isms forum

cisco

CSC
CYBER SECURITY CENTRE

Riesgos y Oportunidades del Post-Quantum en Ciberseguridad

Guía para CISOs

Cisco, a través de su programa de inversiones CDA “Country Digital Acceleration”, llamado DIGITALIZA en España, está comprometido en acelerar la digitalización de nuestro país en los distintos ámbitos de nuestra economía y sociedad. En particular, el desarrollo del conocimiento y concienciación de la práctica de ciberseguridad en las organizaciones españolas es un punto clave. En este contexto, el análisis se centra en el impacto de la computación cuántica sobre los modelos actuales de ciberseguridad, abordando la necesidad de anticipar la transición hacia criptografía post-cuántica, la gestión del riesgo tecnológico y la adaptación de los marcos de gobierno de la seguridad. El documento ofrece orientaciones prácticas dirigidas a CISOs y responsables de seguridad para apoyar la toma de decisiones estratégicas, la planificación de la migración criptográfica y la preparación organizativa ante los retos tecnológicos y regulatorios emergentes asociados al escenario post-quantum.

Autores

Coordinadores

Ángel Ortiz

Iker Osorio

Javier Pinillos

Coordinación

Beatriz García

Coautores

Alberto López

Ana Belén Galán

Chema Rivera

Jaime Castro

Jesús Valverde

Jose Ramón Monleón

Mario Encinas

Álvaro Ontañón

Antonio Fontiveros

David Llorente

Jaime Perea Amor

José González

Kerman Arcelay

Trina de Miguel

Amelia Torres

Arturo Beltrán

Gabriel Moliné

Jesús Abascal

José Ignacio Mora

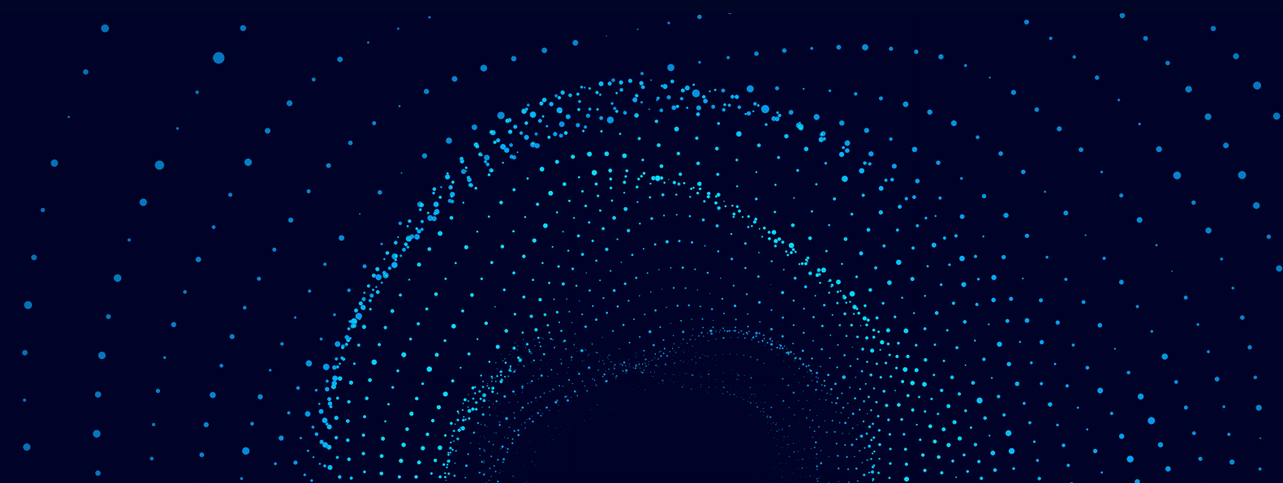
Mariano Benito

Edición

Beatriz García

Diseño y maquetación

Susana Marín



Contenido

1. Introducción

1.1. Objetivo del documento

El presente documento tiene como objetivo proporcionar una visión integral, estructurada y orientada a la acción sobre los Riesgos y Oportunidades derivados de la computación cuántica en el ámbito de la ciberseguridad, con especial foco en su impacto sobre la criptografía, la gestión del riesgo y la resiliencia de las organizaciones.

En este contexto, el documento analiza la evolución de la amenaza cuántica y su creciente relevancia en el entorno tecnológico, regulatorio y geopolítico, así como el estado del arte en criptografía post-quantum (Post-Quantum Cryptography, PQC). La transición hacia este nuevo paradigma no responde únicamente a una evolución tecnológica, sino a un cambio estructural en los fundamentos de la seguridad digital, que afecta directamente a la confidencialidad, integridad, disponibilidad y autenticidad de la información.

A partir de este análisis, se identifican y caracterizan los principales riesgos asociados al escenario post-quantum, incluyendo el modelo harvest now, decrypt later, la obsolescencia progresiva de los algoritmos criptográficos actuales, la dependencia de terceros y proveedores, así como la exposición derivada del uso de tecnologías clave como cloud, IoT, OT e inteligencia artificial. Estos riesgos se analizan no solo desde una perspectiva técnica, sino también desde su impacto en negocio, cumplimiento y reputación.

Se establece un enfoque metodológico que permite a las organizaciones identificar, clasificar y priorizar sus activos criptográficos críticos, evaluar su nivel de exposición y cuantificar el riesgo post-quantum mediante indicadores, modelos de madurez y mecanismos de scoring. Este enfoque facilita la toma de decisiones informadas y alineadas con los objetivos estratégicos de la organización.

Por otro lado, se definen estrategias de mitigación y transición hacia entornos seguros frente a la computación cuántica, incorporando conceptos como la cripto-agilidad, los modelos híbridos y la integración progresiva de estándares PQC en las infraestructuras existentes. Estas estrategias se complementan con recomendaciones prácticas y una hoja de ruta de implantación que permite abordar la transición de forma planificada, realista y sostenible en el tiempo.

1.2. Alcance y público objetivo

El contenido abarca desde la contextualización de la amenaza y el análisis del entorno regulatorio, hasta la identificación de riesgos, la clasificación de activos críticos, la evaluación del nivel de exposición y la definición de estrategias de mitigación y transición. Asimismo, se incluyen elementos clave como modelos de madurez, mecanismos de priorización, integración en el gobierno corporativo y desarrollo de capacidades operativas que permitan a las organizaciones evolucionar hacia un estado de “quantum readiness”.

El documento es transversal y aplicable a organizaciones de distintos tamaños y sectores, con especial énfasis en aquellas que gestionan información sensible, activos críticos o infraestructuras estratégicas. Entre estos sectores se incluyen, de forma destacada, el financiero, energético, sanitario, industrial, telecomunicaciones y administración pública, donde la protección de la información a largo plazo y la continuidad operativa resultan especialmente críticas.

Asimismo, el documento contempla entornos tecnológicos complejos y distribuidos, caracterizados por la adopción de arquitecturas cloud, el despliegue masivo de dispositivos IoT, la integración de sistemas OT y el uso creciente de inteligencia artificial. En estos entornos, la superficie de exposición al riesgo post-quantum se amplía significativamente, lo que requiere un enfoque coordinado y multidimensional.

Está dirigido principalmente a perfiles con responsabilidad en la toma de decisiones estratégicas y en la gestión de la ciberseguridad. Entre ellos se incluyen la Dirección de Seguridad de la Información (CISO), la Dirección de Tecnología (CIO), responsables de riesgos, auditoría interna, cumplimiento normativo y continuidad de negocio, así como miembros de la alta dirección y órganos de gobierno que requieren comprender el impacto del riesgo cuántico desde una perspectiva empresarial. Adicionalmente, el documento resulta de interés para equipos técnicos, arquitecturas de seguridad, responsables de infraestructura y gestión de proveedores, que deberán participar activamente en la implementación de capacidades de cripto-agilidad y en la transición hacia soluciones PQC.

2. Contexto y Justificación

2.1. Evolución de la amenaza cuántica

En los últimos años, la computación cuántica ha dejado de ser un ámbito estrictamente académico para convertirse en un factor relevante dentro del análisis estratégico de riesgos de ciberseguridad. Aunque todavía no existe evidencia pública de un ordenador cuántico capaz de comprometer de forma práctica la criptografía de clave pública actualmente desplegada, el cambio de contexto viene impulsado por la combinación de la presión regulatoria, los largos horizontes de protección de los datos y los ciclos de vida cada vez más extensos de las infraestructuras tecnológicas.

Durante mucho tiempo, la amenaza cuántica fue tratada como un riesgo lejano, sin impacto real en las decisiones de arquitectura o inversión. Sin embargo, esta aproximación ya no resulta sostenible. Reguladores, autoridades de ciberseguridad y organismos de estandarización coinciden en que la preparación frente al escenario post-quantum debe iniciarse con antelación suficiente, incluso cuando la capacidad cuántica criptográficamente relevante todavía no se haya materializado.

Un elemento clave para entender esta urgencia es el denominado riesgo Harvest Now, Decrypt Later (HNDL), que describe la posibilidad de que actores maliciosos estén capturando hoy información cifrada con el objetivo de descifrarla en el futuro. Este escenario afecta especialmente a los datos que deben mantenerse confidenciales durante largos periodos de tiempo y desplaza el foco desde el mero avance tecnológico hacia la gestión del tiempo, la planificación y la gobernanza del riesgo.

En este contexto resulta útil introducir el Teorema de la desigualdad de Mosca[1], que relaciona tres variables: el tiempo durante el cual un dato debe permanecer protegido, el tiempo necesario para completar la migración criptográfica y el horizonte estimado de aparición de un ordenador cuántico relevante. Este razonamiento permite comprender que el riesgo cuántico se materializa antes de la existencia efectiva de dicha capacidad, cuando los plazos de protección y migración superan el margen temporal disponible.

Más allá de las comunicaciones cifradas tradicionales, la amenaza cuántica afecta de forma transversal a dominios críticos como la identidad digital, la firma de software y firmware, los entornos cloud, los dispositivos IoT y los sistemas de tecnología operacional. En estos ámbitos, la obsolescencia criptográfica no solo compromete la confidencialidad, sino también la integridad, la autenticidad y, en determinados casos, la seguridad operativa y física.

Desde una perspectiva de gestión del riesgo, esta combinación de factores introduce una asimetría temporal especialmente compleja: las decisiones criptográficas que se toman hoy condicionan la seguridad de la información durante décadas, mientras que la capacidad de reacción futura está limitada por la inercia tecnológica y organizativa. Esta asimetría es la que convierte la amenaza cuántica en un problema de planificación estratégica y no únicamente en una cuestión de madurez tecnológica.

[1] Mosca, M. (2015). Cybersecurity in a quantum world: Will we be ready? National Institute of Standards and Technology (NIST). https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

2.2. Regulación y compliance (NIS2, DORA, CNSA 2.0, etc.)

Durante años, quienes ocupan el rol de CISO han tratado la computación cuántica como un riesgo estratégico a largo plazo, un elemento que merecía una mención en el registro de riesgos, pero que rara vez competía por atención o presupuesto con las amenazas operativas del día a día. Esa etapa ha terminado.

El cambio no se ha producido en el ámbito científico, donde continúa sin existir un ordenador cuántico criptográficamente relevante, sino en la posición adoptada por reguladores y supervisores. La pregunta clave ya no es cuándo llegará dicha capacidad, sino si las organizaciones pueden demostrar que están gestionando este riesgo de forma proporcionada, estructurada y alineada con el estado del arte.

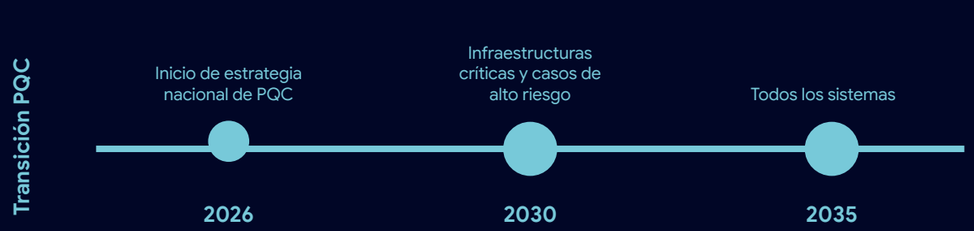
En este contexto, la regulación actúa como un mecanismo de traducción entre una amenaza tecnológica emergente y las obligaciones reales de gobierno corporativo. Los marcos regulatorios no parten de la premisa de una ruptura criptográfica inmediata, sino de la necesidad de demostrar anticipación, control y capacidad de adaptación frente a riesgos que evolucionan en horizontes temporales largos.

NIS2: La criptografía como obligación de gobernanza

La Directiva NIS2 (Directiva (UE) 2022/2555[2]) no menciona explícitamente la criptografía post-quantum ni prescribe algoritmos concretos. Sin embargo, su artículo 21 exige que las entidades esenciales e importantes adopten medidas técnicas, operativas y organizativas adecuadas y proporcionadas, teniendo en cuenta el estado del arte. Asimismo, establece la obligación de disponer de políticas y procedimientos relativos al uso de la criptografía y, cuando proceda, del cifrado.

El Reglamento de Ejecución (UE) 2024/2690[3] concreta estas exigencias técnicas, introduciendo expectativas claras en materia de políticas criptográficas, alineamiento con estándares internacionales y mecanismos de adaptación ante cambios en el entorno de amenazas. En este marco, la criptografía deja de ser un control técnico aislado para convertirse en un elemento de gobernanza sujeto a supervisión y evidencia.

La hoja de ruta coordinada de la Unión Europea para la transición a la criptografía post-quantum, publicada en 2025 por el Grupo de Cooperación NIS[4], refuerza este enfoque al establecer hitos temporales que sirven como referencia común para las organizaciones europeas.



[2] Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2). Diario Oficial de la Unión Europea, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[3] Comisión Europea. (2024). Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y se detallan los casos en que un incidente se considera significativo (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea, L, 2024/2690. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

[4] National Institute of Standards and Technology. (2019). Migration to post-quantum cryptography (NIST Internal Report 8240). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf

DORA: la amenaza cuántica como riesgo operativo en el sector financiero

El Reglamento de Resiliencia Operativa Digital (DORA, Reglamento (UE) 2022/2554)[5], en vigor desde enero de 2025, integra la evolución criptográfica dentro de la gestión del riesgo TIC del sector financiero. Las normas técnicas de desarrollo exigen que las entidades se mantengan al corriente de los avances en criptoanálisis y gestionen las amenazas derivadas de ellos, incluidas las asociadas a la computación cuántica.

A diferencia de otros marcos normativos, DORA no aborda estas cuestiones como recomendaciones técnicas, sino como parte del núcleo de la resiliencia operativa digital. La expectativa regulatoria es que la evolución de la criptografía se gestione de forma sistemática dentro de los procesos habituales de control, auditoría y supervisión.

CNSA 2.0: El reloj estadounidense y su influencia global

Al otro lado del Atlántico, la NSA publicó en septiembre de 2022 la Commercial National Security Algorithm Suite 2.0 (CNSA 2.0[6]), define los algoritmos resistentes al quantum que reemplazarán progresivamente a los actuales en los sistemas de seguridad nacional estadounidenses.

Aunque su ámbito de aplicación directo es limitado, su impacto práctico es global. El calendario de adopción y retirada de algoritmos clásicos establecido por CNSA 2.0 condiciona las hojas de ruta de los principales proveedores tecnológicos, influyendo de facto en la disponibilidad de soluciones compatibles con entornos post-quantum a escala internacional.

En la práctica, muchas organizaciones adoptarán capacidades post-quantum no por una exigencia regulatoria directa, sino como consecuencia de la evolución natural de los productos y servicios que consumen.

[5] European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[6] National Security Agency. (2022). Commercial national security algorithm suite 2.0 (CNSA 2.0) FAQ. U.S. Department of Defense. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

Otros marcos regulatorios y estándares relevantes

Otros marcos regulatorios y normativos refuerzan esta tendencia. PCI DSS endurece los requisitos criptográficos en entornos de pago; el *Cyber Resilience Act* introduce exigencias de seguridad a lo largo de todo el ciclo de vida de los productos digitales; y las posiciones técnicas de agencias nacionales como ANSSI o BSI influyen en las expectativas de los supervisores durante la transposición de NIS2.

Asimismo, iniciativas europeas como el futuro *Quantum Act* apuntan a una progresiva armonización de estándares y criterios de evaluación en materia de seguridad cuántica.

Regulación: el compliance como catalizador, no como destino

Existe el riesgo de abordar la preparación post-quantum como un ejercicio puramente formal de cumplimiento. Sin embargo, la regulación no exige la adopción inmediata de criptografía post-quantum en todos los sistemas, sino la capacidad de demostrar que el riesgo está identificado, gobernado y planificado.

En este sentido, la regulación actúa como un catalizador que convierte un riesgo tecnológico de largo plazo en un programa estructurado de gestión, con responsabilidades, evidencias y horizontes temporales definidos. La traducción de este marco regulatorio en decisiones prácticas y hoja de ruta se desarrolla en el Capítulo 9.

2.3. Estado del arte en criptografía post-cuántica (PQC)

La criptografía post-quantum (Post-Quantum Cryptography, PQC) se encuentra en un punto de madurez significativamente más avanzado que hace apenas unos años. Los algoritmos diseñados para resistir ataques de futuros ordenadores cuánticos han evolucionado desde propuestas académicas hacia estándares formales, hojas de ruta regulatorias y despliegues iniciales en entornos productivos. Este cambio permite que las organizaciones dispongan de una base técnica y estratégica clara para orientar su transición hacia entornos quantum-safe.

Evolución y estandarización internacional

El principal impulsor de esta transición ha sido el proceso de estandarización liderado por el NIST, que ha culminado con la publicación de los estándares FIPS 203, 204 y 205[7], definiendo algoritmos para encapsulación de claves y firmas digitales resistentes a ataques cuánticos.

Los algoritmos seleccionados se estructuran en dos grandes categorías:

- **Encapsulación de claves (KEM):** ML-KEM (basado en CRYSTALS-Kyber), considerado el mecanismo de referencia para intercambio seguro de claves.
- **Firmas digitales:** ML-DSA (CRYSTALS-Dilithium), Falcon y SLH-DSA (SPHINCS+), con distintos compromisos entre eficiencia y robustez.

Estos esquemas se apoyan en problemas matemáticos considerados resistentes frente a computación cuántica, como las redes euclidianas (lattices) o funciones hash.[8]

Adicionalmente, el NIST ha anunciado que en una fase posterior se publicará **FIPS 206**, un cuarto estándar de firma digital post cuántica basado en **Falcon**[9], incorporando mejoras orientadas a su implementación práctica y a su adopción en entornos operacionales con restricciones de rendimiento y tamaño de clave. Este anuncio refuerza el posicionamiento de Falcon como algoritmo complementario a ML DSA dentro del ecosistema post-cuántico definido por el NIST.

En paralelo, la suite Commercial National Security Algorithm Suite 2.0[10] (CNSA 2.0) define una hoja de ruta operativa que trasciende el ámbito estadounidense y actúa como referencia global en la cadena de suministro tecnológica. Esta suite incluye:

- ML-KEM para intercambio de claves
- ML-DSA para firmas digitales
- LMS y XMSS para firma de software y firmware
- AES-256 como base de criptografía simétrica.

Además, establece hitos concretos: **compatibilidad obligatoria en nuevos sistemas a partir de 2027 y retirada progresiva de algoritmos clásicos como RSA y ECC hasta 2035**. Este calendario condiciona directamente las hojas de ruta de los principales proveedores tecnológicos.

Elemento / Algoritmo	Función dentro de CNSA 2.0
ML-KEM	Intercambio de claves
ML-DSA	Firmas digitales
LMS	Firma de software y firmware
XMSS	Firma de software y firmware
AES-256	Criptografía simétrica

Nivel de madurez tecnológica

Desde una perspectiva técnica, la PQC ha superado la fase experimental y se encuentra en una etapa de adopción progresiva, con implementaciones disponibles en librerías criptográficas, protocolos y plataformas cloud.

Entre los avances más relevantes:

- Integración en librerías como OpenSSL y BoringSSL
- Soporte en Transport Layer Security (TLS) en configuraciones híbridas
- Primeras implementaciones en infraestructuras cloud y servicios críticos

Sin embargo, persisten limitaciones estructurales que afectan a su despliegue:

- Mayor tamaño de claves y firmas, con impacto en latencia y consumo de ancho de banda
- Sobrecoste computacional, especialmente en entornos con recursos limitados
- Madurez incompleta del ecosistema PKI, incluyendo certificados híbridos.
- Limitada experiencia operativa a gran escala

Organismos como la ENISA destacan que la transición debe abordarse de forma progresiva y gestionada, dada la complejidad de los entornos reales[11].

[7] National Institute of Standards and Technology. Post-quantum cryptography standardization: Round 3 submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

[8] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer.

[9] National Institute of Standards and Technology. (2022, July 5). NIST announces first four quantum resistant cryptographic algorithms. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[10] National Security Agency. (2025, May 30). Commercial national security algorithm suite 2.0 (CNSA 2.0): Algorithms. U.S. Department of Defense. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[11] European Union Agency for Cybersecurity (ENISA). (2023). Post-quantum cryptography: Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Prácticas actuales de despliegue: enfoque híbrido

El estado del arte no se limita a la selección de algoritmos, sino a su integración operativa. En este sentido, el enfoque predominante consiste en la adopción de modelos híbridos, donde algoritmos clásicos y post-cuánticos coexisten dentro del mismo protocolo.

Este modelo permite:

- Mitigar el riesgo de ataques tipo *harvest now, decrypt later* .
- Mantener compatibilidad con *sistemas legacy*.
- Reducir el riesgo operativo durante la transición.

Un caso representativo es TLS híbrido, que combina ECDHE con ML-KEM con un **mecanismo de encapsulación post-cuántico**, conforme a los trabajos de estandarización más recientes del IETF para TLS 1.3, alineados con ML KEM como algoritmo de referencia definido en FIPS 203.

Este enfoque responde a un principio de resiliencia: la seguridad del sistema se mantiene siempre que al menos uno de los algoritmos permanezca seguro

Adopción por proveedores tecnológicos

Los principales proveedores tecnológicos han comenzado a integrar capacidades PQC en sus plataformas, marcando una transición progresiva hacia entornos “quantum-ready”.

En la práctica, esto se traduce en:

- Terminaciones TLS 1.3 con soporte híbrido (clásico + PQC).
- Servicios de gestión de claves (KMS) con soporte para ML-KEM.
- Migración progresiva del tráfico interno de centros de datos hacia suites PQC.

Asimismo, los fabricantes de módulos de seguridad hardware (HSM) están desarrollando soporte para algoritmos post-cuánticos, un elemento crítico para sectores regulados como el financiero o infraestructuras críticas.

No obstante, el modelo de responsabilidad compartida implica que la adopción completa no depende únicamente del proveedor, sino también de la capacidad de la organización para actualizar clientes, aplicaciones y arquitecturas propias.

Modelos de madurez y preparación organizativa

El estado del arte también se define por la existencia de modelos de madurez que permiten evaluar el nivel de preparación de una organización frente al riesgo cuántico.

Entre los más relevantes destacan:

- PQC Maturity Model (PQCMM)[12]
- Quantum Readiness Assurance Maturity Model (QRAMM)[13]

Estos modelos describen una evolución progresiva desde organizaciones sin visibilidad criptográfica hasta aquellas que:

- Mantienen inventarios completos de algoritmos, claves y certificados (Cryptographic Bill Of Materials - CBOM)
- Aplican principios de cripto-agilidad
- Integran PQC en arquitecturas y procesos por defecto
- Eliminan progresivamente algoritmos no resistentes (“zero legacy”)

Las guías del **NIST NCCoE**[14] y organismos como CISA refuerzan esta aproximación, recomendando el uso de herramientas automatizadas de descubrimiento criptográfico y la ejecución de pilotos tempranos en casos de uso críticos.

