sin embargo, no permite calificar el riesgo como jurídicamente irrelevante. La seguridad jurídica de los sistemas digitales se construye sobre horizontes temporales que no coinciden con el instante en que una vulnerabilidad se materializa. La información puede necesitar permanecer confidencial durante años; una firma electrónica puede tener que ser verificable mucho después de su creación; un registro puede convertirse en evidencia en un procedimiento administrativo o judicial futuro; y un sistema crítico puede tener ciclos de adquisición, certificación y sustitución de una década o más. En estos supuestos, la pregunta jurídicamente pertinente no es solo cuándo existirá un computador cuántico criptográficamente relevante, sino si la organización puede razonablemente completar su transición antes de que el riesgo alcance los activos que hoy está obligada a proteger (Mosca, 2018; Joseph et al., 2022).

La razón técnica que desencadena esta cuestión es bien conocida. El algoritmo de Shor mostró que un computador cuántico suficientemente potente permitiría resolver eficientemente los problemas de factorización y logaritmo discreto sobre los que descansan buena parte de los sistemas asimétricos actuales (Shor, 1997). La consecuencia no es que toda la criptografía convencional quede súbitamente inutilizada: el impacto es particularmente severo en los mecanismos de clave pública, mientras que la criptografía simétrica y las funciones resumen presentan un cuadro diferente y, en términos generales, pueden conservar niveles adecuados de seguridad mediante parámetros apropiados frente a aceleraciones cuánticas como la asociada al algoritmo de Grover (Grover, 1996; Bernstein & Lange, 2017). Para un análisis jurídico, basta con retener esta asimetría: una parte de la infraestructura de confianza que sostiene el cifrado, el establecimiento de claves, la autenticación, la firma y la validación a largo plazo deberá migrar antes de que la amenaza sea explotable a gran escala.

La respuesta tecnológica dominante es la criptografía postcuántica o PQC (Post-Quantum Cryptography), es decir, algoritmos ejecutables en sistemas clásicos cuyo diseño pretende mantener la seguridad aun cuando el adversario disponga de capacidades cuánticas relevantes. Aunque el proceso de normalización ha avanzado sustancialmente, como lo demuestra que, en agosto de 2024,

el National Institute of Standards and Technology de Estados Unidos publicara FIPS 203, FIPS 204 y FIPS 205, correspondientes, respectivamente, a ML-KEM, ML-DSA y SLH-DSA (NIST, 2024a, 2024b, 2024c), lo que constituye un hecho importante para comprender la madurez del proceso internacional, no significa que un estándar NIST se convierta automáticamente en mecanismo autorizado para cualquier sistema sujeto al ENS: el propio anexo II del Real Decreto 311/2022 remite, según la medida de que se trate, a algoritmos y parámetros autorizados por el Centro Criptológico Nacional (CCN) o, en su caso, por el esquema nacional o europeo aplicable (Real Decreto 311/2022, anexo II, medidas [mp.si.2] y [mp.info.3]).

En la Unión Europea, el punto de inflexión jurídico-político se produjo con la Recomendación (UE) 2024/1101 de la Comisión, de 11 de abril de 2024, sobre una hoja de ruta coordinada de aplicación para la transición a la criptografía postcuántica. La Comisión instó a los Estados miembros a desarrollar una estrategia coordinada y sincronizada de transición, prestando especial atención a las infraestructuras críticas y a los sistemas de las administraciones públicas (Comisión Europea, 2024). En junio de 2025, el Grupo de Cooperación NIS publicó una primera hoja de ruta común con hitos y fases de implementación, que parte de la necesidad de actuar antes de que la amenaza sea plenamente operativa, e incluye el inventario de activos criptográficos, el análisis de dependencias y la criptoagilidad entre los primeros pasos, y sitúa la transición de los casos de uso de alto riesgo en un horizonte que no debe superar el final de 2030, reservando horizontes posteriores para categorías de riesgo inferiores (NIS Cooperation Group, 2025). En 2026, ENISA ha continuado el trabajo sobre la hibridación de mecanismos clásicos y post-cuánticos y sobre su encaje en los marcos europeos de certificación (ENISA, 2026).

Conviene subrayar desde el principio la naturaleza jurídica de estos instrumentos. La Recomendación (UE) 2024/1101 no tiene la fuerza vinculante de un reglamento o una directiva, y la hoja de ruta del Grupo de Cooperación NIS opera como instrumento de coordinación y orientación. No sería correcto convertir sus fechas, sin una base normativa adicional, en plazos directamente exigibles a cualquier organización española. Su relevancia jurídica es distinta: contribuyen a consolidar la cognoscibilidad y previsibilidad del riesgo, proporcionan un parámetro técnico-institucional para interpretar obligaciones de seguridad formuladas en términos dinámicos y reducen el espacio para sostener, en el futuro, que la amenaza era desconocida o razonablemente imprevisible. Esta función interpretativa es especialmente significativa en marcos que exigen atender al estado de la técnica, a la evolución de los riesgos o a la actualización continua de las medidas de seguridad.

El ENS -aplicable, como es sabido y así dispone su art. 2, a las entidades del sector público y a las entidades privadas prestadoras de servicios competenciales a las anteriores-, ofrece un terreno particularmente adecuado para este análisis. El Real Decreto 311/2022, de 3 de mayo, no se limita a exigir controles técnicos aislados, sino que configura la seguridad como un proceso integral, basado en riesgos y sujeto a mejora continua. Su artículo 28.2 permite ampliar las medidas mínimas atendiendo, entre otros factores, al estado de la tecnología y a los riesgos a los que estén expuestos los sistemas, mientras que el artículo 39 dispone que el ENS debe mantenerse permanentemente actualizado en paralelo a la evolución tecnológica, a los nuevos estándares y a los riesgos. Además, el artículo 40.2 y el anexo I articulan la categorización de los sistemas en torno al impacto que un incidente podría producir sobre cinco dimensiones: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad (Real Decreto 311/2022, arts. 28.2, 39 y 40.2; anexo I).

El objetivo de este artículo es analizar de qué modo el riesgo cuántico y, de manera más específica, la transición hacia la PQC pueden afectar jurídicamente a esas cinco dimensiones. La tesis central es doble. Primero, la amenaza cuántica no debe analizarse únicamente como una vulnerabilidad criptográfica futura, sino como un riesgo jurídico temporal: puede generar obligaciones presentes cuando el periodo durante el cual un activo debe permanecer protegido sea superior al tiempo razonablemente disponible para migrar. Segundo, la PQC debe contemplarse a la vez como medida de mitigación y como proceso generador de riesgos transitorios. Migrar de forma tardía puede ser negligente, pero migrar de forma precipitada, sin pruebas, interoperabilidad, continuidad ni mecanismos de recuperación, también puede comprometer las propiedades de seguridad que se pretendía proteger (Joseph et al., 2022; Näther et al., 2024; Pérez Bes, 2025).