Implicaciones estratégicas

El estado actual de la PQC confirma que la transición no es un problema exclusivamente tecnológico, sino un proceso organizativo que afecta a:

- Arquitectura de seguridad (PKI, protocolos, identidad).
- Gestión de activos criptográficos.
- Relación con proveedores.
- Cumplimiento normativo y auditoría.

La adopción de PQC exige incorporar capacidades de cripto-agilidad, entendidas como la capacidad de evolucionar algoritmos sin rediseñar sistemas completos[15].

---

[12] Post-quantum Cryptography Forum (PKI Consortium). (2025, October 27). Defining quantum readiness: Introducing the post-quantum cryptography maturity model. https://pkic.org/2025/10/27/defining-quantum-readiness-introducing-the-post-quantum-cryptography-maturity-model/

[13] Quantum Risk Assessment and Maturity Model (QRAMM). https://qramm.org/resources/csnp. QRAMM: Quantum risk assessment and maturity model. https://github.com/csnp/qramm

[14] National Institute of Standards and Technology. National Cybersecurity Center of Excellence (NCCoE). https://www.nccoe.nist.gov/

[15] National Institute of Standards and Technology. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NISTIR 8309). https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

3. Panorama de riesgos del Post-Quantum

3.1. *"Harvest Now, Decrypt Later"*

El riesgo *"Harvest Now, Decrypt Later"*, o "Cosechar ahora, descifrar después", representa una de las amenazas más inminentes y silenciosas derivadas de la computación cuántica, ya que no requiere esperar a la disponibilidad de ordenadores cuánticos funcionales para causar impacto en el presente.

Este riesgo se materializa porque la criptografía de clave pública actual protege los datos hoy, pero no garantiza su confidencialidad frente a futuras capacidades cuánticas[16].

El impacto de este riesgo no recae en la pérdida de disponibilidad o integridad inmediata, sino en la exposición futura de la confidencialidad. Por lo tanto, el nivel de riesgo HNDL de una organización está directamente relacionado con el "horizonte de confidencialidad" o ciclo de vida de su información. Si una empresa maneja datos que deben mantenerse en secreto durante décadas, como historiales médicos, secretos industriales, propiedad intelectual, infraestructuras críticas o información estratégica de negocio y recursos humanos, el ataque HNDL ya ha vulnerado su seguridad hoy. Para cuando el CRQC esté operativo, esa información, ahora descifrada, seguirá siendo valiosa y explotable, generando graves consecuencias operativas, legales (incumplimiento de normativas de protección de datos) y reputacionales.

3.2. Obsolescencia tecnológica y *lock-in*

Este tipo de riesgo aborda el impacto operativo y financiero que la transición a la criptografía post-quantum ejerce sobre la infraestructura física actual y la gestión de proveedores en las organizaciones.

Los nuevos algoritmos post-quantum estandarizados se caracterizan, en términos generales, por requerir tamaños de clave más grandes y un mayor consumo de recursos computacionales (CPU y memoria) en comparación con la criptografía clásica. Esta exigencia técnica genera un riesgo inminente de obsolescencia tecnológica prematura, especialmente crítico en dispositivos con capacidades de procesamiento limitadas o con ciclos de vida muy largos. Equipos como los sistemas de OT, los terminales de punto de venta (TPV) o los sistemas físicos de control de acceso a menudo carecen de la capacidad necesaria para procesar estos nuevos algoritmos. En consecuencia, las organizaciones se enfrentan al riesgo de tener que renovar hardware costoso mucho antes de su amortización planificada para mantener la seguridad de las operaciones.

Paralelamente, la urgencia por mitigar la amenaza cuántica introduce el riesgo de *"lock-in"* o cautividad tecnológica. Ante la presión del mercado, algunos proveedores de tecnología ofrecen soluciones criptográficas propietarias y cerradas bajo la etiqueta de "seguridad cuántica". La adopción de estas alternativas[17] no estandarizadas ata a la organización al ecosistema de un único proveedor, dificultando la integración futura con sistemas de terceros y disparando los costes de mantenimiento a largo plazo. Para mitigar este riesgo, la estrategia de compras debe exigir de forma rigurosa la implementación de algoritmos y protocolos basados en estándares abiertos y oficiales, como los publicados por el NIST.

3.3. Cadena de suministro y terceros

En el escenario post-quantum, la cadena de suministro se convierte en uno de los vectores de riesgo más críticos, no tanto por la existencia de vulnerabilidades individuales, sino por la necesidad de coordinar la transición criptográfica entre múltiples organizaciones interdependientes. Proveedores tecnológicos, integradores y prestadores de servicios gestionan los mismos riesgos de obsolescencia criptográfica y deben iniciar, en paralelo, sus propios procesos de migración hacia algoritmos y arquitecturas post quatum. La falta de sincronización entre estas transiciones introduce un riesgo sistémico: si la organización migra y sus proveedores no lo hacen, pueden producirse incompatibilidades técnicas; si el proveedor migra y la organización no está preparada, el riesgo se materializa en forma de ruptura operativa o degradación del servicio.

Este riesgo de sincronización se ve reforzado por el marco regulatorio vigente. Tanto la Directiva NIS2 como el Esquema Nacional de Seguridad (ENS) trasladan explícitamente a las organizaciones la responsabilidad de gestionar los riesgos derivados de terceros y de la cadena de suministro, incluyendo aquellos relacionados con la criptografía y la resiliencia tecnológica[18].

En particular, NIS2 exige que las entidades esenciales e importantes adopten medidas proporcionadas para mitigar riesgos de ciberseguridad en su ecosistema de proveedores, mientras que el ENS incorpora la obligación de evaluar y controlar los mecanismos criptográficos utilizados por servicios externalizados y sistemas interconectados. En el contexto post-quantum, esto implica que la preparación en PQC no puede abordarse de forma aislada, sino como un proceso coordinado con terceros críticos.

---

[16] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., & Work, D. (2016). Report on post-quantum cryptography (NIST Interagency/Internal Report 8105). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[17] European Union Agency for Cybersecurity. (2024). Cryptography. https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography

[18] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

Para gestionar este riesgo de forma efectiva, la organización debe incorporar requisitos específicos de transición post-quantum en sus relaciones contractuales. Esto incluye exigir visibilidad sobre los algoritmos criptográficos utilizados por proveedores y subproveedores (transparencia criptográfica), conocer sus hojas de ruta de migración, y establecer mecanismos de revisión periódica alineados con los plazos regulatorios y de negocio. En términos prácticos, los contratos deben evolucionar desde una garantía puntual de seguridad hacia un compromiso explícito de capacidad de evolución criptográfica, asegurando que los servicios prestados puedan adaptarse a la retirada progresiva de algoritmos clásicos sin comprometer la continuidad operativa.

En última instancia, el riesgo post-quantum en la cadena de suministro no es un problema técnico individual, sino un riesgo de gobernanza. La organización sigue siendo responsable, ante reguladores, clientes y auditores, de la confidencialidad, integridad y autenticidad de la información procesada por terceros. Abordar este riesgo exige pasar de una evaluación estática del proveedor a un modelo dinámico que garantice visibilidad, control y capacidad de adaptación continua de la seguridad criptográfica a lo largo de toda la cadena de suministro.

3.4. Riesgo de cumplimiento y auditoría

La transición al escenario post-quantum introduce un riesgo específico de cumplimiento[19] y auditoría[20]: la dificultad para demostrar, de forma objetiva y documentada, que la organización está gestionando adecuadamente la obsolescencia criptográfica frente a una amenaza de maduración lenta pero reconocida por los reguladores.

A diferencia de otros riesgos de ciberseguridad, el riesgo cuántico no se manifiesta en fallos inmediatos o incidentes visibles, sino en la exposición acumulada derivada del uso continuado de algoritmos cuya vulnerabilidad futura es conocida. Esta característica complica su tratamiento bajo esquemas de auditoría tradicionales, que suelen apoyarse en evidencias reactivas y no en riesgos prospectivos.

En este contexto, las organizaciones se enfrentan al riesgo de no poder justificar ante auditores, supervisores o autoridades competentes por qué continúan utilizando determinados mecanismos criptográficos, qué criterios siguen para priorizar su sustitución o cómo garantizan que sus planes de transición son proporcionados al riesgo y alineados con los plazos regulatorios emergentes.

La ausencia de inventarios criptográficos completos, métricas de exposición temporal y hojas de ruta documentadas debilita la posición defensiva de la organización incluso en ausencia de incidentes, y puede traducirse en requerimientos correctivos, observaciones regulatorias o pérdida de confianza institucional.

[19] European Commission. (2024). Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

[20] El Bizri, M., El Hajj, A. M., Sliman, L., & Haidar, A. M. (2026). Institutional approaches to post-quantum cryptography: A comparative analysis of migration frameworks. IEEE Access, 14, 3259 3283. https://doi.org/10.1109/ACCESS.2025.3650465

3.5. Riesgo reputacional y contractual

El riesgo reputacional en el escenario post-quantum es quizás el más intangible pero también el más inmediato: las organizaciones que no actúen a tiempo pueden ser percibidas como tecnológicamente inseguras, poniendo en duda su capacidad de proteger datos sensibles o transacciones críticas. La pérdida de confianza puede provenir tanto de clientes como de mercados, supervisores o socios que exigen garantías de uso de criptografía robusta. A esto se suman riesgos contractuales: la incapacidad de garantizar la continuidad criptográfica puede afectar acuerdos con proveedores e incluso la validez legal futura de contratos firmados electrónicamente bajo algoritmos vulnerables. En un entorno donde la confianza es capital, prepararse para el mundo post-quantum no es solo un requisito de seguridad, sino un imperativo de reputación y negocio. El riesgo reputacional y contractual no deriva únicamente de un fallo técnico, sino de no gestionar adecuadamente la transición criptográfica como un proceso estratégico y gobernado.

3.6. Riesgos sobre: IA, IoT, OT y Cloud

Cuando se habla de riesgo cuántico en los comités de dirección, la conversación tiende a orbitar alrededor de un escenario único: alguien descifra nuestras comunicaciones TLS. Es un escenario legítimo, pero peligrosamente incompleto. La realidad es que la criptografía de clave pública no solo protege un canal de comunicación; es el tejido conectivo que sostiene la integridad de los modelos de inteligencia artificial, la autenticación de millones de dispositivos IoT, la confianza en los comandos que recibe un sistema de control industrial y la arquitectura de seguridad de toda nuestra infraestructura cloud. Comprometer ese tejido no significa solo leer datos; significa poder falsificar identidades, inyectar firmware malicioso, manipular modelos de decisión y colapsar cadenas de confianza completas.

Esta sección analiza cómo la amenaza cuántica se manifiesta de forma diferente, y a menudo más peligrosa, en los cuatro dominios tecnológicos que definen la superficie operativa de la mayoría de las organizaciones: inteligencia artificial, Internet de las Cosas, tecnología operacional e infraestructura cloud. Para un CISO, entender estas diferencias no es un ejercicio académico; es la base para priorizar inversiones, negociar con proveedores y dimensionar un programa de migración PQC que no se limite a proteger el correo electrónico.

Inteligencia Artificial: el activo que nadie incluyó en el inventario criptográfico

La explosión de la IA en los últimos años ha creado una nueva categoría de activos críticos que depende de la criptografía de forma omnipresente pero que rara vez aparece en los inventarios criptográficos tradicionales. Los modelos de aprendizaje automático, los pipelines de datos de entrenamiento, las APIs de inferencia y los flujos de aprendizaje federado utilizan criptografía de clave pública para proteger la confidencialidad de los datos, garantizar la integridad de los modelos y autenticar las comunicaciones entre componentes. Sin embargo, cuando se pregunta *¿dónde se utilizan RSA o ECC?*, la respuesta rara vez incluye la infraestructura de IA.

El problema de la vida útil

Los modelos de IA presentan una característica que amplifica el riesgo cuántico: su longevidad combinada con la sensibilidad de sus datos de entrenamiento. Un modelo entrenado hoy con datos sanitarios, financieros o de propiedad intelectual puede permanecer en producción durante años. Los datos que alimentaron ese modelo, y que pueden haber sido transmitidos cifrados con algoritmos vulnerables, podrían contener información cuya confidencialidad debe mantenerse durante décadas. Si esos datos fueron interceptados y almacenados bajo una estrategia harvest now, decrypt later, el compromiso afecta no solo al dato original sino a todo lo que el modelo aprendió de él.

Amenazas específicas al ecosistema de IA

El riesgo cuántico en IA no se limita a la confidencialidad. Hay al menos cuatro vectores que se deben considerar:

- **Inversión de modelos amplificada.** Los ataques de inversión de modelos (*model inversion*) buscan reconstruir datos de entrenamiento a partir de las respuestas del modelo. Hoy, las protecciones criptográficas que envuelven los datos de entrenamiento y los gradientes actúan como barrera. Un adversario con capacidad cuántica podría romper esas protecciones y acceder directamente a los datos originales, haciendo trivial la reconstrucción de información sensible que el modelo memorizó.
- **Extracción de modelos.** Los modelos de IA representan inversiones de millones de euros en datos, computación y conocimiento. Las APIs de inferencia se protegen mediante autenticación basada en criptografía asimétrica. Si esas credenciales se vuelven falsificables, el robo de modelos a través de consultas masivas se convierte en un riesgo a gestionar.
- **Integridad del aprendizaje federado.** El aprendizaje federado depende de protocolos criptográficos (cifrado homomórfico, computación multipartita segura, compartición de secretos) para permitir el entrenamiento colaborativo sin exponer datos individuales. Muchas de estas técnicas se basan en supuestos de dureza computacional que un ordenador cuántico podría invalidar. La migración de estos protocolos a variantes post-cuánticas no es trivial: implica sacrificios significativos en rendimiento y requiere un rediseño de los protocolos de agregación segura.
- **Shadow AI y la deuda criptográfica invisible.** IBM[21] ha documentado un incremento del 1.500% en instancias de *shadow AI* (modelos desplegados sin supervisión del equipo de seguridad) entre 2023 y 2025, con un coste incremental estimado de 670.000 dólares por brecha que involucra IA no autorizada. Estos modelos desplegados en entornos cloud sin gobernanza criptográfica representan una deuda cuántica invisible: algoritmos vulnerables protegiendo activos de alto valor que nadie ha inventariado.

IoT: mil millones de dispositivos que no pueden actualizarse

Si la IA representa el activo invisible en el inventario criptográfico, el IoT representa el activo inmovilizado. Con una estimación de más de 27.000 millones[22] de dispositivos activos y creciendo, el Internet de las Cosas plantea el desafío más estructural de la transición post-cuántica: una masa crítica de dispositivos desplegados con criptografía de clave pública integrada en hardware o firmware que, en muchos casos, no admite actualización remota.

El desafío de los recursos limitados

Los algoritmos PQC estandarizados por el NIST (ML-KEM, ML-DSA, SLH-DSA) generan claves y firmas significativamente más grandes que sus predecesores clásicos y requieren más capacidad de cómputo. Para dispositivos IoT diseñados con restricciones severas de memoria, energía y ancho de banda, este incremento no es un inconveniente menor; puede ser un factor bloqueante. Un sensor industrial con 32 KB de RAM y comunicación LoRaWAN no puede, simplemente, ejecutar ML-KEM-1024.

Investigaciones recientes ofrecen señales esperanzadoras: estudios publicados en 2026 demuestran que la autenticación PQC basada en TLS 1.3 con ML-KEM y ML-DSA alcanza latencias comparables a las del TLS convencional en dispositivos de tipo gateway (como Raspberry Pi 4), identificando el tamaño del certificado como la principal sobrecarga. Pero la viabilidad en gateways no resuelve el problema en la capa de nodo: los dispositivos de campo con microcontroladores de gama baja siguen siendo un punto ciego. La propuesta de ofrecer "cifrado como servicio" desde el gateway para los nodos en proximidad no mejora la seguridad de la comunicación *nodo-a-gateway* si el propio nodo no es capaz de realizar intercambio de claves post-cuántico.

---

[21] IBM – Cost of a Data Breach Report 2025. https://www.ibm.com/reports/data-breach

[22] Statista. (2026). Number of Internet of Things (IoT) connections worldwide from 2022 to 2034. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

La escala del problema

El inventario de IoT plantea tres preguntas incómodas:

- La primera es **cuántos dispositivos desplegados tienen criptografía asimétrica integrada en hardware que no admite actualización**. En muchos sectores (sanidad, energía, transporte, ciudades inteligentes, etc.) la respuesta es la mayoría, y los ciclos de reemplazo se miden en décadas, no en años.
- La segunda es **quién es responsable de la actualización**. En el modelo de responsabilidad compartida del IoT, la frontera entre fabricante, integrador y operador suele ser difusa. Un dispositivo IoT desplegado en 2020 con firmware cifrado mediante ECDSA tiene una deuda de seguridad que alguien tendrá que asumir, y las garantías del fabricante probablemente no cubran la migración PQC.
- La tercera es **cómo priorizar**. No todos los dispositivos IoT tienen el mismo perfil de riesgo cuántico. Un sensor de temperatura ambiental tiene una exposición diferente a un monitor cardíaco conectado o un contador inteligente de la red eléctrica. La priorización debe basarse en la sensibilidad de los datos transmitidos, la vida útil residual del dispositivo y la criticidad del sistema al que está conectado.

La estrategia pragmática

El enfoque más realista para IoT pasa por aceptar que habrá una larga coexistencia entre dispositivos con criptografía clásica y dispositivos *PQC-ready*. Las recomendaciones prácticas incluyen exigir compatibilidad PQC en todas las nuevas adquisiciones de dispositivos IoT a partir de ahora, implementar segmentación de red que aísle los dispositivos heredados no actualizables, utilizar *gateways PQC-capable* como punto de terminación criptográfica para los nodos que no puedan actualizarse, e incorporar requisitos de cripto-agilidad y soporte PQC en los contratos con fabricantes e integradores.

Tecnología Operacional: donde la criptografía rota puede causar daño físico

La tecnología operacional (OT) (sistemas SCADA, PLCs, DCS, etc.) ocupa una posición singular en el panorama de riesgos post-cuánticos. A diferencia del entorno IT, donde una vulnerabilidad criptográfica compromete fundamentalmente la confidencialidad, en OT la criptografía rota puede provocar consecuencias físicas: interrupción de procesos industriales, daños medioambientales, destrucción de equipamiento o, en el peor escenario, riesgo para vidas humanas.

Trust Now, Forge Later: el gemelo olvidado de HNDL

La comunidad de seguridad ha centrado su atención en el riesgo *harvest now, decrypt later* para datos confidenciales. Pero en OT, el riesgo más inmediato y potencialmente devastador es lo que la industria está denominando *Trust Now, Forge Later (TNFL)*: las firmas digitales y los certificados que hoy se consideran fiables podrían ser falsificados mañana, permitiendo el despliegue transparente de firmware malicioso, la suplantación de estaciones de ingeniería autorizadas y la manipulación de cadenas de suministro de software industrial.

A diferencia de la exfiltración progresiva de datos (que puede detectarse y contenerse), un ataque TNFL provoca un colapso inmediato de la confianza y la integridad, con impactos masivos en entornos industriales. Si un atacante puede falsificar la firma de una actualización de firmware de un PLC, puede cargar lógica maliciosa que modifique los parámetros de un proceso químico, desactive un sistema instrumentado de seguridad o provoque una sobrecarga controlada en la red eléctrica.

Los casos de uso criptográfico en OT que están en riesgo

Los entornos OT utilizan criptografía de clave pública en contextos que a menudo pasan desapercibidos en las evaluaciones de riesgo convencionales: autenticación de estaciones de ingeniería y HMIs contra controladores, firma y verificación de firmware y actualizaciones de software industrial, certificados de dispositivos para comunicaciones seguras (OPC UA, MQTT con TLS, DNP3-SA), acceso remoto seguro a través de VPNs industriales, y comunicaciones entre centros de control y subestaciones (IEC 62351)[23]. Cada uno de estos casos de uso representa un punto de entrada potencial para un adversario con capacidad cuántica.

El factor tiempo: ciclos de vida de 20-30 años

El desafío fundamental de OT es temporal. Los activos industriales se diseñan para ciclos de vida de 20 a 30 años. Un sistema de control desplegado hoy estará operativo en 2050, bien dentro de la ventana en la que se espera la llegada de un CRQC. Esto significa que las decisiones de adquisición y diseño que se tomen ahora determinan la exposición cuántica de la próxima generación de infraestructura industrial.

Las ventanas de mantenimiento en OT son escasas y costosas. A diferencia de un servidor IT que puede parchearse en cualquier ventana de mantenimiento, una planta petroquímica o una subestación eléctrica tiene paradas programadas con meses de antelación. Coordinar la migración PQC con estos ciclos de mantenimiento requiere una planificación plurianual que debería empezar ya.

La hoja de ruta para OT

La orientación predominante es adoptar un enfoque híbrido como paso intermedio: implementar criptografía PQC junto con algoritmos clásicos, de manera que la seguridad se mantenga a menos que ambos sean comprometidos simultáneamente. La CNSA 2.0 de la NSA anima explícitamente a empezar a hacer firma dual (clásica + PQC) de firmware de forma inmediata. Varios fabricantes de software industrial ya están realizando firma dual con RSA y ML-DSA desde 2023, anticipando la futura validación de la firma PQC cuando los estándares se estabilicen.

La cripto-agilidad en OT no es un concepto abstracto; se traduce en decisiones de diseño concretas: utilizar capas de abstracción como interfaces PKCS#11 en lugar de algoritmos codificados en duro, permitir que los dispositivos acepten múltiples opciones de algoritmos, y diseñar procesos de actualización de firmware que soporten el tránsito entre suites criptográficas sin interrupción del servicio.

[23] IEC 62351 – Power systems security.

Cloud: la migración PQC más grande está ocurriendo debajo de tus pies

De los cuatro dominios analizados, el cloud es paradójicamente el que presenta la transición más avanzada y el que genera la falsa sensación de seguridad más peligrosa. Los grandes proveedores de servicios cloud (CSPs) están desplegando activamente y publicitan soporte PQC. Lo que puede llevar a pensar que el cloud ya está cubierto, aunque dista mucho de la realidad.

Lo que los CSPs están haciendo

El progreso es real y significativo. AWS ha completado la evaluación de sus sistemas y está desplegando ML-KEM para intercambio de claves híbrido post-cuántico en endpoints de servicio públicos. Servicios como Elastic Load Balancer, CloudFront y Transfer Family ya ofrecen políticas TLS con soporte PQC. Google protege sus comunicaciones internas con PQC desde 2022, y en la actualidad, más de la mitad del tráfico web generado por humanos a través de Cloudflare utilizaba intercambio de claves post-cuántico. Azure y Google Cloud KMS ya soportan ML-KEM para proteger datos contra ataques HNDL.

Lo que queda del lado del cliente

Aquí es donde el modelo de responsabilidad compartida se convierte en una fuente de riesgo cuántico. Lo que los CSPs están proporcionando es, principalmente, protección PQC para el intercambio de claves en tránsito, la capa más urgente por el riesgo HNDL. Pero la migración completa tiene múltiples dimensiones que permanecen del lado del cliente:

- **Actualización de clientes y SDKs.** AWS lo dice explícitamente: la responsabilidad del cliente es actualizar los navegadores web y los clientes que se comunican con los endpoints de servicio. Una organización que utiliza versiones antiguas de SDKs, bibliotecas TLS desactualizadas o clientes propietarios sin soporte ML-KEM no se beneficia de la protección PQC del proveedor, aunque el endpoint la ofrezca.
- **PKI interna y certificados.** Si la organización opera su propia autoridad de certificación para servicios internos desplegados en cloud, la migración de la cadena de confianza completa es responsabilidad del cliente. Y esta migración está bloqueada por un cuello de botella técnico: a fecha de hoy, la IETF aún no ha finalizado el estándar para certificados híbridos, aunque se espera que lo haga a principios de 2026. Esto significa que los primeros certificados post-cuánticos públicos no estarán ampliamente disponibles ni serán de confianza universal para todos los navegadores antes de 2027.
- **HSMs y gestión de claves.** No todos los módulos de seguridad hardware (HSMs) soportan actualmente los algoritmos PQC. Los fabricantes de HSMs están apuntando a 2025-2026 para la integración de algoritmos aprobados por el NIST en elementos seguros, pero la sustitución o actualización de HSMs en producción es un proceso que implica contratación, instalación y recertificación, y que domina la línea temporal de la migración en sectores como banca, defensa y control industrial.
- **Elementos con criptografía propia.** Cualquier aplicación desplegada en cloud que utilice implementaciones criptográficas propias (bibliotecas embebidas, protocolos personalizados, cifrado de bases de datos) queda fuera del alcance de la migración del CSP. Según el informe *State of Post-quantum Cryptography Readiness 2025* del Trusted Computing Group[24], el 81 % de las organizaciones encuestadas considera que sus bibliotecas criptográficas y HSMs no están preparados para la integración de criptografía post cuántica, lo que introduce una deuda criptográfica significativa difícil de abordar sin inventarios y planes de migración específicos.

La amenaza multinivel en cloud

Estudios recientes examinan cómo las amenazas cuánticas afectan cada capa de la pila cloud de forma diferente. La capa de red es vulnerable a la interceptación de datos en tránsito (HNDL clásico). La capa de datos (bases de datos gestionadas, almacenamiento de objetos, analytics) es vulnerable a la desprotección de datos almacenados si las claves de cifrado fueron negociadas con algoritmos vulnerables. La capa de runtime (serverless, contenedores) puede exponer datos en memoria si los entornos de ejecución se ven comprometidos a través de certificados falsificados. Y la capa de identidad y acceso, que depende de certificados X.509 y tokens firmados con RSA o ECDSA, es vulnerable a la suplantación completa de identidades.

Actividades a llevar a cabo con los servicios cloud

La **primera acción** es dejar de tratar la migración PQC del CSP como si cubriera todo el stack. Solicitar a cada proveedor cloud su hoja de ruta PQC documentada, con plazos concretos para cada servicio y una delimitación clara de responsabilidades. AWS ha sido particularmente transparente en este aspecto, pero la transparencia no equivale a cobertura completa.

La **segunda** es inventariar los elementos propios que utilizan criptografía asimétrica fuera del perímetro del CSP: bibliotecas TLS en contenedores, certificados emitidos por CAs internas, conexiones VPN entre cloud y on-premises, y cualquier cifrado de datos en reposo que utilice claves negociadas con algoritmos vulnerables.

La **tercera** es empezar a activar las funcionalidades PQC que los CSPs ya ofrecen. Si AWS CloudFront soporta PQC en conexiones cliente-a-edge por defecto, verificar que los clientes que se conectan a esas distribuciones estén utilizando navegadores o SDKs compatibles. Si Google Cloud KMS soporta ML-KEM, evaluar su uso para las cargas de trabajo con datos de larga vida.

---

[24] Trusted Computing Group. (2025). State of post-quantum cryptography readiness 2025. https://trustedcomputinggroup.org/wp-content/uploads/State-of-PQC-Readiness-2025-November-2025.pdf

La convergencia de riesgos: cuando los dominios se cruzan

Los cuatro dominios analizados no existen en silos. Las organizaciones reales operan modelos de IA desplegados en cloud que procesan datos de dispositivos IoT conectados a sistemas OT. Cada intersección crea superficies de riesgo cuántico compuestas que son más que la suma de sus partes.

Un sistema de mantenimiento predictivo en una planta industrial, por ejemplo, combina sensores IoT (que transmiten datos cifrados con ECDSA), una plataforma cloud (que almacena y procesa esos datos), un modelo de IA (entrenado con años de datos operativos) y una integración con el sistema SCADA (que recibe las recomendaciones del modelo). Un adversario que capture los datos de telemetría cifrados hoy y los descifre mañana obtiene no solo la información operativa de la planta, sino la capacidad de alimentar su propio modelo adversarial con datos reales de entrenamiento. Y si puede falsificar la firma del modelo o de las actualizaciones que el modelo envía al SCADA, puede manipular decisiones operativas con consecuencias físicas.

Priorización basada en impacto, no en dominio

La tentación natural es abordar la migración PQC por dominio tecnológico: primero IT, luego cloud, después IoT, finalmente OT. Pero la priorización más efectiva se basa en el impacto y la exposición temporal, no en la taxonomía tecnológica. El marco de trabajo recomendado articula tres dimensiones:

La primera es la sensibilidad temporal de los datos. Los datos que deben mantener su confidencialidad más allá de 2030-2035, el horizonte estimado para un CRQC, tienen una exposición HNDL real hoy. Esto prioriza datos sanitarios, propiedad intelectual, transacciones con tarjetas de crédito, secretos comerciales y datos gubernamentales clasificados, independientemente de si residen en un servidor on-premises, un bucket S3 o la memoria de un PLC.

La segunda es la criticidad de la cadena de confianza. Los sistemas donde la falsificación de una firma digital tiene consecuencias catastróficas (firmware de sistemas de control industrial, actualizaciones de dispositivos médicos, certificados de infraestructura PKI raíz) deben priorizarse para la protección TNFL, incluso si el riesgo de confidencialidad es menor.

La tercera es la inercia de migración. Los sistemas con ciclos de reemplazo largos y capacidad de actualización limitada (IoT de campo, OT heredado, HSMs en producción) necesitan empezar antes precisamente porque tardarán más. Esperar a que los estándares maduren para iniciar la migración de estos sistemas es una decisión que se pagará con migraciones precipitadas y costosas cuando los plazos regulatorios aprieten.

El mensaje para el consejo de administración

Si hay una idea que debe salir de esta sección para llegar a la mesa del comité de dirección, es esta: la amenaza cuántica no es un problema de cifrado; es un problema de confianza digital. Afecta a la capacidad de la organización para garantizar que sus modelos de IA no han sido comprometidos, que los datos de sus dispositivos IoT son auténticos, que los comandos que reciben sus sistemas industriales son legítimos y que su infraestructura cloud opera bajo una cadena de confianza íntegra.

Los plazos no son lejanos. Los reguladores europeos esperan que las estrategias nacionales de transición estén iniciadas antes de finales de 2026. Las nuevas adquisiciones de sistemas de seguridad nacional estadounidenses deben ser compatibles con CNSA 2.0 desde enero de 2027. Las infraestructuras críticas europeas deben haber completado la transición PQC para 2030. Y los ciclos de migración para sistemas complejos, que es lo que se describe en esta sección, se miden en años, no en meses.

La ventana para actuar de forma ordenada, planificada y con ventaja competitiva está abierta. Pero se está cerrando.

3.7. Modelos de scoring y priorización de riesgos PQC

La sección anterior identificó superficies de riesgo cuántico[25] en IA, IoT, OT y cloud. Pero saber que todo está expuesto no es lo mismo que saber por dónde empezar[26]. Un CISO con presupuesto finito, equipos limitados y docenas de sistemas en su inventario criptográfico necesita algo que la retórica de la urgencia no proporciona: un mecanismo de priorización que sea defendible ante el comité de dirección, comprensible para los equipos técnicos y auditable para los reguladores.

Esta sección presenta los modelos de scoring y priorizaciones más relevantes para la gestión del riesgo cuántico, desde los fundamentos teóricos hasta las herramientas de aplicación práctica. No se trata de adoptar uno y descartar los demás; se trata de entender qué pregunta responde cada modelo y cómo combinarlos en un marco de decisión coherente.

---

[25] National Cyber Security Centre. (2024). Timelines for migration to post-quantum cryptography. Government of the United Kingdom. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[26] Global Risk Institute. (2025). Quantum threat timeline 2025: Executive perspectives on barriers to action. https://globalriskinstitute.org/publication/quantum-threat-timeline-2025-executive-perspectives-on-barriers-to-action/

Teorema de la desigualdad de Mosca: el punto de partida

Cualquier conversación sobre priorización de riesgos PQC debe partir del teorema de la desigualdad de Mosca, formulado por el Dr. Michele Mosca en 2018 y ya introducido en el apartado 2.1. Su elegancia reside en su simplicidad: si X + Y > Z, la organización ya va tarde.

Donde:

X = el tiempo que los datos deben permanecer confidenciales (la vida útil de seguridad requerida)

Y = el tiempo necesario para migrar los sistemas criptográficos a soluciones quantum-safe

Z = el tiempo restante hasta que exista un CRQC

Si la suma del tiempo de protección requerido y el tiempo de migración supera el plazo hasta la llegada del CRQC, la organización tiene una ventana de exposición que ninguna acción futura puede cerrar retroactivamente. Los datos capturados hoy bajo una estrategia HNDL serán descifrables antes de que la migración se complete.

Fortalezas y limitaciones operativas

El teorema de la desigualdad de Mosca es extraordinariamente útil como herramienta de comunicación ejecutiva. Permite traducir una amenaza abstracta en una ecuación que cualquier miembro del consejo puede entender: nuestros datos sanitarios necesitan 15 años de protección (X=15), nuestra migración llevará 4 años (Y=4), y las estimaciones sitúan el CRQC en 10-15 años (Z=10-15). X+Y=19 > Z. Por tanto, parece que ya vamos tarde.

Sin embargo, como herramienta de priorización operativa, Mosca tiene limitaciones reconocidas. Es binaria (riesgo o no riesgo, sin gradación), unidimensional (solo considera la dimensión temporal, no el impacto ni la exposición), y trata Z como una variable única cuando en realidad cada organización tiene múltiples valores de X e Y distribuidos entre decenas o cientos de sistemas. Para pasar de “es necesario actuar” a “es actuar aquí primero”, se necesitan modelos más granulares.

QARS: la evolución multidimensional

El modelo *Quantum-Adjusted Risk Score* (QARS), publicado en 2025 dentro del marco PAREK de la UE (*Post-quantum asset and algorithm inventory, risk Assessment, Road mapping, Execution, Key governance*[27]), representa la evolución natural de Mosca. QARS transforma la desigualdad binaria en una puntuación continua y ponderada que integra tres dimensiones:

- **Línea temporal (Timeline):** cuantifica la urgencia basándose en la relación entre la vida útil de seguridad de los datos, el tiempo de migración estimado y el horizonte CRQC. Es la dimensión Mosca refinada con funciones de escalado continuo en lugar de un umbral binario.
- **Sensibilidad (Sensitivity):** evalúa el impacto de un compromiso: clasificación del dato, requisitos regulatorios, consecuencias financieras, reputacionales u operativas de la exposición, etc.
- **Exposición (Exposure):** mide la accesibilidad del activo para un adversario: si los datos transitan por redes públicas, si el sistema está expuesto a internet, si existen controles compensatorios que dificultan la captura, etc.

Cada dimensión se calibra mediante pesos ajustables por sector, lo que permite que una entidad financiera pondere la sensibilidad regulatoria de forma diferente a un operador de infraestructura energética. El resultado es un valor numérico que alimenta directamente la cola de priorización de la migración: los activos con mayor QARS se migran primero.

Lo que hace a QARS particularmente valioso es su alineamiento directo con la hoja de ruta coordinada de la UE. El modelo proporciona los valores numéricos de probabilidad e impacto que pueden integrarse en registros de riesgo basados en FAIR o NIST SP 800-30[28], asegurando que el riesgo cuántico se evalúe junto con las amenazas clásicas en lugar de quedar aislado en un silo.

---

[27] El PAREK Framework (EU Post-quantum Cryptography Transition Handbook). https://www.pqc.lt

[22] Grigaliūnas, Š., & Brūzgienė, R. (2025). Towards a unified quantum risk assessment: A quantum adjusted risk score (QARS) model within the EU PAREK framework. Electronics, 14(17), 3338. https://doi.org/10.3390/electronics14173338

CARAF: el factor de agilidad organizativa

El *Crypto-Agility Risk Assessment Framework (CARAF)* complementa a QARS incorporando una dimensión que los modelos puramente técnicos omiten: la capacidad organizativa de cambio. CARAF multiplica un factor temporal (similar al teorema de disponibilidad de Mosca) por un factor de impacto-coste que pone el acento en la agilidad criptográfica real de la organización.

En la práctica, CARAF responde a una pregunta diferente: no **¿cuánto riesgo tiene este activo?** sino **¿cuánto nos costará y cuánto tardaremos en mitigar este riesgo?**

Un sistema con riesgo QARS alto, pero con una arquitectura cripto-ágil (capas de abstracción, algoritmos configurables, HSMs actualizables) puede tener un coste de migración bajo y, por tanto, puede programarse con menos urgencia que un sistema con riesgo QARS medio, pero con criptografía fija y dependencias de proveedores sin hoja de ruta PQC.

Para un CISO, la combinación QARS + CARAF produce la matriz de decisión más completa: QARS dice qué migrar primero y CARAF dice qué será más difícil y costoso migrar. La intersección de riesgo y dificultad altos identifica los puntos donde la organización necesita empezar inmediatamente, precisamente porque son los que más tiempo requerirán.

Matriz de decisión QARS + CARAF para priorizar PQC

El marco ISACA Risk IT aplicado al riesgo cuántico

ISACA ha publicado en 2025 una guía práctica que adapta su *Risk IT Framework*[29] a la evaluación de riesgos cuánticos, utilizando como caso de estudio una entidad financiera ficticia (MetroBank). Lo que hace esta adaptación especialmente útil es que encaja la evaluación cuántica dentro de marcos de gobernanza de riesgos que la mayoría de organizaciones ya tienen desplegados, evitando la necesidad de crear una estructura paralela.

El proceso se estructura en cuatro fases: gobernanza del riesgo (establecer el apetito de riesgo cuántico y la estructura de gobierno), evaluación (inventario criptográfico, clasificación de datos y priorización usando la desigualdad de Mosca), respuesta (plan de migración por fases con pilotos de cifrado híbrido) y monitorización (integración de checkpoints PQC en gestión del cambio, respuesta a incidentes y selección de proveedores).

Un aspecto particularmente práctico es la propuesta de calcular una pérdida anual esperada (ALE) específica para el riesgo cuántico por categoría de datos. Por ejemplo, para datos hipotecarios con una retención de 15 años (X=15) y un tiempo de migración estimado de 18 meses para sistemas legacy (Y=1,5), el marco permite cuantificar la exposición financiera y compararla con el coste de la migración, produciendo un argumento de inversión que habla el lenguaje del CFO.

Un modelo de scoring integrado: propuesta práctica

Ninguno de los marcos anteriores es completo por sí solo. Por lo que se propone un modelo de scoring integrado que combine sus fortalezas en un flujo de trabajo operativo:

Paso 1: Inventario y clasificación (CBOM + Mosca)

Para cada activo criptográfico del inventario, calcular la desigualdad de Mosca (X+Y vs. Z) utilizando estimaciones conservadoras de Z. Esto produce una primera clasificación binaria: activos que ya están en zona de riesgo y activos que tienen margen. Es el filtro rápido que separa lo urgente de lo planificable.

Paso 2: Scoring multidimensional (QARS)

Para los activos en zona de riesgo, aplicar el scoring QARS con pesos calibrados al sector de la organización. Esto produce una lista ordenada por puntuación numérica. Los activos con QARS más alto van al frente de la cola de migración.

[23] Carmichael, M. (2025, May 19). How to conduct a quantum risk assessment using ISACA's Risk IT Framework. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-10/how-to-conduct-a-quantum-risk-assessment-using-isacas-risk-it-framework

Paso 3: Evaluación de viabilidad (CARAF)

Para los activos priorizados por QARS, evaluar la dificultad y el coste de migración mediante CARAF. Esto permite identificar los activos que, pese a tener un QARS alto, pueden migrarse rápidamente (los quick wins que generan tracción en el programa) frente a los que requerirán proyectos plurianuales (los que justifican la asignación de presupuesto estratégico).

Paso 4: Integración en el registro de riesgos corporativo

Los valores QARS y CARAF se traducen a los formatos del registro de riesgos existente (FAIR, NIST 800-30, ISO 27005 o el que utilice la organización). El riesgo cuántico debe vivir junto al ransomware, la exfiltración de datos y el riesgo de terceros; no en un documento separado que nadie revisa.

Paso 5: Revisión y recalibración periódica

El valor de Z no es estático. Cada avance significativo en computación cuántica debe desencadenar una recalibración del modelo. Del mismo modo, cada migración completada reduce el valor de Y para ese activo y mejora su posición en el scoring.

Lo que no debería hacer un modelo de scoring

Tan importante como definir qué mide el modelo es establecer qué no debería hacer:

- **No debería pretender predecir cuándo llegará el CRQC**. Ningún modelo puede hacerlo con precisión, y cualquier intento de puntuar riesgos sobre una falsa certeza temporal es contraproducente. Lo que sí puede hacer es evaluar la exposición bajo diferentes escenarios (Por ejemplo, CRQC en 2030, 2035, 2040, etc.) y mostrar a la dirección cómo cambian las prioridades bajo cada supuesto.
- **No debería tratar todos los algoritmos como igualmente vulnerables.** AES-256 permanece seguro en el escenario cuántico (con una reducción de la longitud efectiva de clave, mitigable duplicando el tamaño); RSA-2048 no. El scoring debe distinguir entre activos que usan criptografía simétrica (riesgo bajo) y los que dependen de criptografía asimétrica (riesgo alto).
- **Y no debería convertirse en un ejercicio anual que viva en una hoja de cálculo.** Un modelo de scoring útil es uno que se actualiza con cada cambio en el inventario criptográfico, cada nueva adquisición de software, cada renovación de contrato con un proveedor cloud. La automatización del descubrimiento criptográfico y la integración con herramientas ACDI (Automated Cryptography Discovery and Inventory) es lo que convierte un modelo teórico en una capacidad operativa.

El resultado: un listado priorizado de migración defendible

El objetivo final de todo este ejercicio no es producir un informe bonito. Es producir un listado priorizado de migración que pueda responder a tres preguntas que todo equipo de seguridad enfrentará:

Cuando el auditor pregunte ¿cómo han priorizado su transición PQC?, la respuesta es un modelo documentado con criterios explícitos, pesos justificados y resultados trazables.

Cuando el equipo financiero pregunte ¿por qué necesitamos este presupuesto ahora y no el año que viene?, la respuesta es una cuantificación de la exposición financiera bajo el teorema de la desigualdad de Mosca, respaldada por los plazos regulatorios de la hoja de ruta europea y CNSA 2.0.

Cuando el director de tecnología pregunte ¿por dónde empezamos?, la respuesta es una lista ordenada de activos con su puntuación QARS, su estimación de esfuerzo CARAF y su alineamiento con las ventanas de mantenimiento y los ciclos de renovación contractual.

Esa es la diferencia entre gestionar el riesgo cuántico y simplemente preocuparse por él.

4. Identificación y Clasificación de Activos Críticos

4.1. Metodología *CBOM*

La metodología CBOM (Cryptography Bill of Materials) constituye el estándar de referencia para estructurar y visibilizar los activos criptográficos de una organización. Como evolución natural del SBOM (Software Bill of Materials), este marco metodológico surge ante la necesidad de abandonar los inventarios manuales y estáticos, ofreciendo un formato normalizado, dinámico e interpretable por máquinas para catalogar qué criptografía se utiliza, dónde reside y cómo se implementa en el entorno corporativo[30].

El estándar CBOM no se limita a listar certificados, sino que documenta de forma exhaustiva las dependencias criptográficas en todos los niveles de la arquitectura tecnológica. Para que un CBOM se considere completo y funcional de cara a una transición post-cuántica, la metodología exige que registre, como mínimo, los siguientes atributos:

- **Primitivas y algoritmos:** identificación exacta del algoritmo utilizado (por ejemplo, RSA, ECC, AES) y su propósito (firma digital, cifrado de datos, intercambio de claves).
- **Parámetros criptográficos:** tamaños de clave, curvas elípticas específicas y modos de operación empleados.
- **Bibliotecas y dependencias:** proveedor y versión de la biblioteca de software que ejecuta la criptografía (por ejemplo, OpenSSL, BouncyCastle, etc.), vital para identificar vulnerabilidades en la cadena de suministro.
- **Contexto de uso y ubicación:** protocolos de red asociados (TLS, SSH, IPsec) y el activo físico o lógico donde se ejecuta (servidores web, aplicaciones cloud, dispositivos IoT, o terminales físicos, etc.).

La implementación práctica de esta metodología en infraestructuras heterogéneas requiere un enfoque estructurado. Para ello, el modelo CBOM se apoya en tres fases fundamentales:

1. **Descubrimiento Automatizado (ACDI[31]):** dado el volumen de activos en una corporación, la metodología requiere el uso de herramientas de Descubrimiento e Inventario de Criptografía Automatizado (ACDI, por sus siglas en inglés). Estas soluciones escanean activamente redes, repositorios de código y sistemas en producción (desde servidores centrales hasta redes OT) para extraer la información criptográfica sin depender del factor humano.
2. **Normalización y Formateo:** los datos descubiertos se compilan utilizando estándares de la industria (como extensiones de CycloneDX[32] o SPDX[33]). Esto asegura que el inventario sea interoperable y pueda ser consumido por otras herramientas de seguridad (SIEM, plataformas de gestión de vulnerabilidades).
3. **Gestión de Postura y Ciclo de Vida:** el CBOM deja de ser una foto fija para convertirse en un cuadro de mando vivo. Permite a la dirección de ciberseguridad aplicar modelos de "scoring" de riesgo, identificando de un vistazo qué sistemas críticos utilizan criptografía clásica vulnerable y planificando su migración o aislamiento de forma priorizada.

En definitiva, la adopción de este marco metodológico proporciona una radiografía exacta y en tiempo real de la postura criptográfica, facilitando la identificación inmediata de componentes vulnerables a la amenaza cuántica. El CBOM se erige, así como el cimiento técnico ineludible sobre el cual se debe construir cualquier estrategia de cripto-agilidad.

4.2. Clasificación de datos por horizonte de confidencialidad

El riesgo cuántico no afecta por igual a todos los datos de una organización. La variable determinante no es solo la sensibilidad del dato en el momento presente, sino cuánto tiempo debe seguir manteniéndose la confidencialidad de ese dato en el futuro. Esta dimensión temporal es lo que se denomina horizonte de confidencialidad.

El concepto está directamente ligado a la citada amenaza Harvest Now, Decrypt Later (HNDL). Dado que los datos sensibles retienen su valor durante muchos años, iniciar ahora la transición a la criptografía post-cuántica se hace imprescindible para evitar brechas de seguridad en el futuro.

La clasificación por horizonte de confidencialidad debe ser tratada como en una herramienta de priorización de la migración, no simplemente en un ejercicio taxonómico.

Se han definido cinco niveles de clasificación, ajustables por cada organización en función de su sector, su marco regulatorio y su apetito de riesgo. El criterio rector de la escala es el horizonte temporal de confidencialidad, es decir, cuánto tiempo debe permanecer protegido un dato y no únicamente cuán sensible es en el presente.

---

[30] OWASP CycloneDX Project. (2024). Cryptography Bill of Materials (CBOM). https://cyclonedx.org/capabilities/cbom/

[31] Cybersecurity and Infrastructure Security Agency (CISA). (2026). Strategy for migrating to automated post-quantum cryptography discovery and inventory tools. https://www.cisa.gov/resources-tools/resources/strategy-migrating-automated-post-quantum-cryptography-discovery-and-inventory-tools

[32] OWASP CycloneDX Project. (2024). CycloneDX: Software Bill of Materials standard. https://cyclonedx.org/

[33] Linux Foundation. (2024). SPDX specification: Software Package Data Exchange. https://spdx.dev/

A continuación, se describen los 5 niveles principales por horizonte temporal:

- **Nivel 1.** Comprende datos cuyo valor informativo expira en menos de dos años. El riesgo de compromiso retroactivo es bajo, pero estos activos deben estar presentes en el inventario criptográfico para garantizar la trazabilidad completa del ciclo de vida.
- **Nivel 2.** Agrupa datos con horizontes de dos a cinco años. La criptografía actual puede ser suficiente a corto plazo, pero estos activos deben incorporarse a la hoja de ruta de migración y gestionarse bajo criterios de agilidad criptográfica, reduciendo progresivamente los ciclos de vida de los mecanismos de protección.
- **Nivel 3.** marca el umbral a partir del cual la ventana de confidencialidad se solapa con los escenarios de madurez de la computación cuántica. Los datos con horizontes de entre cinco y quince años deben considerarse en riesgo activo y requieren la adopción de mecanismos de protección híbridos como medida transitoria prioritaria.
- **Nivel 4.** recoge activos cuya confidencialidad debe sostenerse entre quince y treinta años. Para estos datos, la migración a criptografía post-cuántica no admite demora y debe planificarse con carácter inmediato.
- **Nivel 5.** corresponde a activos con horizonte de confidencialidad indefinido o superior a treinta años. Representan el mayor riesgo frente a ataques y exigen los controles más robustos disponibles, incluyendo el despliegue de criptografía post-cuántica en su forma más madura y el aislamiento reforzado de los sistemas que los custodian.