2. El riesgo cuántico como riesgo jurídicamente previsible

2.1. Previsibilidad, horizonte temporal y deber de diligencia

El Derecho de la ciberseguridad se caracteriza crecientemente por obligaciones de conducta basadas en el riesgo y no por garantías absolutas de resultado. El hecho de que un incidente llegue a producirse no determina por sí mismo el reproche; la cuestión central es si las medidas adoptadas eran apropiadas, proporcionadas y razonables teniendo en cuenta el conocimiento disponible, la naturaleza de los activos, el impacto previsible y el estado de la técnica. Esta lógica es visible en el ENS y también en el Derecho de la Unión. El artículo 32.1 del Reglamento (UE) 2016/679 exige seleccionar medidas técnicas y organizativas apropiadas atendiendo, entre otros elementos, al estado de la técnica y al riesgo, e incluye expresamente la capacidad de garantizar de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento. Por su parte, el artículo 21 de la Directiva (UE) 2022/2555 (NIS2) exige medidas de gestión de riesgos de ciberseguridad adecuadas y proporcionadas, incluyendo políticas y procedimientos relativos al uso de criptografía y, cuando proceda, cifrado (Reglamento (UE) 2016/679, art. 32; Directiva (UE) 2022/2555, art. 21.2.h).

En este contexto, la previsibilidad del riesgo cuántico no exige conocer la fecha exacta del denominado *Q-Day*[1]. En gestión de riesgos, la incertidumbre temporal no equivale a inexistencia del riesgo. De hecho, la fórmula conocida como 'Mosca's theorem' o desigualdad de Mosca invita a comparar tres magnitudes: el tiempo durante el cual la información debe permanecer segura, el tiempo necesario para migrar el sistema y el tiempo estimado hasta que la tecnología cuántica pueda comprometer la criptografía utilizada. Si la suma de los dos primeros supera el tercero, la exposición relevante ya ha comenzado, aunque el atacante todavía no pueda descifrar los datos (Mosca, 2018). Desde el punto de vista jurídico, el valor de este razonamiento reside en desplazar la evaluación desde una fecha especulativa hacia variables que la organización sí puede y debe conocer: vida útil del activo, plazo de conservación, criticidad, dependencia criptográfica y duración de la transición.

La doctrina reciente ha comenzado a llamar la atención sobre esta transformación del problema técnico en uno de gobernanza y cumplimiento. Balarabe sostiene que los marcos jurídicos deberían incorporar comprobaciones de preparación cuántica y enfoques prospectivos, precisamente porque

[1] En este trabajo, *Q-Day* designa el momento hipotético en el que un computador cuántico criptográficamente relevante pueda comprometer de forma práctica los principales mecanismos de criptografía de clave pública actualmente desplegados, en particular los basados en RSA y en criptografía de curvas elípticas (ECC).

el impacto sobre la protección de datos, la propiedad y la seguridad no se materializará de forma uniforme ni instantánea (Balarabe, 2025). En una perspectiva más amplia, Truby y Baysal han situado el Q-Day dentro del debate sobre las obligaciones estatales y el orden jurídico internacional, mostrando que la disrupción criptográfica puede afectar estructuras de confianza que trascienden la mera seguridad informática (Truby & Baysal, 2026). Sin necesidad de asumir todas las consecuencias de esas propuestas, existe ya una base suficiente para afirmar que la gobernanza jurídica de la transición no puede diferirse hasta la existencia de un ataque cuántico efectivo.

2.2. La relevancia de la Recomendación (UE) 2024/1101 y de la hoja de ruta europea

Aunque la Recomendación (UE) 2024/1101 es un acto de *soft law*, su contenido tiene relevancia interpretativa. Al pedir estrategias nacionales coordinadas y una transición sincronizada, la Comisión identifica la amenaza, la eleva a prioridad de política pública y propone que los Estados miembros actúen anticipadamente (Comisión Europea, 2024). El posterior documento del Grupo de Cooperación NIS concreta esa orientación en una secuencia de inventario, análisis de riesgo, planificación, pilotos, criptoagilidad, contratación, adaptación de certificación y migración de casos de uso priorizados (NIS Cooperation Group, 2025). La existencia de este itinerario institucional altera el contexto en el que se valora la diligencia de una organización sometida a deberes generales de gestión del riesgo.

Esta afirmación exige una cautela: los instrumentos no vinculantes no pueden utilizarse para crear por vía interpretativa una infracción que el legislador no ha tipificado ni para imponer automáticamente un algoritmo, producto o fecha concreta a una entidad. Sí pueden, en cambio, integrar el entorno técnico-regulatorio que ayuda a concretar conceptos jurídicos indeterminados o estándares abiertos, como 'estado de la técnica', 'medidas apropiadas', 'riesgos previsibles' o 'mejora continua'. La diferencia es decisiva: la hoja de ruta europea no sustituye al ENS ni a las decisiones del CCN sobre criptología de empleo, pero sí puede contribuir a demostrar que el riesgo ha sido formalmente identificado por las autoridades competentes y que existe una trayectoria de transición razonablemente esperable.

Este efecto es particularmente claro en el ENS. El artículo 7 exige que el análisis y la gestión de riesgos sean parte esencial del proceso de seguridad y se mantengan permanentemente actualizados; el artículo 27 obliga a actualizar y mejorar de manera continua el proceso integral de seguridad; el artículo 28.2 admite medidas adicionales atendiendo al estado de la tecnología y a los riesgos; y el artículo 39 ordena la actualización permanente del propio esquema. En consecuencia, aunque hoy no exista una obligación general y autónoma de implantar de inmediato un determinado algoritmo post-cuántico en todo sistema ENS, sí existe una base normativa para exigir que el riesgo sea incorporado al ciclo de análisis y gestión cuando sea materialmente relevante para los activos y servicios de la organización.

En el ámbito español, esta orientación europea ha encontrado una concreción especialmente relevante en la Guía CCN-TEC 009 BP/37, *Recomendaciones para una transición postcuántica segura*, publicada por el Centro Criptológico Nacional en julio de 2026. El documento parte de que la amenaza cuántica puede comprometer los mecanismos criptográficos sobre los que descansan actualmente la confidencialidad, la integridad, la autenticación y el no repudio, y advierte de que la respuesta no puede diferirse hasta la aparición efectiva de un ordenador cuántico criptográficamente relevante. En coherencia con la hoja de ruta coordinada de la Unión Europea, la Guía propone abordar la transición como un proceso anticipado y gobernado, que comprende el descubrimiento de los activos y dependencias criptográficas, la adquisición y despliegue de nuevas

soluciones, la criptoagilidad[2], el eventual empleo de mecanismos híbridos[3] y la planificación temporal de la migración, estableciendo como referencia su culminación antes de finales de 2030 para los sistemas de riesgo alto y antes de finales de 2035 para los de riesgo medio (Centro Criptológico Nacional, 2026). Desde una perspectiva jurídica, la relevancia de la BP/37 excede, por tanto, su contenido estrictamente criptográfico: aun sin constituir por sí misma una modificación del marco normativo del Esquema Nacional de Seguridad, constituye una referencia técnica institucional particularmente cualificada para interpretar la evolución del riesgo y del estado de la tecnología que las organizaciones deben considerar al adoptar y revisar sus medidas de seguridad, reforzando así la idea de que la preparación frente al riesgo cuántico forma ya parte de una gestión prospectiva y diligente de la ciberseguridad.