Independientemente del nivel asignado, todos los activos deben figurar en el inventario criptográfico de la organización. Los de niveles inferiores permiten una migración gradual; los de niveles superiores determinan la secuencia y la urgencia del plan de transición.

Esta clasificación es la entrada natural al proceso de creación del *Cryptography Bill of Materials (CBOM)*. Cada activo del inventario criptográfico debe anotarse con su nivel de horizonte de confidencialidad.

Nivel	Horizonte	Tipo de datos	Tipología de datos	Sectores representativos	Riesgo cuántico	Prioridad Migración	Control criptográfico recomendado
Nivel 1 Corta duración	**< 2 años**	Datos efímeros	Tokens de sesión, datos de telemetría transitorios, caché temporal cifrado, logs operativos de corto ciclo	Aplicaciones web, IoT no crítico, analytics operacional	Bajo	Baja	Criptografía clásica actual suficiente a corto plazo. Incluir en inventario CBOM para futuras rotaciones.
Nivel 2 Duración Media	**2 – 7 años**	Datos operacionales	Datos de clientes y contratos activos, comunicaciones corporativas sensibles, credenciales de autenticación de larga vida, registros de RRHH	Retail, telecomunicaciones, servicios cloud, RRHH	Moderado	Media-Baja	Evaluar crypto-agility. Incluir en hoja de ruta PQC. Reducir ciclos de vida de certificados (< 90 días).
Nivel 3 Larga duración	**7 – 15 años**	Datos sensibles	Registros financieros y regulatorios, datos fiscales, propiedad intelectual, comunicaciones diplomáticas, logs de auditoría	Banca, seguros, administración pública, farmacéutica	Medio-alto	Alta	PQC híbrido (ML-KEM + RSA/ECC). Inventario CBOM prioritario. Rotar claves TLS/VPN.
Nivel 4 Muy larga duración	**15 – 30 años**	Datos críticos	Historiales clínicos, expedientes judiciales, datos de infraestructuras críticas (OT/SCADA), secretos industriales estratégicos	Sanidad, justicia, energía, agua, transporte crítico	Alto	Muy alta	PQC híbrido inmediato (ML-KEM + ECDH). Migración a PQC puro antes de 2028.
Nivel 5 Crítico	**> 30 años**	Datos estratégicos	Secretos de Estado, claves raíz de PKI nacional, datos biométricos irrevocables	Defensa y seguridad nacional, inteligencia, registros civiles	Crítico	Urgente	PQC puro (ML-KEM + ML-DSA). QKD donde aplique. Aislamiento físico.

Tabla de nivel de horizonte temporal por confidencialidad de los datos

4.3. Cómo preparar un correcto inventario

El inventario criptográfico no es un ejercicio técnico ni un documento puntual, sino la **infraestructura de decisión** sobre la que se apoya todo el programa post-cuántico. Su valor no reside en el volumen de activos listados, sino en su capacidad para permitir decisiones defendibles ante la alta dirección, los auditores y los organismos reguladores.

Un inventario correctamente preparado debe cumplir tres principios clave:

1. Nacer con una finalidad clara

El error más habitual es construir inventarios exhaustivos pero inertes. Desde su concepción, el inventario debe estar orientado a responder preguntas concretas, como:

- ¿Qué activos exponen datos con una vida útil superior al horizonte cuántico?
- ¿Dónde existe dependencia de criptografía no actualizable?
- ¿Qué migraciones condicionan más la hoja de ruta por coste, complejidad o tiempo?

Un inventario en un Excel, confeccionado para cubrir un “check” de una auditoría y que no vuelve a consultarse hasta la auditoría del año próximo es un desperdicio de recursos.

Si el inventario no sirve para priorizar, justificar presupuesto o responder a un auditor, no está cumpliendo su función.

2. Integrar contexto de riesgo, no solo elementos técnicos

Cada activo incluido en el inventario debe ir acompañado, como mínimo, de:

- Contexto de negocio (qué proceso soporta y qué impacto tendría su compromiso).
- Horizonte temporal relevante, en línea con la clasificación definida en el punto 4.2.
- Capacidad de evolución, es decir, si permite cripto agilidad o está anclado a soluciones heredadas, ya que podemos tener certificados compatibles con *quantum-safe*, pero debemos garantizar que se emplean adecuadamente, como el caso de los certificados web hybrid-PQC sobre TLS 1.3, configurando los servidores para no responder a peticiones de handshake inferiores.

Este enfoque convierte el inventario en una herramienta de gestión del riesgo, y no en una mera relación técnica de componentes.

3. Diseñarse como un activo vivo desde el primer día

En el escenario post-cuántico, un inventario estático queda obsoleto en cuestión de meses. Nuevas aplicaciones, renovaciones de certificados, cambios de proveedor o despliegues en la nube modifican de forma continua la superficie criptográfica.

Por ello:

- El inventario debe actualizarse de forma recurrente, idealmente mediante plataformas de gestión del ciclo de vida de certificados (CLM, según sus siglas en inglés) con capacidad de descubrimiento automatizado, como las de IBM, iSara o Keyfactor (ver apartado 12.2 para más información).
- Debe integrarse con procesos existentes (gestión de cambios, adquisiciones, despliegue de software).
- Debe generar evidencias reutilizables para fines de cumplimiento (NIS2, DORA, auditoría interna).

No se puede migrar lo que no se conoce, ni gobernar lo que no es visible.

Preparar correctamente el inventario criptográfico es, en 2026, la acción más rentable y menos especulativa que puede acometer una organización: habilita la priorización, reduce improvisaciones futuras y convierte la amenaza post cuántica en un programa gestionable desde hoy.

4.4. Inventario de algoritmos, llaves y certificados

El inventario de algoritmos, claves y certificados permite conocer con precisión dónde, cómo y con qué mecanismos se protege la información dentro de la organización. En el contexto post-quantum, esta capacidad deja de ser un ejercicio técnico para convertirse en un elemento estructural de la gestión del riesgo, la cripto-agilidad y el cumplimiento normativo.

Introducción y propósito

La transición hacia criptografía resistente a la computación cuántica exige visibilidad completa sobre los activos criptográficos. Sin un inventario preciso, la organización carece de capacidad para:

- Evaluar su exposición real frente a amenazas cuánticas
- Priorizar la migración de algoritmos vulnerables
- Garantizar la eficacia de los mecanismos de protección existentes

Un inventario bien estructurado debe responder a cinco preguntas fundamentales:

1. **Qué existe:** identificación de todos los objetos criptográficos, incluidos los integrados en soluciones de terceros
2. **Dónde se encuentran:** localización en sistemas, aplicaciones, infraestructuras y dispositivos
3. **Si son adecuados:** evaluación de su robustez frente a los requisitos de seguridad actuales y futuros
4. **Si los procesos son confiables:** análisis del ciclo de vida de claves, identidades y controles asociados
5. **Qué priorizar:** base para definir planes de mitigación y transición hacia PQC

Este enfoque está alineado con las recomendaciones del NIST, que destaca la necesidad de visibilidad y gestión centralizada como prerrequisito para la transición post-quantum.

Alcance del inventario criptográfico

El inventario debe cubrir de forma exhaustiva todos los componentes criptográficos, independientemente del entorno o tecnología.

Algoritmos criptográficos

Se deben identificar todos los algoritmos utilizados, incluyendo:

- Cifrado simétrico y asimétrico
- Intercambio de claves
- Firmas digitales
- Funciones hash y modos de operación

Especial atención debe prestarse a algoritmos vulnerables a ataques cuánticos, como RSA, Diffie-Hellman y criptografía de curva elíptica, cuya seguridad se ve comprometida por algoritmos cuánticos como Shor.

Llaves o claves criptográficas

Las claves representan el núcleo operativo de la seguridad criptográfica. El inventario debe incluir:

- Tipo, longitud y algoritmo asociado
- Ubicación (keystores, HSM, cloud, aplicaciones)
- Ciclo de vida completo: generación, distribución, rotación, expiración y destrucción
- Controles de acceso y responsabilidades

Una gestión inadecuada de claves puede invalidar la seguridad del sistema, independientemente del algoritmo utilizado.

Certificados digitales

Los certificados digitales sustentan la confianza en múltiples procesos:

- Autenticación de identidades (usuarios, dispositivos, servicios)
- Establecimiento de canales seguros (TLS, VPN)
- Firma de software, firmware y documentos

El inventario debe incluir:

- Autoridad de certificación emisora
- Algoritmo de firma
- Periodo de validez
- Dependencias con sistemas críticos y terceros

En el contexto post-quantum, estos elementos adquieren especial relevancia debido al riesgo de falsificación futura (Trust Now, Forge Later)

Infraestructuras y dependencias criptográficas

El inventario debe extenderse a los elementos que soportan la criptografía:

- Librerías, frameworks y protocolos (TLS, SSH, APIs)
- Hardware criptográfico (HSM, TPM)
- Dependencias de terceros y servicios cloud
- Sistemas legacy o no actualizables
- Implementaciones en firmware, IoT o sistemas industriales

Este enfoque permite identificar riesgos ocultos derivados de dependencias externas o componentes no gestionados directamente.

Herramientas de descubrimiento

Abordar la creación de un inventario de material criptográfico puede convertirse en un reto significativo, especialmente en organizaciones de gran tamaño o con infraestructuras digitales complejas. Para hacerlo de forma eficaz es imprescindible apoyarse en herramientas de descubrimiento automático, que permitan acelerar el inventariado, mejorar su precisión y reducir riesgos habituales como los falsos positivos, el Shadow IT o los llamados "agujeros negros" criptográficos.

En la siguiente tabla se resumen las posibles fuentes con herramientas automatizadas, algunas posiblemente ya desplegadas, como EDR, y su aportación al inventario criptográfico.

Fuente	¿Qué se descubre?	¿Qué aporta al inventario criptográfico?
Descubrimiento pasivo de red	Protocolos TLS, suites criptográficas, certificados utilizados en comunicaciones	Visibilidad del uso real de la criptografía, detección de sistemas legacy, Shadow IT y entornos sin agente
Descubrimiento en hosts y endpoints	Certificados locales, claves, keystores, librerías criptográficas	Identificación de material criptográfico almacenado o instalado en sistemas y puestos de trabajo
Descubrimiento en aplicaciones y código	Algoritmos, tamaños de clave, librerías criptográficas, claves embebidas	Visibilidad de la criptografía integrada en aplicaciones propias y de terceros
Descubrimiento de certificados y PKI	Certificados TLS/SSL, certificados internos, emisores, caducidades	Control del ciclo de vida de certificados y reducción del riesgo de caídas de servicio
Descubrimiento en cloud y SaaS	Uso de KMS, HSM gestionados, cifrado en servicios cloud	Eliminación de puntos ciegos en entornos cloud e híbridos

Fuentes de descubrimiento automático de activos criptográficos

4.5. Casos de uso sectoriales

Organismos como CISA, NIST y NSA coinciden en que no es posible mitigar el riesgo cuántico sin un inventario exhaustivo de activos criptográficos, que permita entender: qué activos existen, qué datos protegen, cuánto tiempo deben permanecer confidenciales, y qué impacto tendría su compromiso.

Este enfoque es transversal, pero adquiere matices específicos según el sector, como se detalla a continuación.

Sector financiero y bancario

Activos criptográficos críticos que se pueden encontrar típicamente:

- Infraestructuras de pagos (SWIFT, SEPA, RTGS)
- Certificados PKI para autenticación de transacciones
- Firmas digitales de órdenes, contratos y activos digitales
- HSM y gestión de claves en banca electrónica y móvil

Caso de uso: en banca, el inventario criptográfico se utiliza para clasificar sistemas según su "exposición cuántica", priorizando aquellos activos:

- con datos de larga vida (información financiera, identificación de clientes),
- expuestos a redes públicas,
- y con alto impacto sistémico en caso de fallo.

Marcos como el Post-Quantum Financial Infrastructure Framework (PQFIF[34]) y guías de FS-ISAC[35] y Europol[36] recomiendan inventariar primero los casos de uso de criptografía asimétrica que sostienen la integridad y no repudio de transacciones financieras.

Infraestructuras críticas y sector industrial (OT / ICS)

Activos criptográficos críticos que se pueden encontrar típicamente:

- Firmware firmado en PLCs y dispositivos industriales
- Certificados IDevID y LDevID de dispositivos OT
- Canales cifrados entre sistemas SCADA
- Sistemas de autenticación máquina-a-máquina

Caso de uso: en entornos OT, donde los ciclos de vida superan con frecuencia los 15–25 años, la identificación de criptografía embebida es clave para:

- detectar algoritmos no actualizables,
- clasificar activos sin capacidad de crypto-agility,
- y anticipar ventanas de obsolescencia por riesgo cuántico.

La IETF[37] y NIST NCCoE[38] destacan estos activos como prioritarios debido a la imposibilidad práctica de reemplazo rápido una vez desplegados.

---

[34] Corvelo Costa, D. B. (2025). Post-quantum Financial Infrastructure Framework (PQFIF): A roadmap for the quantum-safe transition of global financial infrastructure. Submitted to the U.S. Securities and Exchange Commission (Crypto Assets Task Force). https://www.sec.gov/files/cft-written-input-daniel-bruno-corvelo-costa-090325.pdf

[35] Financial Services Information Sharing and Analysis Center (FS ISAC). (2025). Post-quantum cryptography resources for the financial sector. https://www.fsisac.com/knowledge/pqc

[36] Europol. (2026). Prioritising post-quantum cryptography migration activities in financial services.

https://www.europol.europa.eu/media-press/newsroom/news/joint-report-outlines-practical-approach-to-prioritising-post-quantum-cryptography-migration-in-financial-services

[37] Guidance for migration to Post-quantum Cryptography. https://www.ietf.org/archive/id/draft-kwiatkowski-pquip-pqc-migration-00.html

[38] NIST NCCoE - Migration to Post-quantum Cryptography. https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

Telecomunicaciones y 5G/6G

Activos criptográficos críticos que se pueden encontrar típicamente:

- Gestión de identidades de red (SIM/eSIM, AKA)
- Certificados y claves en roaming internacional
- Infraestructura PKI de operadores
- Señalización cifrada entre nodos de red

Caso de uso: organismos como GSMA han desarrollado bibliotecas de casos de uso PQC que parten explícitamente del inventario criptográfico de red para:

- Mapear dependencias entre sistemas.
- Clasificar activos por criticidad de servicio.
- Evaluar el impacto cuántico sobre disponibilidad, autenticación y confidencialidad.

La identificación de activos criptográficos permite evaluar qué elementos deben migrarse antes del despliegue masivo de 6G, previsto para la próxima década.

Administración pública y defensa

Activos criptográficos críticos que se pueden encontrar típicamente:

- PKI gubernamental y certificados raíz
- Comunicaciones clasificadas
- Documentos firmados con validez legal prolongada
- Sistemas de identidad digital ciudadana

Caso de uso: las agencias gubernamentales utilizan el inventario criptográfico para clasificar activos según la vida útil de la información protegida, priorizando:

- Secretos con valor estratégico a largo plazo.
- Infraestructuras de identidad nacional.
- Cadenas de confianza interinstitucionales.

CISA y NIST recomiendan explícitamente este enfoque como base para la planificación de migraciones antes de 2030 para activos de alta criticidad.

Energía y utilities (electricidad, gas, agua)

Activos criptográficos críticos que se pueden encontrar típicamente:

- IED/RTU/PLC con firmware firmado.
- Certificados IDevID/LDevID en equipos OT.
- Canales SCADA cifrados.
- Pasarelas VPN.
- AMI/medición inteligente.
- PKI de fabricante/operador.

Caso de uso: el inventario revela algoritmos no actualizables (RSA/ECC) y dispositivos sin crypto-agility con ciclos de vida de 15–25 años; se priorizaría migración o estrategias híbridas (clásico+PQC) donde el recambio es difícil. NIST NCCoE documenta arquitecturas y herramientas de descubrimiento criptográfico aplicables a entornos OT; CISA sitúa el inventario como primer paso de *"quantum-readiness"*.

Transporte: aviación y automoción

Activos criptográficos críticos que se pueden encontrar típicamente:

- Aviación: firmware firmado de aviónica, cadenas PKI de aerolínea/airport, comunicaciones de mantenimiento y M2M con larga vida útil.
- Automoción: ECU con firmware OTA firmado, V2X (C-ITS PKI), certificados de fabricación (IDevID), telemática y backend cloud. La IETF cataloga como casos de uso de "aserciones de seguridad de larga duración" el firmware/software firmado y certificados manufactureros, con evaluación de estrategias de migración (incluidas firmas hash-based).

Caso de uso: : inventario para clasificar ECU/aviónica por vida útil y capacidad de actualización, identificando dónde aplicar híbridos o SLH-DSA en cadenas de firma de firmware de larga duración, alineado con FIPS 205.

Salud y biociencia

Activos criptográficos críticos que se pueden encontrar típicamente:

- Historias clínicas cifradas
- Sistemas de firma de resultados médicos
- Dispositivos médicos conectados
- Plataformas de investigación genómica

Caso de uso: en este sector, la clasificación criptográfica se guía por la longevidad del dato sanitario, que puede exceder varias décadas. La identificación temprana de algoritmos vulnerables es esencial para evitar exposiciones futuras de datos altamente sensiblesClasificar activos por criticidad de servicio.

Aseguradoras

Activos criptográficos críticos que se pueden encontrar típicamente:

- Plataformas de suscripción y siniestros.
- PKI para firmas contractuales.
- Intercambio de datos con terceros.
- Portales de cliente.

Caso de uso: similar a banca, con foco en vida útil larga (pólizas, historiales) y alta exposición web/APIs. Inventario para identificar algoritmos vulnerables en autenticación, no repudio y cifrado de datos de clientes, priorizando canales públicos y proveedores clave.

Cloud/SaaS e infra hiperescalar

Activos criptográficos críticos que se pueden encontrar típicamente:

- TLS/QUIC.
- KMS/HSM.
- Tokens e identidades (IdP).
- Cifrado en reposo.
- Code signing en CI/CD.

Caso de uso: CISA propone estrategia de adopción de herramientas automatizadas de descubrimiento e inventario criptográfico (ACDI) para que las agencias (y, por extensión, grandes organizaciones) centralicen inventarios de criptografía vulnerable y reporten progreso. El PQC Inventory Workbook da un modelo práctico de campos y priorización; NIST establece los estándares y tiempos.

Comercio electrónico y retail

Activos criptográficos críticos que se pueden encontrar típicamente:

- Frontales web.
- Gateways de pago.
- MPOS y terminales.
- PKI de tienda.
- Apps móviles; integraciones a terceros.

Caso de uso: inventario para aislar superficies públicas (webs y APIs) y PoS/TPV. Europol los usa como casos de ejemplo para priorizar: primero frontales públicos y PoS por exposición y severidad de impacto.

Legal, identidad y servicios de confianza (eIDAS/PKI corporativa)

Activos criptográficos críticos que se pueden encontrar típicamente:

- Firmas de larga validez (LTV) en documentos y expedientes.
- Timestamps; OCSP/CRL.
- Raíces y sub-CAs.
- Identidades digitales.

Caso de uso: la IETF identifica como críticos los artefactos firmados de larga duración (X.509, firmware/software, certificados manufactureros). Con los FIPS 205 (SLH-DSA) y 204 (ML-DSA) se habilitan estrategias de migración o co-firma para conservar validez décadas. Inventario para clasificar cadenas de confianza y documentación con validez prolongada.

Cadena de suministro de software (DevSecOps)

Activos criptográficos críticos que se pueden encontrar típicamente:

- Code-signing de binarios/containers.
- Firma de paquetes.
- SBOM y, específicamente, CBOM.
- Pipelines CI/CD.
- Repositorios.

Caso de uso: el inventario revela bibliotecas crypto y artefactos firmados con algoritmos vulnerables, para migrar firmas de release y verificación de integridad a PQC. NIST NCCoE publica guías de descubrimiento; la IETF subraya firmware/softwares firmados como casos de larga duración; el CBOM facilita gobernanza continua.primero frontales públicos y PoS por exposición y severidad de impacto.

Educación, I+D y preservación digital

Activos criptográficos críticos que se pueden encontrar típicamente:

- Repositorios de tesis/datasets.
- Propiedad intelectual.
- Evidencias científicas.
- Identidades federadas.

Caso de uso: clasificar por vida útil del conocimiento (larga) y migrar firmas/ sellos con PQC (SLH-DSA) donde la preservación supera décadas.

Smart cities e IoT masivo

Activos criptográficos críticos que se pueden encontrar típicamente:

- PKI de sensores/actuadores.
- Identidades de dispositivo.
- Firmware OTA.
- Pasarelas.
- Plataformas de gestión

Caso de uso: GSMA recoge casos PQC en ecosistemas IoT; la IETF resalta certificados manufactureros y firmware como activos de larga vida. Inventario para segmentar por capacidad de actualización, exposición y densidad de dispositivos, priorizando gateways y dispositivos críticos.

5. Evaluación y Cuantificación del Riesgo Post-Quantum

La evaluación del riesgo post-quantum requiere mecanismos específicos que permitan traducir una amenaza tecnológica de maduración lenta en variables medibles, priorizables y defendibles ante la Alta Dirección, los auditores y los organismos reguladores.

A diferencia de otros riesgos de ciberseguridad, el riesgo cuántico no se materializa de forma abrupta, sino que se acumula de manera progresiva a lo largo del tiempo, condicionado por la vida útil de los datos, los ciclos de migración tecnológica y los hitos regulatorios establecidos por autoridades nacionales e internacionales.

5.1. KPIs y KRIs específicos para riesgos PQC

Según el CyberIndicatorsFramework[39] , un indicador eficaz debe ser exacto, consistente, replicable y basado en datos verificables. En el contexto post-quantum, esto implica definir KPIs orientados al progreso del programa de transición y KRIs orientados a la exposición residual y a la brecha temporal entre riesgo y mitigación.

Distinción entre KPIs y KRIs en el contexto post-quantum

Los KPIs (Key Performance Indicators) miden el avance del programa PQC: inventario, pilotos, migraciones, cobertura de proveedores, etc. Su naturaleza es predominantemente retrospectiva.

Los KRIs (Key Risk Indicators) funcionan como señales tempranas de alerta y permiten identificar si el ritmo de transición es insuficiente para evitar que el riesgo se materialice antes de completar la migración. Su naturaleza es prospectiva y se encuentra directamente vinculada al teorema de la desigualdad de Mosca.

Ambos tipos de indicadores deben integrarse en los sistemas de control interno y reporting corporativo, con definición explícita de umbrales y responsables.

KPIs de inventario y descubrimiento criptográfico

El inventario criptográfico constituye el prerrequisito operativo de cualquier transición PQC y ha sido identificado como primer paso por organismos como la Casa Blanca, el G7 Cyber Expert Group y CISA.

KPIs recomendados:

- Porcentaje de sistemas con inventario criptográfico completado
- Número de activos criptográficos identificados, desagregado por algoritmos vulnerables (RSA, ECC, DH) y algoritmos PQC (ML-KEM, ML-DSA, SLH-DSA)
- Porcentaje de activos con clasificación de criticidad asignada
- Tasa de actualización del inventario
- Cobertura de CBOM sobre aplicaciones críticas

El modelo de inventario, CBOM y ACDI se desarrolla en detalle en el Capítulo 4, por lo que en este apartado se limita su uso como base de medición.

KPIs de migración y despliegue

Una vez completado el inventario, el programa de migración PQC requiere un conjunto de KPIs que permita monitorizar el avance de la sustitución de algoritmos vulnerables y la adopción de los estándares FIPS 203, FIPS 204 y FIPS 205 publicados por el NIST. El G7 CEG destaca la necesidad de establecer métricas cuantificables para demostrar responsabilidad y permitir la recalibración del plan a medida que evoluciona el panorama de amenazas:

- Porcentaje de sistemas críticos migrados a algoritmos post-quantum (*PQC Migration Rate - Critical Systems*): indicador nuclear del programa. La hoja de ruta coordinada de la Unión Europea establece que los casos de uso de alto riesgo deben estar protegidos con PQC antes de 2030.
- Porcentaje de sesiones TLS/HTTPS que utilizan intercambio de claves post-quantum o híbrido (*PQC TLS Adoption Rate*): refleja la penetración real de PQC en las comunicaciones de producción. Las soluciones híbridas PQC/clásico garantizan la interoperabilidad durante el período de transición.
- Porcentaje de proveedores críticos con hoja de ruta PQC documentada y verificada *(Vendor PQC Readiness Rate)*: dado que la mayoría de las organizaciones depende de productos y servicios de terceros, la cadena de suministro criptográfica es una de las principales fuentes de riesgo residual. El G7 CEG recomienda comprometerse con los proveedores de forma temprana para garantizar que sus hojas de ruta incluyan soporte PQC.
- Coste acumulado de la migración frente al presupuesto aprobado (*PQC Migration Budget Variance*): la transición criptográfica completa de una gran organización puede superar los cientos de millones de euros (CEPS, 2025). El seguimiento riguroso del presupuesto permite justificar las inversiones ante el consejo de administración en términos de reducción del riesgo en balance.
- Tiempo medio de migración por sistema (*Mean Time to Migrate o MTTM*): permite proyectar la fecha de finalización del programa y detectar cuellos de botella. La experiencia con migraciones previas de protocolos (por ejemplo, la retirada de SSL 1.0 tardó más de diez años) indica que los plazos iniciales suelen subestimarse.

KRIs de exposición y vulnerabilidad

Los indicadores de riesgo PQC deben medir la probabilidad de que la amenaza cuántica se materialice antes de que la organización complete su migración. El concepto fundamental que articula este análisis es el Teorema de la desigualdad de Mosca: si la suma del tiempo de exposición de los datos sensibles y el tiempo necesario para completar la migración supera el tiempo restante hasta la disponibilidad de un CRQC, la organización se encuentra en situación de riesgo sistémico. Los KRIs de esta categoría cuantifican cada uno de estos factores:

- Porcentaje de datos con requisito de confidencialidad a largo plazo protegidos con criptografía vulnerable (*HNDL Exposure Rate*): mide directamente la exposición al ataque HNDL. Los sectores con mayor período de retención de datos (defensa, salud, finanzas) presentan el mayor riesgo.
- Brecha estimada entre el plazo de migración proyectado y el horizonte de aparición del CRQC (*Migration Gap Index*): KRI estratégico que sintetiza la desigualdad del teorema de Mosca. Cuando el índice es negativo, la organización no completará la migración antes de que el riesgo cuántico sea plausible. Requiere actualización periódica conforme evoluciona la estimación del horizonte cuántico, que sitúa la disponibilidad de un CRQC entre cinco y quince años.
- Porcentaje de sistemas críticos sin plan de migración definido (*Unplanned Critical Systems Rate*): los sistemas sin hoja de ruta documentada representan el riesgo más inmediato. Este KRI alerta sobre vacíos en la planificación y permite priorizar la acción del equipo de seguridad.
- Nivel de cripto-agilidad de la arquitectura (*Crypto-Agility Maturity Score*): mide la capacidad de la organización para sustituir componentes criptográficos sin rediseñar los sistemas que los usan. La cripto-agilidad es identificada por el CEPS Task Force (2025) como el principio rector fundamental de la transición post-quantum. Un score bajo indica dependencias rígidas que aumentan el coste y el tiempo de migración.
- Número de incidentes de seguridad relacionados con gestión de credenciales criptográficas (*Crypto Incident Rate*): indicador operativo que conecta el estado actual de la gestión criptográfica con el riesgo real. Los fallos en la gestión del ciclo de vida de claves y certificados son un precursor de compromisos más graves (Global Digital Trust, 2025).
- Porcentaje de cumplimiento con los hitos regulatorios PQC aplicables (*Regulatory Compliance Rate*): NIS2, DORA y el Cyber Resilience Act establecen obligaciones de seguridad que están siendo interpretadas en clave post-quantum por los reguladores europeos. El incumplimiento de los hitos de la hoja de ruta de la UE (2026/2030/2035) genera exposición normativa directa.

Cuadro de mando PQC para la alta dirección

Los indicadores PQC deben agruparse en un dashboard ejecutivo que permita a la Dirección comprender el riesgo sin necesidad de detalle técnico.

Elementos mínimos:

- Estado del inventario criptográfico: porcentaje de cobertura global, número de activos vulnerables identificados y tendencia trimestral. Este dato conecta directamente con el riesgo en balance de la organización.
- Progreso de migración frente a hitos regulatorios: semáforo de cumplimiento respecto a los plazos 2026, 2030 y 2035 de la hoja de ruta coordinada de la UE, con proyección de si el ritmo actual es suficiente.
- Índice de exposición HNDL: volumen estimado de datos sensibles en riesgo de compromiso diferido, expresado en términos de impacto de negocio para facilitar la comparación con otros riesgos corporativos y la toma de decisiones de inversión.
- Estado de madurez de proveedores críticos: proporción de proveedores con soporte PQC confirmado frente al total, con identificación de las dependencias de mayor riesgo.
- Score de cripto-agilidad: indicador sintético del grado en que la arquitectura tecnológica puede adaptarse a nuevos algoritmos sin intervenciones de rediseño costosas. Debe compararse con el benchmark sectorial cuando esté disponible.

La integración de estos indicadores en ERM, reporting al Board y auditoría se desarrolla de forma específica en el Capítulo 8.

La gestión del riesgo post-quantum no puede ser eficaz sin un sistema de indicadores que traduzca la complejidad técnica de la transición criptográfica en señales claras y accionables para quienes toman las decisiones estratégicas en la organización.

[39] ISMS Forum. The CISO and senior management. https://www.ismsforum.es/ficheros/descargas/the-ciso-and-senior-management1765382437.pdf

5.2. Herramientas y frameworks de evaluación

La evaluación del riesgo post-quantum y el seguimiento del progreso de migración requieren un ecosistema de herramientas y marcos metodológicos que permitan operacionalizar los indicadores definidos en la sección anterior. El mercado y los organismos normativos han desarrollado en los últimos años un conjunto significativo de recursos: desde herramientas de descubrimiento automático de activos criptográficos hasta modelos de madurez que permiten benchmarking sectorial. Este apartado revisa los principales frameworks de evaluación, las herramientas técnicas disponibles y su integración en los sistemas de gobierno corporativo.

Marcos normativos de referencia

El ecosistema normativo que rodea la transición post-quantum ha madurado considerablemente desde la publicación de los estándares FIPS por el NIST en agosto de 2024. Varios marcos de referencia sirven como guías de evaluación para las organizaciones:

- **NIST NCCoE PQC Migration Project**[40]: el Centro Nacional de Excelencia en Ciberseguridad (NCCoE) del NIST ha desarrollado una serie de documentos de orientación que constituyen la referencia técnica más completa disponible. El documento SP 1800-38 (CSWP 48)[41] proporciona guías de migración prácticas; el IR 8547[42] establece plazos estratégicos para la transición de algoritmos específicos; y el CSWP 39[43] analiza los enfoques para lograr crypto-agilidad. Estos documentos conforman el marco de evaluación de referencia para cualquier organización que quiera alinear su programa PQC con las mejores prácticas internacionales.
- **Hoja de ruta coordinada de la UE para la transición PQC**[44]: publicada en junio de 2025 por el Grupo de Cooperación NIS, establece tres hitos de obligado seguimiento para las organizaciones europeas: 2026 (estrategias nacionales establecidas), 2030 (casos de uso de alto riesgo migrados) y 2035 (adopción completa en sectores de menor riesgo). Esta hoja de ruta es el instrumento de evaluación y comparación más relevante para las organizaciones en el espacio europeo.
- **G7 Cyber Expert Group Quantum Roadmap**[45] (enero 2026): referencia específica para el sector financiero, describe seis fases de transición (concienciación, inventario, evaluación de riesgos, ejecución, pruebas y validación continua) y recomienda establecer métricas cuantificables para cada fase. Su modelo de dos velocidades (sistemas críticos antes de 2030-32; resto antes de 2035) es aplicable a organizaciones de otros sectores con adaptaciones.
- **ENISA directrices para la transición PQC**[46]: la Agencia Europea de Ciberseguridad ha publicado orientaciones que complementan la hoja de ruta de la UE con recomendaciones técnicas sobre algoritmos híbridos, gestión de identidades digitales y actualización de infraestructuras de clave pública. Sus directrices se alinean con los estándares ETSI ISG QSC (TR 103 619, TS 103 744) en materia de especificaciones de seguridad cuántica.
- **CISA Automated Cryptographic Discovery Initiative (ACDI)**[47]: la Agencia de Seguridad de Infraestructuras y Ciberseguridad de Estados Unidos ha impulsado el desarrollo de herramientas de descubrimiento criptográfico automatizado como parte de su programa de preparación post-quantum. Aunque orientado inicialmente a la administración pública federal estadounidense, el marco ACDI es una referencia metodológica útil para cualquier organización que quiera automatizar su proceso de inventario.

Herramientas de inventario y descubrimiento criptográfico

La evaluación del riesgo post-quantum no es viable sin visibilidad real sobre el uso de criptografía en los sistemas de la organización. Dado el carácter transversal y embebido de la criptografía en infraestructuras modernas, la automatización resulta imprescindible para mantener la fiabilidad del inventario y la calidad de los datos utilizados en los indicadores.

Desde el punto de vista de la evaluación, las herramientas se agrupan en las siguientes categorías funcionales:

- Análisis de código y CBOM, incluyendo extensiones de SBOM como CycloneDX, orientadas a identificar algoritmos criptográficos, bibliotecas y capacidades de evolución.
- Análisis de tráfico y protocolos criptográficos, que permiten detectar el uso real de suites TLS, algoritmos de intercambio de claves y certificados en producción.
- Plataformas de gestión del ciclo de vida de certificados y claves (CLM / KMS / HSM), que proporcionan visibilidad centralizada y datos críticos para KPIs y KRIs de exposición y agilidad.

---

[40] National Cybersecurity Center of Excellence. (n.d.). Migration to post-quantum cryptography. National Institute of Standards and Technology. https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

[41] National Institute of Standards and Technology. (2024). Cybersecurity framework profile for the responsible use of artificial intelligence (Initial public draft) (NIST CSWP 48). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.48.ipd.pdf

[42] National Institute of Standards and Technology. (2024). Transition to post-quantum cryptography standards (NIST IR 8547). https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[43] National Institute of Standards and Technology. (2023). Cybersecurity framework profile for the hybrid satellite networking environment (NIST CSWP 39). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf

[44] European Commission. (2023). Coordinated implementation roadmap for the transition to post-quantum cryptography. Directorate-General for Communications Networks, Content and Technology. https://digital-strategy.ec.europa.eu/es/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[45] Group of Seven. (2023). G7 cyber expert group: Quantum technologies roadmap. U.S. Department of the Treasury. https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

[46] European Union Agency for Cybersecurity. (2024). Post-quantum cryptography: Current state and quantum mitigation (Version 2). ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf

[47] GovTribe. (n.d.). Automated cryptography discovery and inventory (ACDI) tools. https://govtribe.com/topic-insights/automated-cryptography-discovery-and-inventory-acdi-tools

- Plataformas de descubrimiento criptográfico integral, que combinan análisis de código, red y configuración para ofrecer una visión unificada del inventario.

La descripción técnica y funcional de estas herramientas, así como su papel en la construcción del inventario criptográfico y del CBOM, se desarrolla en detalle en el Capítulo 4. En este apartado se consideran como fuentes de datos para la evaluación del riesgo y el seguimiento del avance del programa PQC.

Frameworks de evaluación de riesgo cuántico

Más allá de los modelos de madurez, existen marcos metodológicos específicos para cuantificar y gestionar el riesgo cuántico que los CISOs pueden integrar en sus sistemas de gobierno:

- **El teorema de la desigualdad de Mosca como herramienta de priorización:** el teorema formulado por Michele Mosca establece que una organización enfrenta riesgo sistémico cuando el tiempo de vida de los datos sensibles más el tiempo necesario para completar la migración supera el horizonte de aparición del CRQC. Esta fórmula proporciona una base cuantitativa para priorizar qué sistemas y datos deben migrarse primero, y es la base del KRI de brecha de migración descrito en la sección 5.1.4.
- **Marco ERM para el riesgo criptográfico:** los marcos de gestión de riesgos empresariales (ERM) permiten integrar el riesgo post-quantum en la visión consolidada de riesgos corporativos. Global Digital Trust[48] propone vincular el riesgo criptográfico a la exposición del balance mediante escenarios de riesgo críticos, cuantificando el impacto en términos monetarios. Este enfoque facilita la justificación de inversiones ante el consejo de administración.
- Hexágono de facetas criptográficas: Global Digital Trust propone ampliar el modelo CIA tradicional con tres facetas adicionales: disponibilidad, no repudio con conservación de evidencias, y validación/confianza. Este marco hexagonal proporciona una visión más completa del impacto criptográfico y debe incorporarse en los marcos de control sobre los que se estructuran los indicadores de seguridad.
- Análisis de coste-beneficio de opciones de mitigación: el CEPS Task Force[49] recomienda analizar las distintas opciones de mitigación: soluciones de hardware híbrido (HSM con soporte PQC, generadores cuánticos de números aleatorios), migraciones de software y enfoques de criptografía híbrida. La cuantificación del coste de la inacción debe superar el coste de migración para que el caso de negocio sea sólido.

Integración de herramientas en la gobernanza corporativa

La adopción de herramientas y frameworks de evaluación solo genera valor real cuando se integra en los procesos de gobierno corporativo de la organización. El CyberIndicatorsFramework subraya que los indicadores de ciberseguridad deben estar alineados con la estrategia global de la organización y permitir demostrar ante la alta dirección la reducción de riesgos y el cumplimiento de los planes de seguridad. Para el contexto PQC, esta integración implica:

- Creación de una función de gestión criptográfica dedicada: el CEPS Task Force recomienda establecer unidades de cripto-gestión con responsabilidad clara sobre el programa de migración PQC, el mantenimiento del inventario criptográfico y la supervisión de los indicadores de seguimiento. La existencia de un comité de dirección PQC con patrocinio ejecutivo es una recomendación específica del sector financiero, extensible a cualquier organización de tamaño relevante.
- Incorporación del riesgo PQC en los informes de riesgo corporativo: los KRIs definidos en la sección 5.1.4 deben aparecer en los informes periódicos de riesgo que el CISO eleva al comité de auditoría y al consejo de administración, expresados en términos de impacto en negocio y no en términos puramente técnicos.
- Integración con herramientas de GRC y CMDB: las plataformas de gestión de gobernanza, riesgo y cumplimiento (GRC) permiten centralizar el seguimiento de los KPIs y KRIs PQC junto con otros indicadores de seguridad. La integración con la base de datos de gestión de configuración (CMDB) es fundamental para mantener actualizado el inventario criptográfico en entornos TI dinámicos.
- Alineación con el ciclo de auditoría y marcos de cumplimiento: las herramientas de evaluación PQC deben integrarse en el calendario de auditorías de seguridad. Los marcos de cumplimiento sectoriales (ENS en España, NIS2, DORA, PCI-DSS) están incorporando progresivamente requisitos relacionados con la preparación post-quantum que deben documentarse mediante los indicadores definidos.
- Colaboración con el ecosistema sectorial: la naturaleza sistémica de la amenaza cuántica hace que la colaboración entre organizaciones sea una palanca de valor crítica. El CEPS Task Force recomienda participar en grupos de trabajo como el Quantum-Safe Financial Forum europeo o el FS-ISAC, y coordinar las exigencias de preparación PQC con los proveedores tecnológicos para reducir la fragmentación y aprovechar el conocimiento colectivo.

La combinación de herramientas automatizadas de descubrimiento criptográfico, modelos de madurez contrastados y marcos de evaluación de riesgo integrados en el gobierno corporativo constituye la base sobre la que las organizaciones pueden construir un programa de transición post-quantum riguroso, medible y sostenible en el tiempo.

[48] Global Digital Trust Insights 2026 – PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

[49] CEPS Task Force – Comments on the NIS Cooperation Group Roadmap for the Transition to Post-quantum Cryptography. https://cdn.ceps.eu/2025/10/Task-FORCE-Comments-on-the-NIS-CG-Roadmap-on-PQC-Transition_FINAL.pdf

5.3. Nivel de madurez en Post-Quantum readiness. Metodología y paradigma

Una organización post-quantum ready es aquella que ha reconocido el impacto estructural de la computación cuántica sobre la criptografía de clave pública y ha planificado e iniciado la transición desde algoritmos vulnerables (RSA, ECC, DH) hacia estándares de criptografía post-quantum (PQC).

En los próximos años, tanto organizaciones públicas como privadas deberán sustituir progresivamente los mecanismos criptográficos tradicionales por nuevos estándares resistentes a futuros ordenadores cuánticos. Estos estándares ya han sido definidos por organismos de referencia, y las recomendaciones actuales coinciden en la necesidad de iniciar de forma temprana la planificación, el inventario y la preparación organizativa.

Aunque no existe un modelo "oficial" único y universal, sí existen referencias públicas complementarias que permiten evaluar de forma coherente la madurez post-quantum. Entre las más relevantes destacan: PQCMM del PKI Consortium: propone cinco niveles de madurez (Inicial, Básico, Avanzado, Gestionado y Optimizado) y define como capacidades clave el inventario criptográfico completo, el uso de SBOM/CBOM, la cripto-agilidad y la capacidad de deshabilitar legado (zero-legacy) y Quantum Readiness Assurance Maturity Model (QRAMM): marco abierto que estructura la evaluación en cuatro dimensiones, visibilidad e inventario criptográfico, gobernanza y riesgo, ingeniería de protección de datos y preparación técnica, y ofrece herramientas de assessment y mapeo con marcos de control.

Ambos modelos coinciden en un principio fundamental: la madurez post-quantum no depende exclusivamente del despliegue de nuevos algoritmos, sino de la acumulación progresiva de capacidades organizativas, técnicas y de gobierno.

La siguiente tabla resume dichas capacidades, asociándolas a cada nivel de madurez. La tabla describe capacidades y estados organizativos, no métricas cuantitativas ni resultados de scoring de riesgo.

Capacidad / Dimensión	Nivel 1 – Inicial	Nivel 2 – Básico	Nivel 3 – Avanzado	Nivel 4 – Gestionado	Nivel 5 – Optimizado
Gobernanza y Roadmap	**Sin roadmap formal; acciones ad-hoc. (PQCMM L1)**	Roadmap inicial aprobado; roles definidos. (CISA Quantum-Readiness)	Roadmap con dependencias y riesgos; steering activo. (QRAMM)	Roadmap integrado en carteras/ PMO y auditorías. (NCCoE CSWP-48 mapeado a CSF/800-53)	Mejora continua y métricas ejecutivas ligadas a metas de NIST IR 8547.
Descubrimiento e inventario	**Conocimiento parcial; sin repositorio único. (PQCMM L1)**	Inventario inicial manual por dominios. (PQC Coalition Workbook)	Inventario centralizado de algoritmos/llaves/ certificados/ protocolos. (NCCoE Discovery)	ACDI automatizado y recurrente; cobertura alta. (CISA ACDI)	Inventario "live" con calidad de datos y dashboards de riesgo. (QRAMM)
CBOM / SBOM	**No existen o están inconexos. (PQCMM L1)**	SBOM parcial en builds críticos. (QRAMM)	CBOM mantenido por sistema/activo. (Ivezic – CBOM)	CBOM integrado a gestión de cambios y riesgo. (PQCMM L4)	CBOM/SBOM como fuente de verdad para auditoría y compliance. (NCCoE CSWP-48)
Cripto-agilidad	**Cambios de algoritmo requieren rediseño. (PQCMM L1)**	Soporte básico de feature flags o config. (PQCMM L2)	Mecanismos de crypto-agility en funciones críticas. (PQCMM L3)	Zero-legacy configurable: operar sin algoritmos no-PQC. (PQCMM L4)	PQC por defecto; legado sólo bajo excepción controlada. (PQCMM L5)
Híbridos / compuestos	**No aplicable o no soportado. (PQCMM L1)**	Pruebas limitadas en pilots. (NCCoE Interoperability)	Uso selectivo en canales críticos. (IETF PQUIP use cases)	Soporte declarado (híbrido/ compuesto) y gestionado. (PQCMM L4)	Estrategia híbrida/ compuesta institucionalizada hasta retirada total de legado conforme IR 8547.
Adopción de FIPS 203/204/205	**Sin despliegues; pruebas ad-hoc. (PQCMM L1)**	ML-KEM/ML-DSA/ SLH-DSA disponibles en pilot. (NIST PQC)	Despliegue en dominios priorizados por riesgo. (NCCoE Discovery→Prioritization)	Cobertura amplia y compatibilidad multi-vendor. (NCCoE Interoperability)	Adopción por defecto y back-out controlado; objetivos alineados a 2030/2035. (NIST IR 8547)
Code-signing / firmware	**RSA/ECC sin plan de sustitución. (PQCMM L1)**	Pilotos con HBS (LMS/XMSS). (NSA CNSA 2.0 + NIST SP 800-208)	SLH-DSA (FIPS 205) y/o HBS en builds críticos. (NIST PQC)	Firma PQC generalizada; control de claves/contadores (estado). (SP 800-208)	100% de artefactos firmados con PQC; verificación en secure-boot. (CNSA 2.0)
Terceros / Supply chain	**Sin roadmaps PQC de proveedores. (CISA)**	Recolección básica de roadmaps y dependencias. (CISA)	Requisitos PQC en contratos; evaluación de riesgo de terceros. (QRAMM)	Alineación de versiones/protocolos PQC a escala. (NCCoE)	Vendor lock-in mitigado; interoperabilidad verificada de forma continua. (NCCoE Interoperability)
Riesgo y priorización	**Sin criterio formal de priorización. (PQCMM L1)**	Matriz simple (vida útil, exposición). (CISA)	Modelo de riesgo y hoja de ruta por casos de uso. (NCCoECSWP-48 →CSF/800-53)	Priorización dinámica ligada a inventario ACDI/ CBOM. (CISA ACDI + CBOM)	Riesgo residual medido vs. plazos IR 8547 y tolerancias corporativas.
Monitorización & reporting	**Reportes esporádicos; sin KPIs. (PQCMM L1)**	KPIs básicos (cobertura de inventario). (PQC Coalition Workbook)	Reporting periódico a steering y riesgo/ cumplimiento. (QRAMM)	Dashboards ligados a CSF 2.0/800-53 (CSWP-48).	Scorecards ejecutivos con metas 2030/2035 y trendlines. (NIST IR 8547)

Tabla de capacidades y niveles de madurez post-quantum

5.4. Ejemplos prácticos de scoring y dashboards ejecutivos

Prepararse para la era post-cuántica exige pasar del marco conceptual a herramientas prácticas de decisión. La Dirección necesita instrumentos que permitan medir la exposición real, priorizar actuaciones y monitorizar el progreso de la transición de forma objetiva.

Este apartado presenta ejemplos prácticos de modelos de scoring, mecanismos de cuantificación y estructuras de dashboard ejecutivo alineadas con la toma de decisiones.