3. Las cinco dimensiones del ENS como categorías jurídicas de análisis

El anexo I del Real Decreto 311/2022 identifica expresamente las dimensiones de confidencialidad [C], integridad [I], trazabilidad [T], autenticidad [A] y disponibilidad [D]. Su función no es meramente descriptiva: determinan el nivel de seguridad requerido para las informaciones y servicios, influyen en la categoría del sistema y condicionan la selección de medidas y refuerzos del anexo II. El artículo 40.2 remite a la valoración del impacto que tendría un incidente con perjuicio para cualquiera de estas dimensiones (Real Decreto 311/2022, art. 40.2 y anexo I).

El propio anexo I refuerza la naturaleza jurídica de estas dimensiones al incluir, entre los criterios para graduar el perjuicio, el incumplimiento de leyes o regulaciones. Un impacto bajo puede asociarse a un incumplimiento formal subsanable; un impacto medio, a un incumplimiento material o formal no subsanable; y un impacto alto, a un incumplimiento grave de una ley o regulación (Real Decreto 311/2022, anexo I, apartado 3). Las dimensiones funcionan así como interfaces entre el riesgo técnico y sus consecuencias jurídicas. La pérdida de confidencialidad puede implicar una violación de datos personales, de secretos empresariales o de deberes de reserva; la pérdida de autenticidad puede erosionar la imputación de un acto electrónico; la pérdida de trazabilidad puede afectar la prueba y la rendición de cuentas; la pérdida de disponibilidad puede impedir la prestación de un servicio público; y la pérdida de integridad puede comprometer la validez o fiabilidad de información utilizada para adoptar decisiones.

El glosario del ENS define la confidencialidad como la propiedad de que la información no se ponga a disposición ni se revele a sujetos no autorizados; la integridad como la propiedad de que el activo de información no haya sido alterado de manera no autorizada; la autenticidad como la garantía de que una entidad es quien dice ser o de la fuente de los datos; la disponibilidad como la posibilidad de que entidades o procesos autorizados accedan a los activos cuando lo requieran; y la trazabilidad como la posibilidad de atribuir de forma indiscutible las actuaciones de una persona o proceso a esa entidad (Real Decreto 311/2022, anexo IV). Estas definiciones permiten construir un marco sistemático para estudiar la transición postcuántica sin reducir el problema a la ruptura del cifrado.

[2] La denominada *criptoagilidad* es la capacidad de un sistema de seguridad para cambiar de códigos, llaves o algoritmos de cifrado de forma rápida y sencilla.

[3] En este trabajo, por *mecanismos híbridos* se entienden las construcciones que combinan uno o más componentes criptográficos tradicionales con uno o más componentes postcuánticos, de modo que al menos uno de los componentes sea postcuántico y al menos uno tradicional.

Dimensión	Riesgo cuántico de origen	Riesgo de transición PQC	Proyección jurídica principal
Disponibilidad	Compromiso indirecto de autenticación/infraestructura y potencial interrupción de servicios.	Fallos de interoperabilidad, capacidad, rendimiento, actualización o reversión.	Continuidad, resiliencia y prestación efectiva de servicios.
Confidencialidad	Descifrado futuro de comunicaciones o datos capturados hoy; exposición de claves.	Configuraciones híbridas defectuosas, inventarios incompletos o migraciones parciales.	Deberes de secreto, protección de datos, información sensible y gestión prospectiva del riesgo.
Integridad	Falsificación de firmas o controles basados en criptografía vulnerable.	Errores de implementación, downgrade, fallos en cadenas de actualización o firma.	Fiabilidad de documentos, software, registros y decisiones basadas en datos.
Autenticidad	Suplantación mediante compromiso de certificados, firmas o mecanismos de clave pública.	Ruptura de cadenas de confianza, incompatibilidades PKI y validación heterogénea.	Imputación de actos electrónicos, identidad y servicios de confianza.
Trazabilidad	Debilitamiento posterior del valor probatorio de logs, firmas o sellos sustentados en mecanismos vulnerables.	Pérdida de verificabilidad histórica durante la migración o conservación insuficiente de evidencias.	Auditoría, rendición de cuentas, cadena de custodia y prueba electrónica.

Tabla 1. Doble vector de riesgo cuántico sobre las cinco dimensiones de seguridad del ENS (Fuente: elaboración propia a partir del Real Decreto 311/2022, la Recomendación (UE) 2024/1101 y la hoja de ruta del Grupo de Cooperación NIS (Comisión Europea, 2024; NIS Cooperation Group, 2025)).

4. Disponibilidad: la transición como riesgo de continuidad y resiliencia

La disponibilidad es, a primera vista, la dimensión menos directamente conectada con la ruptura cuántica de la criptografía. El algoritmo de Shor no provoca por sí mismo una caída de servidores ni una denegación de servicio. Sin embargo, una lectura jurídicamente adecuada debe atender tanto a los efectos indirectos de la pérdida de autenticación e integridad como, sobre todo, a los riesgos operativos de la transición. El ENS define disponibilidad como la posibilidad de que sujetos o procesos autorizados accedan a los activos cuando los requieren, y dedica el artículo 26 a la continuidad de la actividad, exigiendo copias de seguridad y mecanismos que permitan continuar las operaciones cuando se pierdan los medios habituales (Real Decreto 311/2022, art. 26 y anexo IV).

La migración postcuántica puede tensionar esta dimensión por varias vías. Los nuevos mecanismos no son intercambiables de forma transparente con cualquier protocolo o infraestructura heredada. Según el algoritmo y el caso de uso, las claves, firmas o mensajes pueden tener tamaños superiores; pueden existir dispositivos embebidos sin capacidad de actualización; las bibliotecas criptográficas pueden comportarse de forma distinta; y las cadenas de certificados, VPN, sistemas de autenticación, HSM o servicios de firma pueden requerir cambios coordinados. La literatura de migración destaca precisamente la complejidad, el elevado esfuerzo de realización, la falta de experiencia y la necesidad de pruebas como obstáculos recurrentes (Joseph et al., 2022; Näther et al., 2024).

Desde el punto de vista jurídico, estas dificultades transforman una actualización criptográfica en un problema de continuidad. Una organización que sustituya un mecanismo crítico sin pruebas suficientes podría provocar indisponibilidad, incompatibilidades entre administraciones o imposibilidad de validar credenciales. En sentido inverso, mantener indefinidamente una infraestructura vulnerable por miedo a interrumpir el servicio puede dejar el sistema expuesto a riesgos previsibles. La diligencia exige equilibrar ambos vectores mediante una transición gradual, reversible cuando resulte necesario, probada en entornos representativos y priorizada conforme a criticidad.

El ENS ya contiene principios suficientemente amplios para encuadrar esta obligación. La seguridad se concibe como un proceso integral durante todo el ciclo de vida; las especificaciones de seguridad deben incluirse en el ciclo de vida de los servicios y sistemas; y las medidas pueden ampliarse según el estado de la tecnología y el riesgo (Real Decreto 311/2022, arts. 5, 28.2 y 36). Esto significa que la disponibilidad no debe evaluarse únicamente durante el estado final post-cuántico, sino también durante el camino de migración. En sistemas de categoría alta o que soporten servicios esenciales, una estrategia de transición sin plan de continuidad puede ser jurídicamente tan problemática como la ausencia de transición.

Existe además una dimensión contractual y de cadena de suministro. Muchas entidades no controlan directamente las bibliotecas, módulos criptográficos, equipos de red, servicios de nube o componentes de identidad que utilizan. La posibilidad de migrar depende de calendarios de proveedores, licencias, actualizaciones de firmware, certificaciones y compatibilidad entre productos. Una contratación que no contemple actualización criptográfica, portabilidad o sustitución puede generar bloqueo tecnológico y convertir un riesgo futuro en indisponibilidad estructural. Por ello, la disponibilidad postcuántica exige incorporar la migrabilidad y la capacidad de actualización en la gobernanza de adquisiciones, aun cuando todavía no se imponga una solución criptográfica concreta.

5. Confidencialidad: del «harvest now, decrypt later» al deber actual de protección

La confidencialidad es la dimensión en la que el riesgo cuántico resulta más intuitivo y, probablemente, la que mejor demuestra por qué una amenaza futura puede producir consecuencias jurídicas presentes. La posibilidad de almacenar hoy comunicaciones cifradas y descifrarlas en el futuro cuando exista capacidad cuántica suficiente se conoce como *harvest now, decrypt later* (HNDL). El atacante no necesita romper hoy el cifrado: le basta con capturar datos cuyo valor o sensibilidad persista hasta el momento en que la protección criptográfica pueda ser vencida. La hoja de ruta europea de 2025 identifica expresamente este problema y lo relaciona con datos que requieren largos periodos de confidencialidad (NIS Cooperation Group, 2025).

La consecuencia jurídica es importante: el deber de confidencialidad no se satisface necesariamente porque el dato resulte indescifrable el día en que se transmite. Si la organización conoce que determinada información debe mantenerse reservada durante diez, veinte o treinta años y utiliza un mecanismo cuyo horizonte razonable de seguridad puede ser inferior, el análisis de riesgo debe incorporar esa dimensión temporal. De lo contrario, se confundiría confidencialidad instantánea con confidencialidad durante todo el ciclo de vida exigible.

El ENS ofrece apoyo normativo a esta interpretación. La medida [mp.si.2] exige mecanismos criptográficos que garanticen confidencialidad e integridad de la información en los supuestos en los que resulta aplicable y dispone el uso de algoritmos y parámetros autorizados por el CCN. La Guía CCN-STIC 807 desarrolla los mecanismos criptográficos autorizados para el ENS y relaciona su fortaleza con los niveles de seguridad requeridos (CCN, 2022). A su vez, el artículo 28.2 permite incorporar medidas adicionales en función del estado de la tecnología, de la naturaleza de la información y de los riesgos. La combinación de estas previsiones sugiere que la conformidad no puede reducirse a una fotografía estática de algoritmos: requiere gestionar su vigencia durante el periodo en el que la información siga necesitando protección.

Cuando los sistemas ENS tratan datos personales, esta exigencia se refuerza. El artículo 3 del Real Decreto 311/2022 preserva la aplicación del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018, precepto que se concreta en la Disposición adicional primera de esta última norma, que exige que los responsables enumerados en su artículo 77.1[4] "*deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado*", añadiendo "*En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad*".

El artículo 32 RGPD exige medidas apropiadas atendiendo al estado de la técnica y al riesgo e incluye el cifrado de datos personales como una medida posible, no como un fin autónomo. El uso de cifrado deja de ser jurídicamente satisfactorio si, por las características del tratamiento y del horizonte de conservación, deja de constituir una medida adecuada frente a amenazas razonablemente previsibles. La consecuencia no es que toda entidad deba migrar inmediatamente todos sus tratamientos a PQC, sino que debe valorar cuáles tienen una vida de confidencialidad que justifique anticipar la transición.

La misma lógica puede proyectarse sobre secretos empresariales, información sensible del sector público, propiedad intelectual, expedientes administrativos, datos estratégicos o información clasificada, aunque cada categoría se rija por su propio régimen jurídico. En todos los casos, la pregunta central es la duración del deber de secreto. Cuanto mayor sea ese periodo, antes comienza

[4] Que comprenden: a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos. b) Los órganos jurisdiccionales. c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local. d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas. e) Las autoridades administrativas independientes. f) El Banco de España. g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público. h) Las fundaciones del sector público. i) Las Universidades Públicas. j) Los consorcios. k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

el riesgo HNDL. La evaluación no puede hacerse exclusivamente por tipo de algoritmo; debe integrar sensibilidad, plazo de conservación, probabilidad de captura, actores adversarios, capacidad de recolección masiva y consecuencias del descifrado tardío.

La transición postcuántica también puede generar riesgos propios de confidencialidad. Un despliegue híbrido mal configurado puede rebajar la seguridad al componente más débil; una migración parcial puede dejar activos olvidados; una nueva biblioteca puede introducir vulnerabilidades de implementación; la coexistencia de varias infraestructuras de claves puede multiplicar secretos y puntos de custodia; y una dependencia excesiva de soluciones inmaduras puede abrir canales de ataque no contemplados. Por ello, la PQC no debe considerarse un simple reemplazo de algoritmo, sino una modificación arquitectónica sometida a análisis de riesgos, pruebas, gestión de claves y auditoría (ENISA, 2022; Joseph et al., 2022).

6. Integridad: documentos, software y datos cuya fiabilidad debe sobrevivir al cambio criptográfico

La integridad, definida en el ENS como la propiedad de que el activo de información no haya sido alterado de forma no autorizada, se apoya frecuentemente en mecanismos criptográficos de firma, autenticación de mensajes, sellado o funciones resumen (Real Decreto 311/2022, anexo IV). El riesgo cuántico afecta de manera especial a los supuestos en los que la garantía de integridad descansa en firmas de clave pública vulnerables. Si un adversario pudiera obtener una clave privada a partir de información pública o producir firmas válidas fraudulentamente, podría crear objetos que aparentasen haber sido íntegros y legítimamente firmados.

En el ámbito administrativo, esta posibilidad no puede reducirse a la manipulación de un documento aislado. Los sistemas contemporáneos dependen de software firmado, actualizaciones de firmware, repositorios, certificados de código, paquetes y comunicaciones autenticadas. Una ruptura de la infraestructura de firma puede afectar la cadena de suministro y permitir que software modificado supere controles diseñados para garantizar su procedencia e integridad. Del mismo modo, bases de datos o evidencias conservadas durante largos periodos pueden perder parte de su capacidad de demostrar que no han sido alteradas si los mecanismos criptográficos que sostienen esa garantía dejan de ser confiables.

El anexo II del ENS vincula expresamente la medida de firma electrónica [mp.info.3] con las dimensiones de integridad y autenticidad. Para niveles medio y alto incorpora refuerzos relativos a certificados, algoritmos autorizados y verificación y validación durante el tiempo requerido por la actividad administrativa. Esta última exigencia es especialmente relevante: la seguridad de una firma no termina en el instante de creación, porque la Administración puede necesitar verificarla años después. La transición postcuántica obliga, por tanto, a pensar en estrategias de conservación de la capacidad probatoria, renovación de evidencias y validación a largo plazo.