Modelo de Scoring y Cuantificación Detallada del Riesgo Cuántico

El modelo de scoring permite traducir la exposición post-quantum en valores comparables, facilitando la priorización de activos y sistemas en función de su urgencia y criticidad. A diferencia de los modelos de madurez, que describen el estado global de las capacidades organizativas, el scoring se aplica a activos concretos, incorporando variables de riesgo y de viabilidad de mitigación.

Los enfoques más utilizados combinan principios derivados del teorema de la desigualdad de Mosca, junto con modelos multidimensionales como QARS o CARAF, que permiten matizar la urgencia en función del impacto real y de la capacidad de respuesta de la organización.

El scoring se articula en cinco dimensiones:

a) Inventario y Descubrimiento Criptográfico

Objetivo: Tener una visibilidad completa de todos los activos criptográficos, un primer paso considerado crítico y universalmente recomendado.

Métrica	Descripción	Puntuación (0-5)
Completitud del Inventario (CBOM)	Porcentaje de sistemas y aplicaciones cubiertos en el inventario criptográfico (Cryptographic Bill of Materials).	0: Sin inventario. 5: Inventario completo y automatizado.
Identificación de Algoritmos Vulnerables	Capacidad para identificar y etiquetar algoritmos vulnerables (RSA, ECC) en el inventario, usando herramientas como CodeQL o eBPF.	0: Sin capacidad. 5: Identificación en tiempo real.
Clasificación por Horizonte de Confidencialidad	Grado en que los datos protegidos por la criptografía están clasificados según su "vida útil" (shelf-life), es decir, cuánto tiempo deben permanecer seguros.	0: Sin clasificación. 5: Todos los datos críticos clasificados.

b) Agilidad Criptográfica (Crypto-Agility)

Objetivo: capacidad para reemplazar algoritmos y certificados de forma rápida y automatizada, un pilar central para proveedores como Google Cloud.

Métrica	Descripción	Puntuación (0-5)
Modularidad de la Criptografía	Porcentaje de aplicaciones que usan bibliotecas modulares en lugar de algoritmos codificados ("hardcoded") .	0: Todo codificado. 5: 100% modular.
Automatización del Ciclo de Vida	Nivel de automatización en la gestión de certificados (emisión, rotación, revocación) con herramientas como DigiCert Trust Lifecycle Manager.	0: Procesos manuales. 5: Ciclo de vida totalmente automatizado.
Tiempo de Mitigación de Vulnerabilidades (MTTR)	Tiempo medio para reemplazar un algoritmo vulnerable una vez identificado, un KPI clave de eficiencia.	0: Meses/Años. 5: Horas/Días.

c) Planificación y Gobernanza de la Migración

Objetivo: establecer una estrategia formal, con recursos y responsabilidades claras, para la migración a PQC.

Métrica	Descripción	Puntuación (0-5)
Estrategia y Hoja de Ruta Formal	Existencia de una hoja de ruta plurianual para la migración a PQC, con presupuesto asignado y alineada con plazos como los del NIST (2030-2035).	0: Sin plan. 5: Plan detallado, financiado y comunicado.
Asignación de Roles y Responsabilidades	Definición de un equipo multifuncional (ej. "Grupo de Amenazas Cuánticas") y roles como el "Ingeniero PQC".	0: Sin responsables. 5: Equipo multifuncional con roles claros.
Políticas y Estándares Actualizados	Inclusión del riesgo cuántico y los requisitos de PQC en las políticas de seguridad, desarrollo y adquisiciones, idealmente como "cripto-como-código".	0: Sin mención. 5: Políticas alineadas con PQC y automatizadas.

d) Proyectos Piloto y Pruebas

Objetivo: validar la viabilidad técnica y el impacto en el rendimiento de los nuevos algoritmos PQC en entornos controlados.

Métrica	Descripción	Puntuación (0-5)
Ejecución de Pruebas de Concepto (PoC)	Número de algoritmos PQC (ej. Kyber, Dilithium) probados en entornos de laboratorio.	0: Ninguno. 5: Múltiples PoCs completados con éxito.
Despliegue de Pilotos Híbridos	Implementación de esquemas híbridos (clásico + PQC) en aplicaciones no críticas, una práctica estándar en la industria.	0: Sin pilotos. 5: Pilotos en producción en sistemas de bajo riesgo.
Análisis de Impacto en el Rendimiento	Medición del impacto de los algoritmos PQC en latencia, CPU y ancho de banda, ya que las claves y firmas son más grandes.	0: Sin análisis. 5: Análisis de rendimiento detallado y documentado.

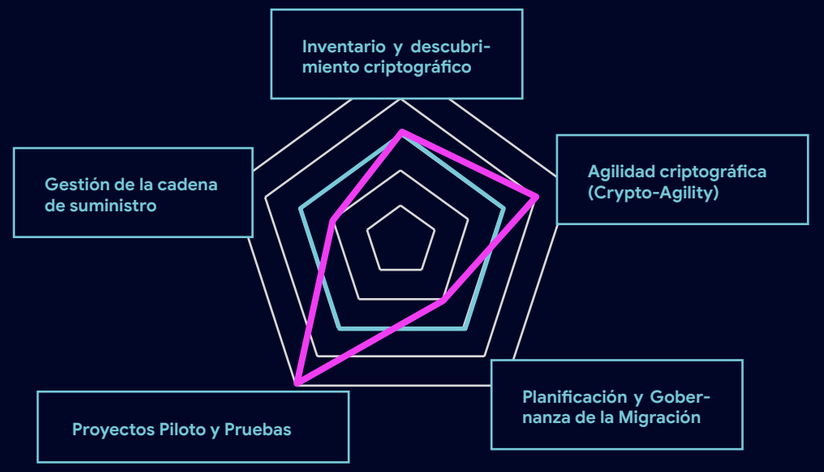
e) Gestión de la Cadena de Suministro

Objetivo: asegurar que los proveedores de software y hardware estén preparados para la transición a PQC.

Métrica	Descripción	Puntuación (0-5)
Evaluación de Proveedores Críticos	Porcentaje de proveedores críticos evaluados sobre su hoja de ruta y preparación para PQC.	0: 0%. 5: 100%.
Inclusión de PQC en Contratos	Inclusión de cláusulas que exigen el soporte de PQC en los nuevos contratos y renovaciones con proveedores.	0: Nunca. 5: Cláusula estándar en todos los contratos.
Cobertura de SBOM/ CBOM de Terceros	Porcentaje de software de terceros para el que se dispone de un Manifiesto de Software (SBOM) o Criptográfico (CBOM).	0: 0%. 5: >90%.

A modo ilustrativo, el modelo puede aplicarse de forma homogénea a los distintos dominios de evaluación, obteniendo una puntuación sintética por dimensión que facilite su comparación y posterior agregación.

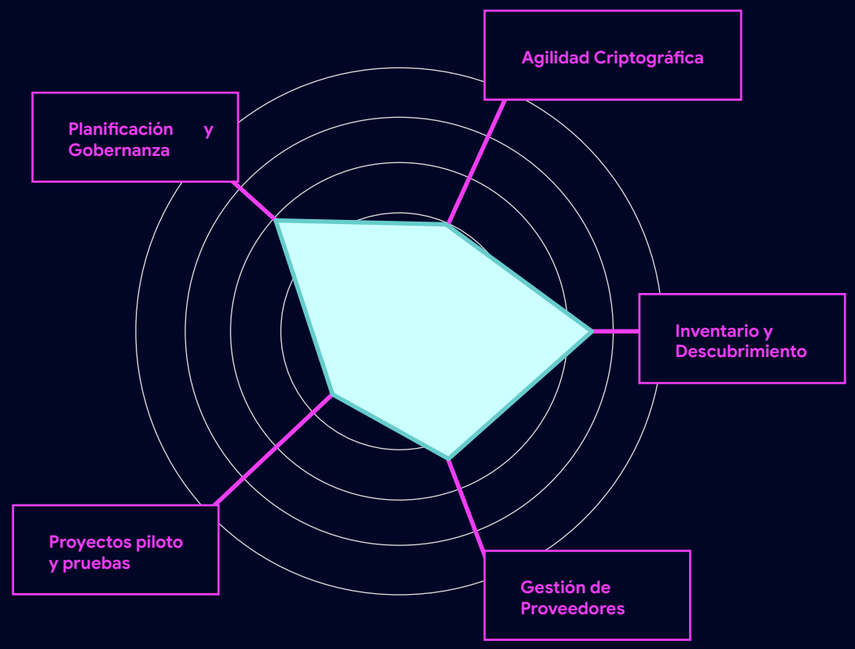
a) Inventario y Descubrimiento Criptográfico	3
b) Agilidad Criptográfica	4
c) Planificación y Gobernanza de la Migración	2
d) Proyectos Piloto y Pruebas	5
e) Gestión de la Cadena de Suministro	2



Perfil comparativo de preparación post-quantum por dimensión

Este gráfico de radar, ideal para visualizar la madurez en múltiples dominios, muestra nuestra madurez en las cinco áreas clave. El objetivo es alcanzar un nivel "Establecido" (puntuación de 3) para finales de 2026.

- Inventario y Descubrimiento: 3.5 (Establecido)
- Agilidad Criptográfica: 2.0 (En Desarrollo)
- Planificación y Gobernanza: 3.0 (Establecido)
- Proyectos Piloto y Pruebas: 1.5 (Inicial)
- Gestión de Proveedores: 2.5 (En Desarrollo)



Nivel de madurez y exposición post-quantum por dimensión

El análisis pone de manifiesto una fortaleza clara en la visibilidad de los activos criptográficos, apoyada en el uso de herramientas de inventario automatizado, frente a una debilidad relevante en la capacidad de sustitución ágil de algoritmos, especialmente evidenciada por el retraso en la ejecución de pilotos híbridos.

Una vez priorizados los activos y dominios críticos mediante el modelo de scoring, el siguiente paso natural consiste en traducir dicha priorización en términos económicos comprensibles para la Dirección.

Deuda financiera es un término análogo a la "deuda técnica", representa el coste acumulado de no abordar las vulnerabilidades criptográficas y la migración a PQC. Se calcula sumando el coste de remediación de todos los sistemas vulnerables y el valor potencial de los datos en riesgo. Este indicador monetario es clave para comunicar la urgencia a la dirección.

Modelo de Costes de Remediación (CR): Estima el coste de "pagar" la deuda.

$$CR = (Horas\_Dev \times Tarifa\_Hora) + Coste\_HW\_SW + Coste\_Consultoría + Coste\_Pruebas$$

- Horas de Desarrollo: esfuerzo para refactorizar código, actualizar librerías y reconfigurar sistemas.
- Coste de HW/SW: adquisición de nuevos Módulos de Seguridad de Hardware (HSM) compatibles con PQC, licencias, etc.
- Coste de Consultoría: gastos en expertos externos para auditorías y guía estratégica.
- Coste de Pruebas: esfuerzo para validar la interoperabilidad y el rendimiento.

Valor Financiero de los Datos en Riesgo (VaR): Estima el impacto de una brecha de datos.

$$VaR = Probabilidad\_Incidente \times Impacto\_Financiero$$

- Probabilidad de Incidente: Aumenta a medida que se acerca el "Día Q".
- Impacto Financiero: Suma de costes directos e indirectos como multas regulatorias (GDPR, DORA), daño reputacional, pérdida de negocio y litigios.

Creación de un "Quantum Risk Score" (QRS) por Activo

Para priorizar activos individuales, se puede desarrollar una puntuación de riesgo que permita centrarse primero en lo más importante.

1. Definición de Variables Clave:

- Vida Útil de los Datos (VUD): el tiempo que los datos deben permanecer confidenciales
- Criticidad del Activo (CA): el impacto en el negocio (operativo, financiero, reputacional) si el activo se ve comprometido
- Tiempo de Migración (TM): el esfuerzo y tiempo necesarios para migrar el activo a PQC

2. Definición de Escalas de Calificación (Ejemplo 1-5):

- VUD: 1 (< 1 año), 3 (1-5 años), 5 (> 10 años) [Source 1]
- CA: 1 (Bajo impacto), 3 (Impacto moderado), 5 (Crítico para el negocio)
- TM: 1 (< 6 meses), 3 (6-24 meses), 5 (> 3 años)

3. Fórmula Ponderada para el Quantum Risk Score (QRS):

Se asignan pesos (w) a cada variable según la estrategia de la organización.

$$QRS = (w\_VUD \times VUD) + (w\_CA \times CA) + (w\_TM \times TM)$$

- Esta fórmula permite clasificar los activos. Se da prioridad a aquellos donde la suma de la vida útil de los datos y el tiempo de migración supera el horizonte de la amenaza (VUD + TM > Horizonte_Amenaza), un concepto conocido como la "desigualdad de Mosca"

Para tener un valor único de cada a la dirección se puede optar por dos iniciativas:

- Poner la media de los activos más críticos para la organización. Este punto dará una visibilidad mayor del riesgo al que se enfrenta la organización.
- Poner la media de todos los activos de la organización. Puede difuminar el riesgo de los activos más importantes con el de los menos importantes.

Se recomienda el primero con un botón de desglose que permita ver el detalle del alcance.

Herramientas, Arquitectura y Casos Prácticos

La teoría se materializa a través de herramientas, una arquitectura de datos bien definida y proyectos piloto que ya están en marcha.

1. Herramientas para la Automatización y Pruebas

Inventario y Gestión (Comerciales):

- SandboxAQ (AQtive Guard): plataforma de gestión de la postura criptográfica (CPM) para visibilidad en tiempo real
- Keyfactor Command: realiza escaneos para crear un inventario centralizado
- AppViewX (AVX ONE): ofrece descubrimiento y cuadros de mando de resiliencia
- Otras: QuSecure, QryptoCyber, y CryptoNext Security

Inventario y Estándares (Código Abierto):

- CBOMkit (de la PQCA): Herramientas para generar y gestionar CBOMs.
- Cryptobom-Forge: Herramienta desarrollada por Santander para ayudar a los desarrolladores a identificar componentes vulnerables en su código.
- CycloneDX: Estándar de OWASP para SBOMs extendido para incluir detalles criptográficos.

Pruebas y Simulación:

- Simulador de PQC de Utimaco: Permite probar los nuevos estándares PQC en entornos propios.
- AppViewX PQC Test Center: Servicio en línea para probar la generación de certificados PQC.

2. Arquitectura Técnica para la Creación de Dashboards

Para construir un dashboard ejecutivo dinámico, es crucial integrar los datos de las herramientas de inventario en plataformas como Power BI o Tableau.

- **Capa de Adquisición de Datos:** se utilizan herramientas como SandboxAQ o Keyfactor para descubrir activos criptográficos. La mayoría ofrece APIs REST para la extracción de datos. Existe un conector personalizado de Power BI para la API de Keyfactor disponible en GitHub.
- **Capa de Integración y Almacenamiento (ELT):** se cargan los datos brutos en un data warehouse en la nube (ej. Azure Synapse, Google BigQuery). Aquí, los datos se limpian, normalizan y enriquecen con contexto de negocio de otras fuentes como un ERP o un sistema de gestión de activos.
- **Capa de Modelado de Datos:** dentro del data warehouse, se crea un modelo de datos optimizado, como un modelo en estrella para Power BI. Este modelo relaciona los activos criptográficos con las unidades de negocio, la criticidad de las aplicaciones y la sensibilidad de los datos:
  - Tabla de Hechos (Inventario Criptográfico): contiene métricas como ID_Activo, Algoritmo, Es_Vulnerable_PQC, Quantum_Risk_Score, Deuda_Criptografica (valor monetario).
  - Tablas de Dimensiones: incluyen Sistemas (Unidad_Negocio, Criticidad_Negocio), Vulnerabilidades y Madurez PQC.
- **Capa de Visualización (BI):** se conecta Power BI o Tableau al modelo de datos para construir los informes y dashboards interactivos.

Dashboard Ejecutivo para la Transición a PQC

Un dashboard ejecutivo traduce la complejidad técnica en una visión clara para la alta dirección. Su objetivo es responder a preguntas clave: ¿Cuál es nuestro nivel de riesgo? ¿Cuál es el nivel de progreso de acuerdo con el plan? ¿Dónde debemos enfocar los recursos? Los datos se obtienen de las herramientas de gestión y los modelos de cuantificación financiera.

Resumen Ejecutivo

Métrica Clave	Valor	Tendencia	Estado
Puntuación General de Madurez PQC	2.8 / 5.0		En Desarrollo
Puntuación de Riesgo Cuántico (Agregada)	6.5 / 10		Alto
Deuda Criptográfica (Estimada)	€15M		Alta
Progreso de la Hoja de Ruta	35%		En curso
Cobertura del Inventario (CBOM)	70%		Moderado

Progreso de la Hoja de Ruta de Migración a PQC

Un diagrama de Gantt permite mostrar el estado de las principales iniciativas de una hoja de ruta dividida en fases estratégicas. Otras visualizaciones útiles incluyen gráficos de tendencia para seguir la evolución de la "Deuda Criptográfica" o diagramas de Sankey para ilustrar cómo las vulnerabilidades contribuyen al riesgo general.

Ejemplo Diagrama de Gantt:

Hito	Q1 2026	Q2 2026	Q3 2026	Q4 2026	Estado
Fase 1: Descubrimiento y Gobernanza					Completado
Fase 2: Pilotos Híbridos (Banca Privada)					En Curso
Fase 3: Migración Producción (Tier 1)					Pendiente
Fase 4: Optimización y Retiro					Pendiente

Indicadores Clave de Rendimiento (KPIs)

Métricas específicas para monitorizar el progreso del programa de migración. Las tablas detalladas permiten a los usuarios explorar los datos subyacentes.

Progreso de la Migración:

- Aplicaciones críticas migradas a PQC: 15% (ejemplo)
- Porcentaje de algoritmos PQC desplegados: 10% (ejemplo)
- Certificados migrados a modo híbrido: 22% (ejemplo)

Reducción de Riesgos:

- Sistemas vulnerables a HNDL mitigados: 250 / 1,200 (21%) (ejemplo)
- Reducción de la Puntuación de Riesgo Cuántico (trimestral): -0.5 puntos (ejemplo)

Gobernanza y Cadena de Suministro:

- Proveedores críticos con hoja de ruta PQC: 15 de 40 (38%) (ejemplo)
- Nuevos contratos con cláusula PQC: 60% (ejemplo)

En general se puede decir que la transición hacia la criptografía post-quantum es un maratón estratégico, no un sprint técnico. Requiere una planificación cuidadosa, una inversión sostenida y, sobre todo, una visibilidad clara del progreso y los riesgos.

Los modelos de scoring, las metodologías de cuantificación financiera y los dashboards ejecutivos, alimentados por una arquitectura de datos robusta y un ecosistema de herramientas, son indispensables en este proceso. Permiten a las organizaciones:

- **Cuantificar el riesgo financieramente:** transformar un problema abstracto en un riesgo de negocio medible y monetizable, utilizando conceptos como la "Deuda Criptográfica" con fórmulas de coste específicas y marcos como FAIR.
- **Priorizar inversiones:** identificar dónde enfocar los recursos basándose en un "Quantum Risk Score" por activo y en datos de herramientas de inventario como SandboxAQ o Keyfactor.
- **Construir un caso de negocio sólido:** utilizar la arquitectura técnica recomendada (ELT, data warehouse, modelo en estrella, etc) para integrar datos técnicos con datos de negocio y presentar una visión unificada del riesgo.
- **Automatizar la gobernanza:** implementar la "cripto-como-código" utilizando flujos de CI/CD y herramientas como OPA para garantizar la agilidad y el cumplimiento de las políticas de forma automática.
- **Comunicar eficazmente:** proporcionar a la alta dirección una visión clara del estado de la preparación a través de KPIs concretos y visualizaciones como mapas de calor y gráficos de radar, facilitando la toma de decisiones.
- **Aprender de la experiencia práctica:** incorporar las lecciones aprendidas de los pilotos de la industria sobre la integración con sistemas heredados, la gestión de claves híbridas y la validación de la cadena de suministro.

Al adoptar un enfoque estructurado y basado en métricas, las empresas pueden pasar de la simple conciencia del riesgo cuántico a una gestión proactiva. Esto asegura que la confianza digital, pilar de la economía actual, se mantenga intacta frente a los desafíos del mañana.

6. Estrategias de Mitigación y Cripto-agilidad

6.1. Roadmap de transición: dual-stack, modos híbridos, PQC-only

La transición debe garantizar la continuidad operativa y un incremento progresivo de la seguridad, de forma que cada etapa[50] mejore la postura de seguridad existente[51].

1. Dual-stack:

El modelo dual-stack se basa en la coexistencia simultánea de algoritmos criptográficos clásicos, como RSA o ECC, junto con algoritmos de criptografía post-quantum dentro de una misma infraestructura. Su objetivo principal es garantizar la interoperabilidad entre sistemas heredados y nuevos durante el proceso de transición[52].

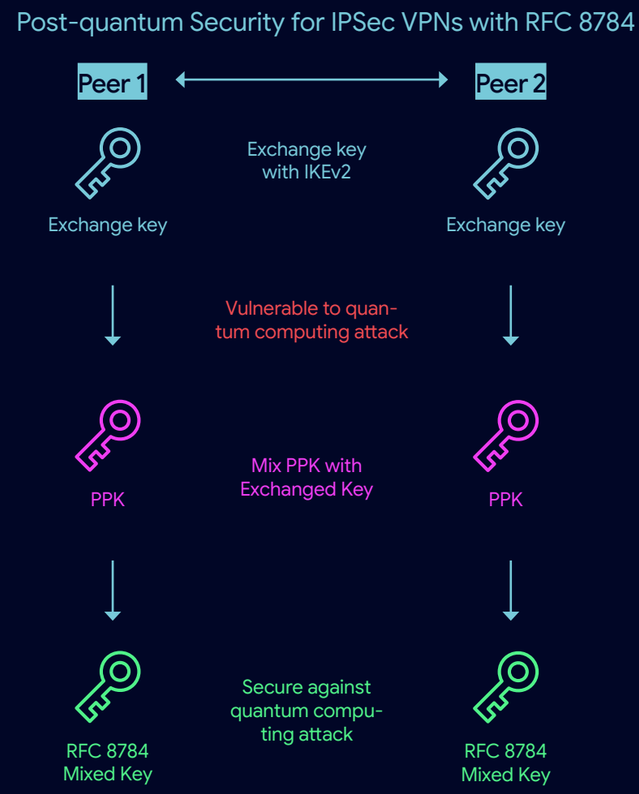
Gracias a ello, es plenamente compatible con infraestructuras existentes como PKI, TLS o VPN.

No obstante, introduce una mayor complejidad en la gestión y no garantiza seguridad post-quantum real en aquellos escenarios donde se siga utilizando criptografía clásica.

2. Modos híbridos:

El enfoque de modos híbridos combina algoritmos clásicos y post-quantum dentro de una misma operación criptográfica. En lugar de coexistir de forma independiente, ambos mecanismos participan conjuntamente en procesos como el intercambio de claves o la firma digital.

Un ejemplo representativo se encuentra en protocolos como TLS, donde se emplean combinaciones del tipo ECDHE + Kyber, generando una clave final derivada de ambos esquemas[53].



Esquema conceptual de un modo híbrido de intercambio de claves[54] (clásico + post-cuántico)

El secreto criptográfico final se obtiene de la combinación de un mecanismo clásico (por ejemplo, ECDHE) y uno post-quantum (por ejemplo, ML KEM), evitando la dependencia de un único algoritmo.

Este enfoque responde a un principio de resiliencia criptográfica: si uno de los esquemas resultara comprometido en el futuro, el canal seguiría siendo seguro mientras el otro permanezca robusto, lo que reduce el riesgo durante el periodo de transición.

No obstante, los modos híbridos introducen retos operativos, como el aumento del tamaño de claves y mensajes, un mayor consumo computacional y una mayor complejidad en la gestión criptográfica, lo que hace necesarias pruebas de interoperabilidad y evaluaciones de rendimiento previas al despliegue.

A pesar de estas limitaciones, existe un consenso amplio en que los modos híbridos proporcionan el mejor equilibrio entre seguridad, compatibilidad y viabilidad operacional, y constituyen el patrón recomendado hasta que el ecosistema de criptografía post-quantumalcance la madurez necesaria para despliegues PQC-only generalizados.

---

[50] European Commission. (2025). A coordinated implementation roadmap for the transition to post-quantum cryptography. Directorate General for Communications Networks, Content and Technology (DG CONNECT). https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[51] G7 Cyber Expert Group. (2026). Advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector.https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector/g7-cyber-expert-group-statement-on-advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector-january-20

[52] European Union Agency for Cybersecurity. (2021). Post-quantum cryptography: Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[53] Kampanakis, P., Panos, D., Kahn, G., & Van Geest, D. (2020). Post-quantum TLS: Operational considerations (Internet Draft, IETF). https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

[54] Quantropi Inc. (2025). QiSpace™ SEQUR PPK Generator: Post-quantum Preshared Keys for hybrid cryptographic security. https://www.quantropi.com/solutions/ppk-generator/

3. PQC-only

El modelo PQC-only representa la fase final del roadmap de transición criptográfica, en la que se elimina completamente la criptografía clásica para operar exclusivamente con algoritmos resistentes a la computación cuántica, como ML-KEM (Kyber) para intercambio de claves o ML-DSA / SLH-DSA para firma digital, integrados en una infraestructura plenamente adaptada.

Su principal ventaja es la obtención de seguridad cuántica completa a largo plazo, eliminando cualquier dependencia de algoritmos vulnerables a ataques como el de Shor y simplificando el stack criptográfico una vez superada la fase de transición.

Sin embargo, la adopción generalizada de un enfoque PQC-only presenta limitaciones relevantes en el estado actual del ecosistema, incluyendo una madurez aún desigual de las implementaciones, dependencias críticas en la cadena de suministro y posibles impactos en rendimiento y compatibilidad, especialmente en sistemas heredados o con restricciones de hardware.

Por este motivo, el modelo PQC-only se considera actualmente un objetivo a medio y largo plazo, más adecuado para entornos cerrados, sistemas de nueva construcción o casos de uso de muy alta criticidad, que para su despliegue inmediato en entornos empresariales heterogéneos.

Comparativa	Dual-stack	Híbrido	PQC-only
Objetivo	Interoperabilidad	Seguridad progresiva	Seguridad total
Nivel de seguridad	Clásico	Clásico + PQC	PQC
Complejidad	Media	Alta	Media
Rendimiento	Alto	Medio	Variable
Riesgo cuántico	Alto	Bajo	Muy bajo
Madurez	Alta	Media	Baja
Recomendación actual	Sí (fase inicial)	Sí (fase principal)	Futuro
Ventajas principales	- Máxima compatibilidad - Bajo impacto inicial - Migración gradual	- Mitiga ruptura de algoritmos - Protección frente a HNDL - Estrategia recomendada	- Seguridad cuántica completa - Simplificación del stack criptográfico
Desventajas principales	- Mayor complejidad operativa - Aumenta superficie de ataque	- Mayor latencia y tamaño - Más consumo computacional - Complejidad de implementación	- Falta de madurez - Impacto en rendimiento - Riesgo por juventud criptográfica

Comparativa de enfoques de transición criptográfica

6.2. Gestión de la cripto-agilidad y actualización continua

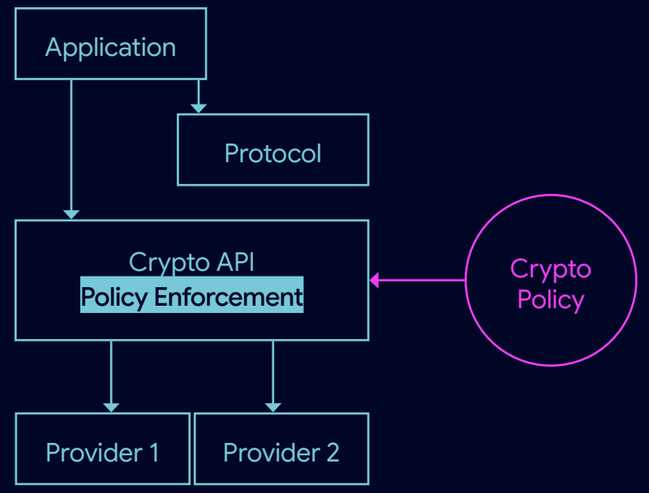
La cripto-agilidad constituye el principio rector de cualquier estrategia post-cuántica viable. En términos operativos, se entiende como la capacidad de sustituir algoritmos, protocolos y bibliotecas criptográficas sin rediseñar los sistemas que los utilizan.

Principios operativos de cripto-agilidad:

1. Desacoplamiento criptográfico

El desacoplamiento criptográfico consiste en separar la lógica criptográfica de la lógica de negocio dentro de los sistemas. Este principio busca evitar que los algoritmos estén embebidos directamente en las aplicaciones, lo que dificultaría su sustitución.

Para lograrlo, se emplean mecanismos como APIs criptográficas, capas de abstracción (abstraction layers) y proveedores criptográficos configurables. Este enfoque permite que las aplicaciones consuman servicios criptográficos sin depender de implementaciones específicas.



NIST CSWP 39[55]. Considerations for Achieving Crypto Agility[56]

El objetivo principal es habilitar la sustitución de algoritmos sin necesidad de rediseñar o reimplementar el sistema completo.

[55] National Institute of Standards and Technology. (2025). Considerations for achieving crypto agility: Strategies and practices (NIST Cybersecurity White Paper 39). U.S. Department of Commerce. https://www.nist.gov/publications/considerations-achieving-crypto-agility

[56] Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W., & Kent, K. (2025). Considerations for achieving cryptographic agility: Strategies and practices (NIST Cybersecurity White Paper CSWP 39). https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/final

2. Negociación dinámica de algoritmos

La negociación dinámica de algoritmos permite que los sistemas seleccionen en tiempo de ejecución los algoritmos criptográficos más adecuados según el contexto, las capacidades del sistema y los requisitos de seguridad. Este principio es clave para garantizar interoperabilidad durante la transición criptográfica.

Esto implica que los sistemas deben soportar múltiples suites criptográficas, incorporar mecanismos de control de versiones y permitir la selección dinámica de algoritmos durante la comunicación. Protocolos como TLS 1.3 ya implementan este enfoque mediante la negociación de cipher suites, y están evolucionando hacia modos híbridos que combinan criptografía clásica y post-quantum.

3. Soporte de algoritmos múltiples

Una arquitectura cripto-ágil debe ser capaz de operar simultáneamente con múltiples algoritmos criptográficos. Esto incluye algoritmos clásicos (como RSA o ECC), algoritmos post-quantum (como Kyber o Dilithium) y combinaciones híbridas de ambos.

El uso de enfoques híbridos se ha consolidado como una estrategia clave en la transición hacia la criptografía post-quantum, ya que permite mantener la seguridad incluso si uno de los algoritmos resulta comprometido.

Este principio no solo aporta resiliencia, sino que también facilita pruebas, validación progresiva y despliegues controlados.

4. Gestión del ciclo de vida criptográfico

La cripto-agilidad requiere una gestión activa y estructurada del ciclo de vida de los mecanismos criptográficos. Esto implica no solo desplegar algoritmos, sino también gobernar su evolución, uso y retirada.

Entre los elementos clave de este principio se incluyen el inventario criptográfico, la clasificación de activos, las políticas de rotación de claves y algoritmos, y los planes de deprecación.

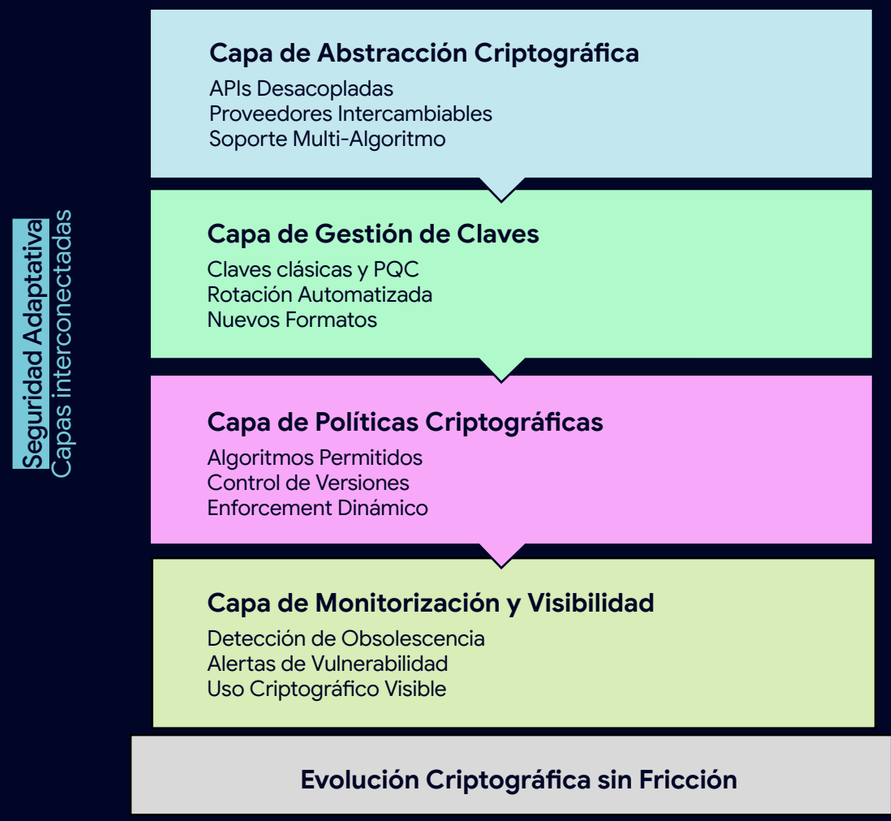
5. Cripto-agilidad como proceso continuo

Finalmente, la cripto-agilidad no debe entenderse como un proyecto puntual, sino como un proceso continuo dentro de la organización. La evolución constante de amenazas, tecnologías y estándares obliga a mantener una actitud proactiva y adaptativa. Este proceso continuo implica:

- Evaluación constante del estado criptográfico
- Actualización de algoritmos
- Incorporación de nuevas tecnologías
- Sustitución de mecanismos obsoletos.

Estos principios dan lugar a tener que diseñar una suerte de arquitectura de cripto-agilidad basadas en capas y tratada como un proceso de mejora continua.

Arquitectura de Cripto-agilidad



Recomendaciones técnicas para implantar cripto-agilidad

A partir de estos principios, las principales recomendaciones técnicas son:

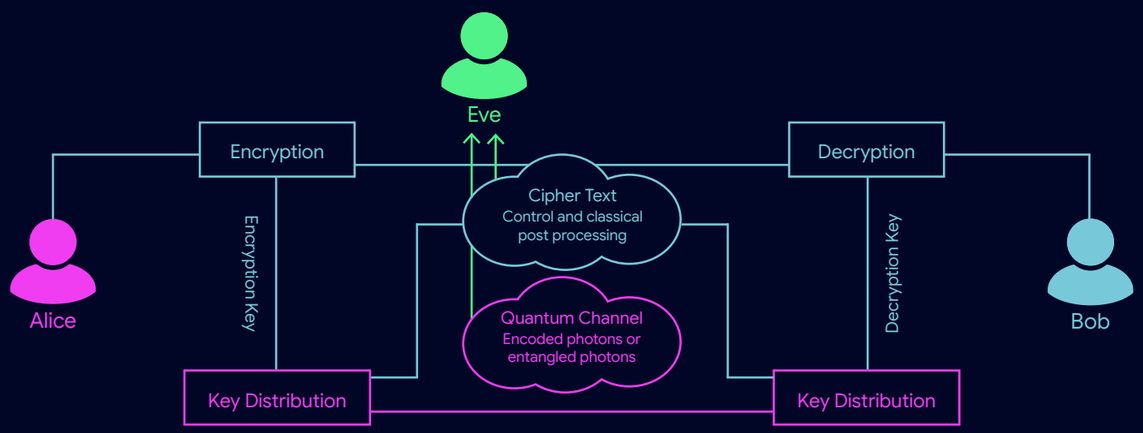
- Diseñar sistemas crypto ready, con soporte multi-algoritmo y alto nivel de configurabilidad.
- Adoptar esquemas híbridos como patrón de transición para equilibrar seguridad y compatibilidad.
- Automatizar los cambios criptográficos siempre que sea posible, reduciendo la intervención manual.
- Controlar dependencias externas, especialmente librerías, dispositivos y plataformas de terceros.
- Aplicar un enfoque iterativo, con pruebas controladas y despliegues progresivos.

La correcta implementación de la cripto-agilidad constituye el cimiento técnico sobre el que pueden desplegarse con éxito las estrategias de mitigación post-quantum, reduciendo el riesgo operativo y facilitando la evolución futura hacia entornos plenamente resistentes a la computación cuántica.

6.3. Quantum Key Distribution (QKD): hype vs realidad

La distribución cuántica de claves (Quantum Key Distribution, QKD) es una tecnología criptográfica cuyo objetivo es generar y distribuir claves secretas entre dos partes utilizando principios de la mecánica cuántica, como la no clonación del estado cuántico y la detección de interferencias durante la transmisión. A diferencia de la criptografía convencional, QKD no cifra datos directamente, sino que proporciona material criptográfico que posteriormente se emplea en algoritmos de cifrado clásicos.

Desde una perspectiva técnica, QKD requiere canales físicos dedicados, como fibra óptica o enlaces ópticos en espacio libre, y se apoya en protocolos específicos, siendo BB84[57] el más conocido. La detección de cualquier intento de interceptación durante la distribución de claves constituye su principal ventaja teórica desde el punto de vista de seguridad.



Arquitectura de distribución cuántica de claves (QKD) y procesamiento criptográfico clásico extremo a extremo[58].

En los últimos años, QKD ha evolucionado desde entornos de laboratorio hasta despliegues operativos reales en redes estratégicas y proyectos piloto, especialmente en sectores de alta criticidad. No obstante, su adopción sigue siendo limitada debido a varios factores: costes elevados, complejidad técnica, restricciones de distancia, dependencia de hardware especializado y dificultades de escalado en entornos distribuidos o de Internet global.

[57] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (pp. 175–179)

[58] Aliro Quantum. (s. f.). Protocols for key distribution. https://www.aliroquantum.com/protocols-for-key-distribution

[59] European Commission. (2008). Totally secure network communication demonstrated. CORDIS—Community Research and Development Information Service. https://cordis.europa.eu/article/id/29965-totally-secure-network-communication-demonstrated

Desde el punto de vista de la estrategia post-quantum, es importante subrayar que QKD[59] no sustituye a la criptografía post-quantum (PQC). Mientras que PQC es una solución basada en software y altamente escalable, QKD es una tecnología basada en hardware, adecuada únicamente para contextos donde puede controlarse estrictamente la infraestructura física y el perímetro de seguridad.

En la práctica, el enfoque dominante es complementario: utilizar PQC como base criptográfica general y considerar QKD como una capa adicional en entornos muy específicos de alta seguridad, donde los requisitos de confidencialidad y los recursos disponibles justifican su complejidad y coste.

En consecuencia, QKD[60] debe evaluarse como una tecnología de nicho, potencialmente valiosa en escenarios concretos, pero no como un sustituto general de la transición hacia criptografía post-quantum basado en estándares abiertos y software-driven.

6.4. Integración de PQC en infraestructuras existentes

La integración de la criptografía post-quantum (PQC) en infraestructuras ya desplegadas debe abordarse de forma estratificada, atendiendo a las distintas capas técnicas que componen el entorno tecnológico. Este enfoque permite reducir el riesgo operativo, preservar la continuidad del servicio y adaptar el ritmo de transición a la criticidad y madurez de cada dominio.

Estrategias de integración por capas de infraestructura

1. Perímetro de red y capa de transporte

En el perímetro de red, la prioridad es proteger el tráfico en tránsito sin interrumpir los servicios existentes. En este nivel, la transición hacia PQC se materializa principalmente en los mecanismos de establecimiento de claves y autenticación.

Migración gradual de TLS

- Sustituir o complementar los conjuntos de cifrado dependientes de RSA o ECDHE por suites TLS 1.3 híbridas que incorporen intercambios de claves post-quantum, como ECDHE + ML KEM.
- Probar previamente el impacto en rendimiento, latencia e interoperabilidad en servidores web, proxies, balanceadores de carga y pasarelas API, siguiendo las recomendaciones del IETF PQUIP y ENISA.

[60] Geng, M. (2025). Advances of quantum key distribution and network nonlocality. Entropy, 27(9), 950. https://doi.org/10.3390/e27090950

VPN y comunicaciones seguras

- Actualizar pasarelas VPN para soportar intercambios de claves y certificados híbridos que integren algoritmos post-quantum.
- Priorizar las comunicaciones que protegen datos de larga duración o altamente sensibles, donde el riesgo de ataques Harvest Now, Decrypt Later es mayor.

2. Infraestructura de clave pública (PKI)

Las infraestructuras de clave pública constituyen el núcleo de la identidad digital y uno de los elementos más críticos de la transición post-quantum.

PKI híbrida

- Diseñar PKI capaces de emitir certificados que incluyan claves clásicas y post-quantum, conforme a los desarrollos normativos sobre certificados híbridos X.509.
- Ajustar políticas de certificación, perfiles de certificados y periodos de validez teniendo en cuenta el mayor tamaño de claves y firmas post-quantum.

Actualización de autoridades de certificación

- Planificar la migración de autoridades raíz e intermedias mediante esquemas de coexistencia y certificación cruzada.
- Documentar procedimientos de renovación y revocación masiva de certificados a medida que se adopten nuevos estándares.

3. Aplicaciones, servicios y datos en reposo

La integración de PQC impacta directamente en aplicaciones de negocio, servicios digitales y mecanismos de protección de datos en reposo.

Capa de aplicación

- Revisar las bibliotecas criptográficas utilizadas en aplicaciones web, móviles y microservicios, y sustituirlas por librerías que implementen algoritmos post-quantum estandarizados por el NIST.
- Validar la compatibilidad funcional y el impacto en rendimiento en entornos de prueba antes del despliegue.

Datos en reposo

- Evaluar la conveniencia de introducir algoritmos post-quantum en mecanismos de cifrado de bases de datos, copias de seguridad y cifrado de discos, especialmente cuando se emplea criptografía de clave pública para la gestión de claves.

4. Sistemas integrados, OT e IoT

Los entornos industriales, sistemas embebidos y dispositivos IoT presentan retos específicos debido a sus limitaciones técnicas y largos ciclos de vida.

Restricciones de hardware

- Muchos dispositivos carecen de recursos suficientes para implementar directamente algoritmos PQC intensivos en cómputo o memoria.
- Es necesario evaluar impacto en latencia y consumo y priorizar algoritmos optimizados para dispositivos de bajas prestaciones.

Ciclos de vida prolongados

- Los sistemas con ciclos de vida de 10–20 años requieren estrategias específicas, como el uso de pasarelas seguras, mecanismos híbridos en puntos de agregación y actualizaciones OTA planificadas.
- La planificación de adquisición de hardware compatible con PQC debe iniciarse con antelación, incluso cuando el despliegue efectivo se prevea a varios años vista.

Rol de los proveedores, estándares y proyectos de I+D

La transición a PQC depende en gran medida del ecosistema tecnológico y de la evolución de estándares y productos.

Colaboración con proveedores

- Recopilar y mantener información sobre versiones de productos, firmware y servicios con soporte PQC, incorporando requisitos explícitos en contratos y procesos de compra.
- Validar las implementaciones de proveedores mediante pruebas de laboratorio y proyectos piloto, verificando interoperabilidad y rendimiento.

Estándares y grupos de trabajo

- Seguir de forma continuada las recomendaciones de organismos de estandarización y marcos regulatorios sectoriales (NIST, ETSI, ENISA), que están publicando guías específicas de preparación para PQC.
- Considerar la integración de PQC con otras tecnologías cuánticas seguras, como QKD, en arquitecturas híbridas y de alcance limitado.

Proyectos y convocatorias

- Aprovechar iniciativas europeas orientadas a la transición de infraestructuras criptográficas, que proporcionan financiación, marcos de referencia y plataformas de validación tecnológica.
- En el ámbito industrial, desarrollar pilotos en entornos controlados con métricas de rendimiento y estrategias de despliegue progresivo.

6.5. Gestión de proveedores y contratos

En los últimos años, QKD ha evolucionado desde entornos de laboratorio hasta despliegues operativos reales en redes estratégicas y proyectos piloto, especialmente en sectores de alta criticidad. No obstante, su adopción sigue siendo limitada debido a varios factores: costes elevados, complejidad técnica, restricciones de distancia, dependencia de hardware especializado y dificultades de escalado en entornos distribuidos o de Internet global.

Desde el punto de vista de la estrategia post-quantum, es importante subrayar que QKD[59] no sustituye a la criptografía post-quantum (PQC). Mientras que PQC es una solución basada en software y altamente escalable, QKD es una tecnología basada en hardware, adecuada únicamente para contextos donde puede controlarse estrictamente la infraestructura física y el perímetro de seguridad.

Clasificación de proveedores

El primer paso es clasificar los proveedores según su importancia en cuanto al impacto en post-quantum y el papel que desempeñan en la protección de la información. A continuación, se propone una clasificación en siete niveles:

Nivel	Tipo de proveedor	Riesgo
1 - Crítico	Gestiona directamente claves de seguridad o certificados digitales	Muy alto
2 - Muy alto	Transporta y/o almacena información sensible cifrada	Alto
3 - Medio-alto	Almacena datos a largo plazo en formato cifrado	Medio-alto
4 - Medio	Suministra el software y las librerías con funciones de cifrado	Medio
5 - Bajo	No utiliza información sensible que precise de cifrado	Bajo

Esta clasificación permite priorizar esfuerzos y aplicar controles proporcionales al riesgo real que introduce cada proveedor.

Caracterización de proveedores

Antes de contratar o renovar el contrato con un proveedor, es necesario realizar una serie de preguntas sobre su nivel de preparación frente a la amenaza cuántica. No se trata de un examen técnico imposible, sino de verificar que el proveedor es consciente del riesgo y tiene un plan para afrontarlo.

A continuación, se proponen una serie de preguntas para ello:

- ¿Dispone de un inventario actualizado de todos los sistemas de cifrado que utiliza?
- ¿Conoce la tecnología post-quantum y tiene identificados los riesgos y retos que supone?
- ¿Ha analizado qué ocurriría con su servicio si los algoritmos de cifrado actuales quedaran obsoletos?
- ¿Tiene un plan concreto, con fechas, para migrar a los nuevos estándares de cifrado post-quantum?
- ¿Sus sistemas permiten actualizar el cifrado sin rediseñar toda la arquitectura tecnológica?
- ¿Qué política tiene sobre cuánto tiempo conserva datos cifrados de sus clientes?
- ¿Qué procedimientos tiene para detectar y reportar en menos de 24 una vulnerabilidad grave en sus sistemas de cifrado?

Las respuestas a estas preguntas permiten asignar una puntuación de madurez al proveedor, desde el nivel cero, sin conciencia del problema, hasta el nivel cinco, migración completada y procesos de mejora continua. Esta puntuación nos servirá para tomar decisiones como a qué proveedor contratar, los compromisos a exigir compromisos y dónde concentrar los esfuerzos de seguimiento.

Un proveedor que no conoce su propio riesgo criptográfico no puede gestionarlo. La primera pregunta que hay que hacerle es si es consciente del mismo.