Conviene evitar una conclusión excesiva: el descubrimiento futuro de una debilidad criptográfica no convierte automáticamente en inexistentes o jurídicamente nulos todos los documentos firmados en el pasado. El Reglamento eIDAS regula efectos jurídicos y requisitos de firmas, sellos y sellos de tiempo, y el valor de una evidencia dependerá del tipo de firma, del momento, de los datos de validación y del conjunto probatorio. El riesgo cuántico afecta a la confianza técnica y a la capacidad de demostrar integridad o autoría, no opera como una regla general de nulidad retroactiva. Precisamente por ello, la conservación de evidencias de validación, la renovación de sellos y otros mecanismos de preservación adquieren importancia preventiva

(Reglamento (UE) n.º 910/2014, arts. 25, 26 y 41; Real Decreto 311/2022, anexo II, [mp.info.3] y [mp.info.4]).

La migración a PQC introduce también riesgos de integridad en su fase de implantación. Nuevos esquemas de firma deben integrarse en protocolos, formatos documentales, dispositivos de creación, herramientas de validación y sistemas de archivo. Los mecanismos híbridos pueden reducir el riesgo de apostar de forma exclusiva por una primitiva nueva, pero multiplican la lógica de validación y crean la posibilidad de errores de composición o ataques de degradación si el sistema acepta indebidamente la parte clásica cuando debería exigir ambas. La orientación europea sobre hibridación muestra que esta cuestión ya forma parte de la agenda de certificación y normalización (ENISA, 2026). Jurídicamente, el criterio debería ser funcional: la migración solo es adecuada si mantiene o mejora la garantía de integridad exigible durante todo el periodo relevante.

7. Autenticidad: identidad digital, certificados y atribución jurídica de actos electrónicos

La autenticidad ocupa una posición central en la transición porque numerosos mecanismos de identificación y atribución dependen de criptografía asimétrica. El ENS la define como la propiedad por la que una entidad es quien dice ser o por la que se garantiza la fuente de procedencia de los datos (Real Decreto 311/2022, anexo IV). La amenaza cuántica afecta así a certificados, firmas, autenticación de servidores y clientes, infraestructuras de clave pública y otros mecanismos que permiten vincular una acción digital con una persona, organismo, dispositivo o servicio.

Si la clave privada asociada a una identidad pudiera derivarse o una firma pudiera falsificarse, la consecuencia no sería meramente técnica sino que se erosionaría la imputación jurídica del acto. En la administración digital, la atribución es presupuesto para consentimientos, solicitudes, resoluciones, intercambios interadministrativos, notificaciones, acceso a expedientes y múltiples operaciones automatizadas. En entornos empresariales, afecta contratación, órdenes de pago, actualizaciones, accesos privilegiados y comunicaciones con terceros. La autenticidad es, por tanto, una infraestructura jurídica de confianza.

El Reglamento eIDAS y su reforma mediante el Reglamento (UE) 2024/1183 proporcionan un marco europeo para identificación electrónica y servicios de confianza. Sus reglas sobre firmas electrónicas, sellos, sellos de tiempo y certificados se apoyan en requisitos jurídicos y técnicos que deben evolucionar conforme lo hagan los mecanismos criptográficos. El hecho de que eIDAS atribuya efectos jurídicos a determinadas categorías de firma no elimina el deber de mantener la seguridad de los medios de creación, validación y conservación. Tampoco permite asumir que una cadena de confianza técnicamente comprometida siga ofreciendo indefinidamente el mismo nivel de garantía. El problema jurídico es, por tanto, preservar la continuidad de la confianza durante la transición sin confundir evolución criptográfica con pérdida automática de validez de actos pasados.

La arquitectura del ENS refleja esta conexión. La medida [mp.info.3] exige, cuando resultan aplicables sus refuerzos, algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo, y dispone que la verificación y validación de la firma se garantice durante el tiempo requerido por la actividad administrativa. La medida es jurídicamente significativa porque incorpora el tiempo como elemento de seguridad de la autenticidad. La transición postcuántica debe garantizar no solo que las nuevas firmas sean seguras, sino que los ecosistemas de validación puedan distinguir de forma fiable entre evidencias históricas correctamente producidas y falsificaciones posteriores.

A ello se añade el riesgo de migración de las PKI. Cambiar algoritmos en una infraestructura de certificados requiere coordinar autoridades de certificación, dispositivos, políticas de certificados, protocolos, navegadores, servidores, aplicaciones y mecanismos de revocación. Una transición fragmentada puede producir periodos en los que unas partes acepten credenciales que otras no reconocen, con impacto simultáneo en autenticidad y disponibilidad. De ahí que la criptoagilidad —la capacidad organizativa y técnica de sustituir mecanismos criptográficos sin rediseñar por completo el sistema— deba entenderse también como una medida de gobernanza jurídica: reduce el riesgo de que la organización quede atrapada entre una solución vulnerable y otra aún no interoperable (NIS Cooperation Group, 2025; Joseph et al., 2022).

8. Trazabilidad: la fragilidad temporal de la evidencia electrónica

La trazabilidad es probablemente la dimensión en la que la aproximación jurídica aporta mayor valor diferencial. El ENS la define como la propiedad por la que las actuaciones de una entidad, persona o proceso, pueden ser trazadas de forma indiscutible hasta dicha entidad (Real Decreto 311/2022, anexo IV). El artículo 24 exige registrar actividades de los usuarios con la información necesaria para monitorizar, analizar, investigar y documentar actuaciones indebidas o no autorizadas, e insiste en la identificación única de cada usuario para determinar quién realizó una actividad.

La trazabilidad no depende exclusivamente de criptografía, pero su fuerza probatoria suele apoyarse en firmas, sellos, autenticadores, cadenas de custodia, controles de integridad y sellos temporales. Si alguno de esos elementos pierde seguridad con el tiempo, puede surgir una forma de 'fragilidad temporal de la prueba': el registro fue correctamente generado y era fiable cuando se produjo, pero años después resulta más difícil demostrar que no pudo ser falsificado o alterado. El problema es especialmente relevante en procedimientos sancionadores, responsabilidad patrimonial, litigios contractuales, investigaciones de incidentes, auditorías y cualquier contexto en el que la evidencia digital deba conservarse durante periodos prolongados.

El ENS contiene una previsión especialmente adecuada para este escenario. La medida [mp.info.4] se aplica a información susceptible de utilizarse como evidencia electrónica en el futuro y exige proteger los datos necesarios para verificar la fecha con la misma seguridad que la información fechada en términos de disponibilidad, integridad y confidencialidad; además, dispone la renovación regular de los sellos de tiempo mientras la información siga siendo requerida y exige sellos cualificados conforme a eIDAS cuando la medida resulte aplicable. La renovación temporal puede adquirir una nueva función en la era postcuántica: no solo prolongar la validez frente a caducidad o revocación, sino trasladar la evidencia a mecanismos criptográficos que mantengan garantías frente a amenazas futuras.

La dimensión probatoria exige una política de transición especialmente cuidadosa. Una migración mal documentada puede romper la continuidad de la cadena de custodia, perder metadatos de validación o impedir reconstruir qué algoritmo y qué certificado se utilizaron en una fecha determinada. La mera sustitución de una firma o sello sin conservar los elementos necesarios para justificar la transformación podría incluso debilitar la evidencia que pretendía reforzarse. Por ello, las organizaciones deben tratar la migración como un proceso auditable: inventariar evidencias con vida larga, conservar datos de validación, documentar transformaciones, aplicar sellos o mecanismos de preservación cuando proceda y garantizar que las herramientas futuras puedan verificar la historia criptográfica del objeto.

Esta cuestión conecta asimismo con la rendición de cuentas. Si la trazabilidad permite atribuir acciones y depurar responsabilidades, una organización que no preserve adecuadamente la verificabilidad de sus registros puede perder capacidad para demostrar cumplimiento, investigar incidentes o defender decisiones. El riesgo cuántico afecta así no solo a la seguridad primaria del sistema, sino también a la 'seguridad de la prueba' que permite acreditar después que el sistema se comportó conforme a Derecho. Es una dimensión que justifica incorporar horizontes de conservación y valor probatorio al inventario criptográfico, y no limitar este último a protocolos de comunicación o bases de datos cifradas.

9. Riesgos transversales de la transición postcuántica

9.1. El inventario criptográfico como presupuesto jurídico de la gestión del riesgo

No puede gestionarse un riesgo criptográfico que la organización desconoce. El primer obstáculo práctico es identificar dónde existe criptografía, qué función cumple, qué algoritmo y parámetros utiliza, quién es responsable del componente, qué datos protege, cuánto tiempo deben permanecer protegidos y qué dependencias condicionan su sustitución. La hoja de ruta europea sitúa el inventario de activos criptográficos y el mapa de dependencias entre los primeros pasos de la transición (NIS Cooperation Group, 2025). Desde la perspectiva jurídica, el inventario no es una finalidad técnica autónoma, sino la evidencia que permite demostrar que el análisis de riesgos se ha realizado sobre una base completa y que la priorización responde a criterios racionales.

Un inventario incompleto puede producir falsos positivos de cumplimiento: la organización migra la capa visible —por ejemplo, TLS en determinados servicios— mientras permanecen certificados embebidos, firmas de firmware, archivos históricos, sistemas industriales, VPN, claves en equipos no actualizables o integraciones con terceros. La gestión del riesgo cuántico exige por ello una visión de cadena de dependencias y no una lista de algoritmos. Esta exigencia encaja con el enfoque de ciclo de vida y cadena de suministro del ENS, así como con la obligación general de documentar la Declaración de Aplicabilidad y las decisiones de gestión del riesgo (Real Decreto 311/2022, arts. 28 y 36).

9.2. Criptoagilidad y neutralidad frente a soluciones concretas

La transición se produce en un entorno todavía dinámico. Aunque existen estándares post-cuánticos consolidados, el ecosistema de protocolos, productos, certificaciones y perfiles de interoperabilidad sigue evolucionando. La respuesta jurídica no debería consistir en cristalizar prematuramente una tecnología concreta, sino en exigir capacidad de adaptación. La criptoagilidad permite sustituir algoritmos, parámetros, certificados o proveedores sin reconstruir el sistema completo y reduce el coste de responder tanto a avances cuánticos como a vulnerabilidades que pudieran descubrirse en algoritmos post-cuánticos (NIS Cooperation Group, 2025).

Esta idea es coherente con el artículo 39 del ENS, que vincula su actualización a la evolución tecnológica y a la aparición o consolidación de estándares internacionales. También evita un error regulatorio frecuente: confundir cumplimiento con adhesión eterna a un catálogo estático. En criptografía, la seguridad es necesariamente temporal. Los mecanismos que hoy se consideran adecuados pueden dejar de serlo; por tanto, la capacidad de reemplazo forma parte de la propia seguridad del sistema.

9.3. Hibridación, estandarización y riesgo de composición

Durante la transición, los enfoques híbridos combinan mecanismos clásicos y post-cuánticos para reducir el riesgo de depender exclusivamente de una primitiva nueva o de mantener únicamente una primitiva vulnerable a futuro. La hoja de ruta europea contempla soluciones híbridas estandarizadas y probadas cuando sean factibles y adecuadas, y los trabajos de ENISA y del European Cybersecurity Certification Group han avanzado sobre la estandarización y evaluación de estos enfoques (NIS Cooperation Group, 2025; ENISA, 2026).

No obstante, 'híbrido' no significa automáticamente 'más seguro'. La seguridad depende de la forma en que se compongan los mecanismos, de qué condiciones se exijan para aceptar una firma o establecer una clave, de la resistencia a downgrade y de la implementación concreta. Una composición defectuosa puede permitir que un atacante fuerce el uso del componente más débil. Jurídicamente, esto aconseja evitar mandatos abstractos de hibridación y exigir, en cambio, soluciones estandarizadas, evaluadas y adecuadas al riesgo. El criterio debe ser la conservación efectiva de las dimensiones de seguridad, no la mera presencia simultánea de dos algoritmos.

9.4. Certificación, auditoría y prueba de diligencia

La transición postcuántica plantea asimismo un problema de aseguramiento. En entornos sometidos al ENS, no basta con desplegar controles; debe existir evidencia de su correcta implantación, revisión y auditoría. El anexo III exige que las autoevaluaciones y auditorías se sustenten en evidencias objetivas y que el análisis de riesgos sea revisado periódicamente. La disposición adicional segunda, en su redacción vigente tras el Real Decreto 1125/2024, dispone que las instrucciones técnicas de seguridad tengan en cuenta las normas armonizadas de la Unión Europea aplicables y que las guías CCN-STIC, especialmente las de la serie 800, se incorporen al conjunto documental utilizado en las auditorías (Real Decreto 311/2022, disposición adicional segunda y anexo III).

Esto crea un puente natural entre transición, certificación y responsabilidad. A medida que se consoliden estándares y criterios europeos o nacionales sobre PQC, las organizaciones deberán poder demostrar qué riesgos identificaron, por qué priorizaron determinados activos, qué pruebas realizaron y cómo gestionaron excepciones. La documentación será relevante no solo para una auditoría ENS, sino también para evaluar ex post la diligencia ante un incidente. En este ámbito, la trazabilidad del propio proceso de transición puede llegar a ser tan importante como la trazabilidad de las operaciones del sistema.

10. Aproximación general a las medidas de mitigación

En el estado actual, y sin anticipar reformas concretas del ENS ni imponer tecnologías todavía sujetas a evolución, es posible formular un conjunto de líneas generales de mitigación. Todas ellas responden a una idea común: la transición debe gobernarse como un programa de gestión del riesgo y no como una sustitución puntual de algoritmos. Esta perspectiva resulta compatible con el ENS, con la Recomendación (UE) 2024/1101 y con la hoja de ruta del Grupo de Cooperación NIS.

La tabla siguiente esboza estas medidas.

Área de aplicación	Descripción
Gobernanza y responsabilidad	La organización debería integrar el riesgo cuántico en su sistema ordinario de gobierno de la seguridad, asignando responsabilidades y

Área de aplicación	Descripción
explícita	mecanismos de decisión. No es imprescindible crear estructuras paralelas si las existentes pueden asumir la función, pero sí identificar quién mantiene el inventario criptográfico, quién determina la vida de protección de la información, quién aprueba prioridades y quién decide excepciones. Esta asignación encaja con la diferenciación de responsabilidades del ENS y evita que la transición quede dispersa entre equipos de infraestructura, compras, archivo, identidad y seguridad sin una dirección común (Real Decreto 311/2022, arts. 13 y 28).
Inventario criptográfico y mapa de dependencias	La primera medida material debe ser localizar y clasificar los usos de criptografía. El inventario debería incluir, al menos, finalidad, algoritmo y parámetros, producto o biblioteca, responsable, proveedor, información o servicio protegido, criticidad, horizonte de confidencialidad o verificabilidad, capacidad de actualización y dependencias. El objetivo no es producir una base de datos exhaustiva por formalismo, sino poder responder a tres preguntas: qué debe migrarse, en qué orden y qué puede impedir la migración (NIS Cooperation Group, 2025).
Priorización basada en tiempo de protección y criticidad	No todos los activos requieren la misma urgencia. La prioridad debería combinar el impacto ENS de las cinco dimensiones con el horizonte temporal de protección. Los datos cuya confidencialidad deba durar muchos años, las infraestructuras de firma y autenticación con larga vida, los sistemas no actualizables y los servicios de alta criticidad deberían situarse en niveles superiores de atención. Esta priorización permite evitar tanto la inacción como una migración masiva e indiscriminada que incremente el riesgo operativo.
Criptoagilidad y diseño para el cambio	Los nuevos desarrollos y adquisiciones deberían reducir el acoplamiento rígido entre aplicaciones y algoritmos concretos, facilitar el reemplazo de primitivas, permitir cambios de parámetros y soportar ciclos de actualización seguros. La criptoagilidad no elimina la necesidad de seleccionar mecanismos autorizados; la complementa, haciendo posible sustituirlos cuando la autoridad competente o la evolución del riesgo lo exijan. En sistemas con larga vida útil, este requisito puede ser más valioso que la elección puntual de un algoritmo específico (Centro Criptológico Nacional, 2026).
Migración gradual, pruebas e interoperabilidad	La adopción debería precederse de pilotos y pruebas en entornos representativos, con especial atención a rendimiento, tamaño de mensajes, compatibilidad con protocolos, dispositivos heredados, recuperación ante fallos y coexistencia con sistemas aún no migrados. Las pruebas deben incluir escenarios de reversión y continuidad. En sistemas interadministrativos o dependientes de terceros, la interoperabilidad debe tratarse como una condición jurídica de disponibilidad y autenticidad, no como un mero detalle de ingeniería (Joseph et al., 2022; Näther et al., 2024).

Área de aplicación	Descripción
Soluciones híbridas cuando sean adecuadas, estandarizadas y evaluadas	Los enfoques híbridos pueden ser útiles durante la transición, pero deberían utilizarse cuando exista una especificación suficientemente madura, pruebas de interoperabilidad y una razón de riesgo que los justifique. La solución debe evitar degradaciones silenciosas hacia el componente clásico y definir claramente las reglas de validación. En entornos sujetos a autorización o certificación criptográfica, la organización deberá respetar las decisiones del CCN y, cuando proceda, los esquemas europeos aplicables; la existencia de un estándar extranjero no sustituye por sí misma esas exigencias.
Preservación a largo plazo de firmas, sellos y evidencias	Las organizaciones deberían identificar documentos, expedientes, registros y evidencias cuya integridad, autenticidad o trazabilidad deban mantenerse durante periodos prolongados. Para ellos debe planificarse la conservación de datos de validación, la renovación de sellos de tiempo, el resellado o las transformaciones que resulten apropiadas conforme a las políticas de firma y al marco eIDAS. Cada transformación debe quedar documentada para preservar la cadena de custodia y la verificabilidad histórica. Esta medida es particularmente relevante para la dimensión de trazabilidad y se alinea con mp.info.3 y mp.info.4 del ENS (Real Decreto 311/2022, anexo II).
Contratación y cadena de suministro	La transición depende en gran medida de proveedores. Los contratos de adquisición y servicios deberían evolucionar hacia requisitos de actualización criptográfica, información sobre dependencias, soporte de estándares reconocidos, calendarios de migración, gestión de vulnerabilidades y mecanismos de salida o sustitución. La ausencia de estas previsiones puede convertir un proveedor en un cuello de botella y comprometer simultáneamente disponibilidad, confidencialidad y autenticidad. La exigencia debe formularse de manera proporcional y tecnológicamente abierta, especialmente mientras el ecosistema continúa madurando.
Monitorización, reevaluación y auditoría	El riesgo debe revisarse a medida que cambien la estimación de capacidades cuánticas, los estándares, las autorizaciones nacionales, los productos certificados y la criticidad de los activos. El ENS ya exige análisis de riesgos actualizado, mejora continua y auditoría periódica. La mitigación postcuántica debería integrarse en esos mecanismos en lugar de crear un ciclo paralelo, de modo que inventario, decisiones, pruebas, excepciones y avances queden disponibles como evidencia de cumplimiento (Real Decreto 311/2022, arts. 7, 27 y 31; anexo III).
Formación y conciencia jurídica del riesgo	Finalmente, la transición exige capacidades profesionales. No es suficiente formar a especialistas en criptografía. Responsables de seguridad, responsables de información y servicios, contratación, archivo, asesoría jurídica, protección de datos y auditoría deben comprender por qué el riesgo tiene una dimensión temporal y cómo una decisión adoptada hoy puede comprometer una obligación futura. La formación debe servir para

Área de aplicación	Descripción
	traducir el lenguaje criptográfico a decisiones de riesgo y de cumplimiento, evitando tanto el alarmismo como la falsa tranquilidad.

Tabla 2. Medidas de mitigación de riesgos. (Fuente: elaboración propia).

11. Discusión: hacia una concepción temporal de la seguridad digital desde la perspectiva jurídica

El análisis de las cinco dimensiones muestra que el rasgo más singular del riesgo cuántico es su temporalidad. En amenazas convencionales, la vulnerabilidad y su explotación suelen estar relativamente próximas. En el escenario cuántico, una organización puede sufrir hoy la captura de información cuyo daño se materializará años después; puede emitir hoy una firma cuya fuerza probatoria deberá conservarse durante décadas; o puede adquirir hoy un sistema que no podrá migrarse cuando la amenaza sea inminente. El deber jurídico de seguridad debe, por tanto, proyectarse sobre el ciclo de vida del activo y no solo sobre el estado actual de la técnica.

Este enfoque permite resolver una aparente paradoja. Si todavía no existe una capacidad cuántica general capaz de romper la criptografía desplegada, podría parecer prematuro exigir actuaciones. Pero si se espera a que exista, la actuación será tardía para la información capturada con anterioridad y para los sistemas cuya migración requiere años. La diligencia razonable se sitúa entre ambos extremos: no presupone una fecha cierta ni exige sustituir indiscriminadamente todos los mecanismos, pero obliga a identificar activos, estimar horizontes, eliminar dependencias evitables y preparar la migración de aquellos casos en los que el tiempo sea un factor crítico.

La segunda consecuencia es que el cumplimiento formal de un catálogo criptográfico no agota la obligación de seguridad. Mientras los mecanismos utilizados sean los autorizados por el marco aplicable, la organización debe emplearlos conforme a las reglas vigentes; pero el ENS incorpora simultáneamente análisis de riesgo, estado de la tecnología, medidas adicionales, revisión y actualización permanente. La seguridad jurídica no consiste en elegir entre cumplimiento normativo y gestión dinámica del riesgo: ambos planos se complementan. El catálogo proporciona un umbral de conformidad; el análisis de riesgos determina si, para un activo concreto, ese umbral debe acompañarse de medidas adicionales de preparación o migración.

La tercera consecuencia es que el concepto de 'estado de la técnica' debe manejarse con prudencia. La publicación de FIPS post-cuánticos por NIST, la Recomendación de la Comisión o los trabajos de ENISA no convierten automáticamente una solución en obligatoria para el ENS. Sí evidencian que la transición ha superado la fase de mera especulación académica y se encuentra en fase de normalización y despliegue. A medida que existan perfiles interoperables, productos evaluados, decisiones del CCN y estándares europeos, el umbral de diligencia podrá desplazarse. La valoración jurídica deberá realizarse en el momento relevante y con arreglo a la información entonces disponible.

Finalmente, la perspectiva de las cinco dimensiones impide reducir la política postcuántica a la confidencialidad. La autenticidad y la integridad afectan la confianza en identidades, documentos y software; la trazabilidad afecta la prueba y la rendición de cuentas; y la disponibilidad puede verse comprometida por una migración defectuosa. Un programa centrado únicamente en cifrar datos con algoritmos resistentes a quantum puede, paradójicamente, empeorar la seguridad global si no preserva estas otras propiedades. El ENS ofrece una ventaja metodológica: obliga a evaluar el

impacto multidimensional y permite integrar la transición en un marco ya conocido por las entidades públicas y por sus proveedores.

12. Conclusiones

De todo lo anterior podemos extraer las siguientes conclusiones:

1. La computación cuántica plantea un problema jurídico de ciberseguridad antes de que exista un computador cuántico capaz de quebrar de forma operativa los mecanismos asimétricos desplegados. La razón es temporal: los activos protegidos hoy pueden seguir necesitando confidencialidad, integridad, autenticidad o valor probatorio cuando la capacidad de ataque sea distinta. El riesgo *harvest now, decrypt later* es la manifestación más evidente, pero no la única.
2. Las cinco dimensiones del ENS proporcionan una estructura jurídicamente fértil para ordenar el problema. El propio anexo I conecta su afectación con el incumplimiento de leyes y regulaciones, de manera que disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad actúan como categorías de transición entre amenaza técnica e impacto jurídico. Esto permite superar el enfoque reductivo que identifica PQC exclusivamente con cifrado de confidencialidad.
3. Deben distinguirse el riesgo cuántico de origen y el riesgo de transición postcuántica. El primero deriva de la futura vulnerabilidad de mecanismos clásicos; el segundo, de la complejidad de migrar sistemas reales. Los fallos de interoperabilidad, los errores de composición híbrida, la pérdida de verificabilidad histórica, la dependencia de proveedores o la indisponibilidad durante cambios de infraestructura pueden comprometer las mismas dimensiones que la PQC pretende proteger. Una política de transición jurídicamente diligente debe minimizar ambos riesgos simultáneamente.
4. La Recomendación (UE) 2024/1101 y la hoja de ruta de 2025 del Grupo de Cooperación NIS no deben presentarse como fuentes autónomas de obligaciones directamente exigibles a cada entidad. Su relevancia consiste en formalizar el conocimiento institucional del riesgo, orientar la coordinación europea y contribuir a concretar expectativas de diligencia en marcos basados en gestión dinámica del riesgo. Para las entidades sometidas al ENS, esta evolución se inserta naturalmente en los arts. 7, 27, 28 y 39 del Real Decreto 311/2022.
5. El núcleo de la mitigación no debe ser, todavía, la imposición indiscriminada de un algoritmo concreto, sino la preparación verificable de la transición: gobernanza, inventario criptográfico, clasificación por horizonte de protección, criptoagilidad, pilotos, interoperabilidad, continuidad, preservación de evidencias, gestión de proveedores, monitorización y auditoría. Cuando los marcos nacionales y europeos consoliden mecanismos, perfiles y certificaciones, esa preparación permitirá migrar de forma ordenada y jurídicamente defendible.

En suma, la transición postcuántica debe entenderse como una nueva manifestación del deber de anticipación propio de la ciberseguridad basada en riesgos. El desafío jurídico no consiste en adivinar la fecha del Q-Day, sino en determinar cuándo una organización razonable, atendiendo al valor y duración de sus activos, al tiempo de migración y al estado de conocimiento institucional, debe empezar a actuar. En el ámbito del ENS, esa pregunta puede formularse sin abandonar su

arquitectura actual: basta con tomarse en serio su carácter dinámico, su enfoque de ciclo de vida y la función normativa de sus cinco dimensiones de seguridad.

Referencias

Balarabe, K. (2025). Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap. European Journal of Risk Regulation, 16(2), 794–813. https://doi.org/10.1017/err.2025.8

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

Centro Criptológico Nacional (CCN). (2022). CCN-STIC-807. Criptología de empleo en el Esquema Nacional de Seguridad. CCN-CERT.

Centro Criptológico Nacional. (2026). *CCN-TEC 009 BP/37: Recomendaciones para una transición postcuántica segura*. Centro Criptológico Nacional.

Comisión Europea. (2024). Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. Official Journal of the European Union, L, 2024/1101.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148. DOUE L 333, de 27 de diciembre de 2022.

ENISA. (2021). Post-Quantum Cryptography: Current State and Quantum Mitigation. European Union Agency for Cybersecurity.

ENISA. (2022). Post-Quantum Cryptography: Integration Study. European Union Agency for Cybersecurity.

ENISA. (2026). Hybridization of traditional cryptographic mechanisms with PQC – Standardisation Status (30 April 2026). European Union Agency for Cybersecurity.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212–219. https://doi.org/10.1145/237814.237866

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605, 237–243. https://doi.org/10.1038/s41586-022-04623-2

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, núm. 294, de 6 de diciembre de 2018, BOE-A-2018-16673.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Näther, C., Herzinger, D., Gazdag, S.-L., Steghöfer, J.-P., Daum, S., & Loebenberger, D. (2024). Migrating software systems towards post-quantum cryptography—A systematic literature review. IEEE Access, 12, 132107–132126. https://doi.org/10.1109/ACCESS.2024.3450306

NIS Cooperation Group. (2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (Part 1, v1.1, 11 June 2025). European Commission.

National Institute of Standards and Technology (NIST). (2024a). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology (NIST). (2024b). FIPS 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology (NIST). (2024c). FIPS 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

Pérez Bes, F. La regulación de las tecnologías cuánticas: una cuestión de seguridad nacional. (2025). Independently published.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, núm. 106, de 4 de mayo de 2022, BOE-A-2022-7191 (texto consolidado con última modificación de 6 de noviembre de 2024).

Real Decreto 1125/2024, de 5 de noviembre, por el que se regulan la organización y los instrumentos operativos para la Administración Digital de la Administración del Estado. Boletín Oficial del Estado, núm. 268, de 6 de noviembre de 2024, BOE-A-2024-22935.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L 119, de 4 de mayo de 2016.

Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, en la redacción resultante del Reglamento (UE) 2024/1183. DOUE L 257, de 28 de agosto de 2014.

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital. DOUE L, 2024/1183, de 30 de abril de 2024.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Truby, J., & Baysal, O. (2026). Q-Day and the international legal order: International law implications of quantum cybersecurity disruption. Journal of Cyber Policy. Advance online publication. https://doi.org/10.1080/23738871.2026.2689321