Qué incluir en los contratos

Los contratos con proveedores deben reflejar las exigencias de seguridad necesarias para asegurar que en la era post-quantum el proveedor no genera riesgos en la cadena de suministro. Se recomienda incorporar al menos cláusulas relacionadas con cuatro aspectos clave:

Cláusula	Qué exige	Para qué sirve
Transparencia e inventario criptográfico	Disponer y entregar anualmente un inventario de todos los sistemas de cifrado en uso	Conocer qué tecnología usa el proveedor y si están preparadas para la era post-quantum
Roadmap de migración	Disponer y compartir un plan concreto de transición a cifrado post-cuántico, con fechas e hitos verificables	Garantiza que el proveedor tiene un camino trazado, no solo buenas intenciones
Notificación de vulnerabilidades	Comunicar en menos de 24 horas cualquier vulnerabilidad grave en sus sistemas de cifrado	Permite a la empresa reaccionar a tiempo ante un riesgo o incidente
Derecho de auditoría	Autorizar a la empresa a verificar, una vez al año, el estado real de la seguridad criptográfica del proveedor	Evita que los compromisos contractuales queden solo sobre el papel

Estas cláusulas deben acompañarse de consecuencias contractuales efectivas, como plazos de corrección, penalizaciones o derecho de resolución en situaciones críticas.

Un contrato sin cláusulas de seguridad criptográfica es un contrato incompleto en la era post-quantum.

Seguimiento

La gestión contractual es solo el punto de partida. Para que resulte eficaz, debe existir un proceso continuo de seguimiento, que incluya validación inicial, revisiones periódicas y alertas ante cambios relevantes.

Cuando un proveedor no asume compromisos adecuados, se recomienda una estrategia de escalada progresiva: concienciación, establecimiento de hitos contractuales, búsqueda de alternativas o aceptación formal del riesgo residual por parte de la alta dirección.

Lo que no se revisa periódicamente acaba quedando solo sobre el papel.

6.6. Planes de contingencia y respuesta ante incidentes

Aunque muchas organizaciones disponen de planes de gestión de incidentes consolidados, la criptografía post-quantum introduce tipos de incidentes, temporalidades e impactos que no quedan plenamente cubiertos por los enfoques tradicionales y que requieren adaptaciones específicas.

El elemento diferencial es que algunos incidentes criptográficos pueden tener efectos retroactivos, como los ataques Harvest Now, Decrypt Later, donde la recopilación de información se produce hoy, pero el daño se materializa años después, cuando ya no existe capacidad de mitigación técnica.

Tipos de incidentes criptográficos post-quantum

No todos los incidentes relacionados con la criptografía post-quantum son iguales. Se pueden agrupar en las siguientes categorías por su naturaleza:

Tipo	Descripción	Cuándo puede ocurrir
Recolección y descifrado diferido (Harvest now, decrypt later)	Un adversario acumula hoy información cifrada de la empresa para descifrarla en el futuro, cuando la tecnología post-quantum lo permita	Ya está ocurriendo aunque el impacto llegará unos años
Vulnerabilidad en el nuevo cifrado	Se descubre un fallo de seguridad en los propios algoritmos de cifrado post-cuántico, una vez implantados	Puede ocurrir en cualquier momento
Error en la transición tecnológica	Durante el proceso de migración al nuevo cifrado, se introduce un error que debilita la seguridad en lugar de reforzarla	Durante el período de transición
Obsolescencia acelerada de un algoritmo	Un avance científico hace que un algoritmo de cifrado quede vulnerable antes de lo previsto	A corto o medio plazo
Compromiso de un proveedor de cifrado	Uno de los proveedores que gestiona claves o certificados sufre una brecha de seguridad	Puede ocurrir en cualquier momento
Ataque a la nueva infraestructura	Una vez implantado el nuevo cifrado post-cuántico, un atacante consigue explotar vulnerabilidades del nuevo sistema	A medio plazo

El tipo de incidente más difícil de gestionar es el primero: HNDL. Por eso, la mejor respuesta es preventiva: migrar al nuevo cifrado antes de que existan ordenadores cuánticos capaces de causar ese daño y asumir que esto pasará.

Algunos incidentes post-quantum ya están ocurriendo, aunque sus consecuencias no se vean todavía. Actuar hoy es la única forma de prevenirlos.

Preparar la respuesta

Cuando se produce un incidente de seguridad criptográfica, el tiempo es un factor crítico. Por eso, antes de que ocurra nada, la organización necesita tener preparada una estructura de respuesta específica.

Se propone crear un equipo de respuesta a incidentes criptográficos —al que se pueden llamar equipo CIRT, de sus siglas en inglés— que funcione como una extensión especializada del equipo de seguridad habitual. Este equipo no necesita estar siempre activo, pero sí tener los roles definidos, los procedimientos escritos y los contactos actualizados.

Perfil en el equipo	Qué aporta
Persona responsable del incidente (Dirección de Seguridad)	Toma decisiones, coordina con la dirección y se comunica con los reguladores
Especialista técnico en criptografía post-quantum	Analiza el impacto técnico y dirige la solución
Especialista en certificados y claves digitales	Gestiona la revocación de certificados comprometidos y la emisión de nuevos
Arquitectura de seguridad	Conoce la tecnología de la empresa y puede evaluar qué sistemas se ven afectados
Área jurídica y cumplimiento normativo	Determina qué hay que notificar y a quién, y en qué plazos
Comunicación corporativa	Gestiona los mensajes hacia clientes, medios y empleados si el incidente trasciende
Enlace con proveedores	Activa los planes de respuesta conjunta con los proveedores afectados

Un equipo de respuesta que no se conoce, no ha practicado y no tiene los procedimientos escritos no es un equipo de respuesta: es una lista de nombres.

Cómo actuar al inicio de una crisis

Cuando se produce un incidente de seguridad criptográfica, el tiempo es un factor crítico. Por eso, antes de que ocurra nada, la organización necesita tener preparada una estructura de respuesta específica.

Se propone crear un equipo de respuesta a incidentes criptográficos (al que se pueden llamar equipo CIRT, de sus siglas en inglés) que funcione como una extensión especializada del equipo de seguridad habitual. Este equipo no necesita estar siempre activo, pero sí tener los roles definidos, los procedimientos escritos y los contactos actualizados.

Momento	Acciones prioritarias
Primeras cuatro horas	Se activa el equipo de respuesta. Se convoca una reunión de crisis con la Dirección de Seguridad, la Dirección de Tecnología, la Dirección de Riesgos y la Asesoría Jurídica. Se evalúa qué datos podrían estar en riesgo consultando el inventario de cifrado. Se informa de forma preliminar a la Dirección General y al Consejo de Administración.
De 4h a 24h	Se aceleran todas las migraciones pendientes al nuevo cifrado. Se inicia la rotación de las claves más expuestas. Si el incidente es grave y la empresa está sujeta a obligación de notificación, se envía la notificación inicial al supervisor regulatorio correspondiente. Se contacta con los proveedores críticos para activar sus propios planes de contingencia.
Días dos a siete	Se ejecuta el plan de migración de emergencia en los sistemas más críticos. Se revisan los datos más sensibles para evaluar el impacto real. Se envía el reporte intermedio al supervisor regulatorio.
Semanas dos a cuatro	Se completa la migración. Se realiza una auditoría del incidente para extraer lecciones aprendidas. Se actualiza el inventario de cifrado y los planes de contingencia. Se envía el reporte final al supervisor.

En una crisis criptográfica, cada hora sin respuesta es una hora en que el riesgo crece. La preparación previa es lo que hace posible actuar con rapidez y orden.

Comunicación durante una crisis

Uno de los errores más habituales en la gestión de crisis tecnológicas es comunicar de la misma forma a audiencias muy diferentes. Un mensaje técnico detallado puede ser necesario para el equipo de ingeniería, pero resulta incomprensible, y contraproducente, para un cliente o para un actor externo.

La regla de oro es traducir siempre el impacto a términos concretos y comprensibles: qué datos pueden verse afectados, qué operaciones están interrumpidas y cuándo se espera recuperar la normalidad. Cada audiencia necesita una respuesta diferente:

A quién	Cuándo	Qué comunicar
Dirección General y Comité de Dirección	En las primeras dos horas	Qué ha ocurrido, cuál es el impacto potencial, qué se está haciendo y qué decisiones/recursos se necesitan
Consejo de Administración	En las primeras cuatro horas (resumen) y a los dos días (informe completo)	Impacto para el negocio y la reputación, acciones en marcha y decisiones que requieren aprobación
Organismos supervisores si aplican	Según los plazos en cada caso	Descripción del incidente, alcance, medidas adoptadas y evolución y reporte continuo
Proveedores afectados	En las primeras cuatro horas	Activación del plan de respuesta conjunto y compromisos de actuación inmediata
Empleados	Si es necesario, a las ocho horas	Instrucciones operativas claras, qué evitar y cómo escalar dudas y problemas
Clientes afectados	Si hay obligación o se considera necesario	Qué ha ocurrido, qué datos están implicados, qué está haciendo la persona y como impacta al cliente

Comunicar bien en una crisis no significa comunicar mucho ni poco: significa comunicar lo correcto, a la persona adecuada, en el momento oportuno.

Ejercicios de preparación y práctica

Cualquier plan de contingencia es susceptible a fallos, por ello es imprescindible que se pruebe de forma recurrente para detectar problemas y mejoras. Por eso, la preparación ante incidentes criptográficos incluye ejercicios periódicos que permiten identificar fallos en los procedimientos antes de que se produzca una crisis real.

Se recomiendan al menos cuatro tipos de ejercicios, con distinta frecuencia e intensidad:

Table top (semestral): ejercicio teórico de cómo respondería la empresa ante un escenario hipotético de incidente. No se usan sistemas reales. El objetivo es identificar dudas, vacíos en los procedimientos y problemas de coordinación.

Simulacro de notificación y comunicación (trimestral): se prueba que el árbol de comunicación funciona y que los plazos de notificación regulatoria son alcanzables.

Simulación técnica (anual): se reproduce en un entorno de pruebas un escenario de compromiso criptográfico real: por ejemplo, revocación masiva de certificados, rotación de claves, activación de algoritmos de emergencia, etc.

Simulacro completo (cada dos años): se combina todo lo anterior en un ejercicio integral que pone a prueba la respuesta de toda la organización, desde el equipo técnico hasta la comunicación con clientes y reguladores si aplica.

En muchos casos, la alerta que genera el incidente no es pública ni incluye aún toda la información. Las preguntas que el ejercicio debe responder son: ¿qué datos de la empresa están en riesgo? ¿Quién toma las decisiones? ¿Qué se comunica y a quién? ¿Cuánto tardaría la empresa en activar el cifrado post-quantumen sus canales más críticos?

Los ejercicios de simulación no son un gasto de tiempo: son la inversión imprescindible para garantizar que la respuesta a una crisis funcione.

Lo mínimo que hay que tener listo en 2026

A modo de resumen práctico, estas son las recomendaciones que una empresa debe tener operativas en 2026 para responder con eficacia ante un incidente criptográfico post-cuántico:

Capacidad	En qué consiste	Esfuerzo estimado
Inventario de cifrado actualizado	Saber qué tecnología de cifrado se usa en cada sistema y qué proveedor la gestiona	Medio
Equipo de respuesta identificado y con procedimientos escritos	Tener claros los roles, los contactos y los pasos a seguir ante cada tipo de incidente	Bajo
Plan de notificación y comunicación externa e interna	Tener preparadas las plantillas y los contactos para notificar	Bajo
Al menos un ejercicio de simulación en los últimos 12 meses	Haber practicado la respuesta ante un escenario hipotético de crisis criptográfica	Bajo
Cláusulas de seguridad post-quantum en los contratos con proveedores críticos	Haber incorporado las exigencias de transparencia, hoja de ruta y notificación en los contratos más importantes	Medio
Secreto perfecto hacia adelante en todos los canales externos	Garantizar que el tráfico cifrado de hoy no podrá ser descifrado en el futuro, aunque se rompa la clave actual y en caso de que se rompa, que el acceso a dicha información no supondrá un riesgo para la empresa	Bajo
Presupuesto de emergencia preaprobado	Disponer de una reserva económica aprobada por el Consejo de Administración para actuar con rapidez si se produce una crisis	Alto

El mensaje más importante que la Dirección de Seguridad debe trasladar al Consejo de Administración es sencillo: prepararse hoy para la amenaza cuántica es mucho más barato que gestionar una crisis cuando esa amenaza se materialice. El coste de la prevención es predecible; el coste de una brecha de seguridad masiva, no.

La pregunta no es si la amenaza cuántica llegará, sino si la organización estará lista cuando llegue. Esa preparación empieza ahora.

7. Oportunidades y Beneficios del Post-Quantum

Una vez revisados los riesgos que presenta el nuevo escenario Post-Quantum para las organizaciones, toca abordar las ventajas que para toda organización tiene abordar dicho escenario de forma proactiva y con la debida antelación.

7.1. Fortalecimiento de la resiliencia organizacional

La PQC fortalece de manera directa la resiliencia organizacional, entendida como la capacidad de proteger la confidencialidad, integridad, autenticidad y disponibilidad de la información frente a cambios estructurales en el entorno tecnológico y de amenazas. A diferencia de enfoques reactivos, la preparación post-quantum permite a la organización anticipar escenarios de ruptura criptográfica[61] y gestionarlos de forma ordenada, reduciendo la probabilidad de interrupciones graves o migraciones de emergencia.

Desde una perspectiva regulatoria, marcos como DORA reconocen explícitamente que los controles criptográficos son elementos esenciales para la resiliencia operativa digital, y exigen un enfoque flexible, basado en el riesgo, capaz de adaptarse a un entorno dinámico[62]. En este contexto, la transición post-quantum convierte la seguridad criptográfica en una capacidad evolutiva y gobernable, superando la rigidez de dependencias tecnológicas heredadas.

Uno de los beneficios más tempranos de este proceso es la incorporación efectiva de la cripto-agilidad. Tal y como la define el NIST, la cripto-agilidad es la capacidad de sustituir algoritmos criptográficos en protocolos, aplicaciones y arquitecturas sin interrumpir el funcionamiento del sistema. Al integrar esta capacidad en el diseño y la planificación tecnológica, la organización no solo se prepara para la amenaza cuántica, sino que mejora su capacidad general de adaptación frente a cualquier cambio disruptivo en el panorama criptográfico.

La resiliencia también se ve reforzada mediante una mejora sustancial de la visibilidad operativa. El inventariado de activos criptográficos obliga a identificar algoritmos, claves, certificados, bibliotecas y dependencias con terceros. Tal y como señalan las guías del NCSC de los Países Bajos, este nivel de visibilidad no solo es imprescindible para la transición a PQC, sino que constituye una base sólida para una gestión avanzada de activos y para el cumplimiento de requisitos como los establecidos por la Directiva NIS2 en materia de seguridad de la cadena de suministro.

Finalmente, la agenda post-quantum ofrece una oportunidad clara desde el punto de vista del gobierno corporativo. La exigencia de NIS2 de que los órganos de dirección supervisen activamente la ciberseguridad permite al CISO elevar la conversación desde decisiones técnicas aisladas hacia un marco de gestión del riesgo alineado con la estrategia de negocio. En este sentido, la preparación post-quantum no añade rigidez, sino que sustituye una seguridad estática por una resiliencia evolutiva, fortaleciendo la disciplina de protección y la capacidad de adaptación de la organización desde el presente[63].

7.2. Ventaja competitiva y diferenciación en el mercado

La adopción anticipada de PQC constituye una ventaja competitiva real, especialmente en mercados donde la confianza, la continuidad del servicio y la seguridad son factores críticos de diferenciación. Frente a enfoques reactivos centrados en el cumplimiento mínimo, las organizaciones que inician antes su transición se posicionan como actores maduros, previsores y fiables.

En el entorno europeo, esta ventaja se ve reforzada por la hoja de ruta coordinada impulsada por la Comisión Europea, con hitos definidos para 2026, 2030 y 2035. Aunque marcos como NIS2 o DORA no imponen todavía una migración obligatoria a PQC, sí generan un contexto que premia la gestión rigurosa de activos, el control de dependencias y la resiliencia operativa. Las organizaciones que ya han avanzado en inventariado, pruebas y planificación llegan mejor posicionadas a auditorías, homologaciones y licitaciones.

La ventaja competitiva no se limita al cumplimiento anticipado. La preparación post-quantum permite alinear la transición criptográfica con los ciclos naturales de renovación tecnológica, reduciendo costes asociados a cambios urgentes y simplificando la relación con proveedores y terceros mediante criterios objetivos de evaluación.

En sectores regulados o de alta exigencia en materia de confianza, la capacidad de demostrar una hoja de ruta post-quantum coherente y verificable refuerza la credibilidad institucional y reduce fricciones con supervisores y socios comerciales. Para el CISO, el escenario post-quantum ofrece así la oportunidad de liderar un cambio estructural antes que el mercado, transformando una obligación futura en una ventaja presente.

[61] Cybersecurity and Infrastructure Security Agency. (2024). Quantum readiness: Migration to post-quantum cryptography. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[62] European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[63] Fierce Network. (2025). Quantum without hype: Making security real before Q Day. https://www.fierce-network.com/broadband/quantum-without-hype-making-security-real-q-day

7.3. Mejora de la confianza de clientes y stakeholders

La gestión proactiva del riesgo asociado a la computación cuántica refuerza de forma directa la confianza de clientes y demás partes interesadas. En el entorno digital actual, dicha confianza no se basa en declaraciones genéricas de seguridad, sino en la capacidad de la organización para demostrar un gobierno del riesgo sólido, verificable y alineado con estándares reconocidos.

Desde la perspectiva del CISO, la credibilidad ante clientes, organismos reguladores, entidades auditoras e inversores se construye a partir de evidencias concretas. La hoja de ruta europea para la transición post-quantum vincula este proceso con la continuidad de los servicios críticos y la seguridad de la cadena de suministro, situando la confianza en la capacidad de identificar datos de larga vida, localizar criptografía vulnerable y gestionar dependencias tecnológicas y de terceros.

La fiabilidad percibida aumenta cuando la preparación post-quantum se integra en disciplinas ya sujetas a auditoría y supervisión, como las exigidas por DORA o la Directiva NIS2. En este marco, medidas de "mínimo arrepentimiento", como el inventario criptográfico exhaustivo o la definición de planes de migración verificables, reducen la incertidumbre futura y evitan decisiones improvisadas.

Desde la perspectiva del Consejo de Administración, este enfoque permite transformar una amenaza tecnológica abstracta en un programa de gestión del riesgo comprensible y auditable, reforzando la confianza de clientes y stakeholders desde el presente.

7.4. Innovación en procesos y tecnologías

La transición a PQC no es solo una obligación técnica; es una palanca para modernizar procesos, acelerar la innovación y mejorar la resiliencia en toda la organización.

Las oportunidades en cuanto a procesos se resumen en:

- Refuerzo de confianza de clientes y reguladores
- Time-to-market más corto en productos y servicios
- Cumplimiento y auditoría mejorados
- Gestión de riesgos de terceros más sólida
- Ventaja competitiva para los que empiezan antes

Las oportunidades en cuanto a tecnología se resumen en:

- Modernizar la base criptográfica con estándares comunes
- Automatizar el inventario y ganar visibilidad
- Anclar la migración a marcos de control (menos esfuerzo de auditoría)
- Mejorar la seguridad del software (code-signing y firmware)
- Diseñar con cripto-agilidad (cambiar sin rehacerlo todo)
- Transición segura con modos híbridos (clásico + PQC)
- Gobernanza con CBOM/SBOM
- Gestión de proveedores con criterios objetivos
- Nuevos servicios en redes e IoT

7.5. Casos de éxito y buenas prácticas internacionales

En el escenario de 2026, los casos de éxito en criptografía post-quantum se caracterizan por la ejecución temprana de despliegues híbridos, pilotos sectoriales y avances en certificación, que demuestran la viabilidad técnica y operativa de la transición.

A. Referentes institucionales y marcos de colaboración en Europa

La Comisión Europea y el Grupo de Cooperación de la Directiva NIS han definido una hoja de ruta común con hitos en 2026, 2030 y 2035, proporcionando un marco estable para la planificación organizativa. Iniciativas impulsadas por organismos nacionales como ANSSI (Francia), el binomio AIVD–NCSC (Países Bajos) o el CCN (España) han convertido la amenaza cuántica en guías prácticas de gestión del riesgo, favoreciendo una adopción anticipada y coordinada.

B. Infraestructuras habilitadoras y servicios en la nube

Una tendencia clave es la adopción de la protección post-quantum como servicio, donde proveedores encapsulan mecanismos híbridos en capas de infraestructura. En este ámbito, Cloudflare y Nokia han documentado despliegues a gran escala con acuerdos de clave híbridos, mientras que proveedores cloud como Google Cloud, AWS y Netskope ya incorporan soporte para mecanismos KEM en servicios de gestión de claves. La experiencia demuestra que la transición resulta más eficaz cuando se inicia con esquemas híbridos y despliegues controlados.

En paralelo, fabricantes como Thales y Utimaco avanzan en la integración de PQC en HSM, trasladando el foco desde el algoritmo hacia la gobernanza de las raíces de confianza.

C. Seguridad en el dispositivo y sistemas industriales

La protección post-quantum ha descendido hasta el nivel del chip y los sistemas embebidos, garantizando la resiliencia en entornos de IoT y OT.

Microelectrónica (Infineon y NXP): se han alcanzado certificaciones de nivel superior (EAL6) para la implementación de PQC en controladores de seguridad. Esto asegura funciones críticas como el arranque seguro (secure boot), la identidad del dispositivo y las actualizaciones de firmware en campo.

D. Referentes en España

El ecosistema español presenta casos de uso avanzados en sectores de alta sensibilidad regulatoria.

En el sector financiero, el proyecto PIQASO (CaixaBank) constituye un caso pionero en banca móvil (2025 2027), evaluando encapsulación de claves, firmas digitales y protección de datos a largo plazo en canales transaccionales.

La participación de Santander como miembro fundador del *Quantum-Safe* Financial Forum de Europol (EC3) subraya la relevancia de la coordinación sectorial y la presión conjunta sobre la cadena de suministro.

Por su parte, BBVA impulsa foros de transferencia de conocimiento, como Bizkaia BBVA Banks in Quantum Days, consolidando el debate estratégico sobre la aplicación real de estas tecnologías.

E. Iniciativas de ciberseguridad nacional

Objetivo de la estrategia española	Acción para las empresas	Impacto esperado 2030
Consolidación del ecosistema	Participación en consorcios público-privados y hubs cuánticos.	España como referente europeo en talento y tecnología cuántica.
Preparación de la sociedad	Formación de talento interno en algoritmos PQC y cripto-agilidad.	Reducción de la brecha de habilidades cuánticas.
Investigación y I+D+i	Colaboración con universidades para pilotos de casos de uso reales.	Transferencia de conocimiento del laboratorio al mercado.
Mercado español cuántico	Adopción de soluciones de startups cuánticas locales.	Soberanía digital y resiliencia en la cadena de suministro.

Objetivos de la estrategia española post-quantum y su impacto para las empresas

En conjunto, estos casos muestran un patrón común: el éxito no reside en migraciones masivas inmediatas, sino en avanzar mediante pilotos controlados, despliegues híbridos y colaboración institucional, permitiendo una transición post-quantum ordenada y sostenible.

8. Integración de la Gestión de Riesgos PQC en el Gobierno Corporativo

8.1. Rol del CISO y la Alta Dirección

La gestión del riesgo post-quantum marca una evolución clara del papel de la ciberseguridad en el gobierno corporativo. La criptografía deja de ser un asunto puramente técnico para convertirse en un elemento estructural que afecta a la protección de la información a largo plazo, la resiliencia operativa, la dependencia de terceros y la continuidad del negocio. En este contexto, el riesgo post-quantum debe ser tratado como un riesgo estratégico y no como una cuestión tecnológica aislada.

El CISO desempeña un papel central en esta transición. Su función consiste en traducir la complejidad técnica del escenario post-quantum en decisiones comprensibles para la Alta Dirección, integrando el riesgo criptográfico en los marcos corporativos de gestión del riesgo, inversión y planificación. Tal y como recoge el III Libro Blanco del CISO[64], su rol no se limita a la supervisión de controles, sino que actúa como asesor estratégico, facilitador del gobierno del riesgo y punto de conexión entre tecnología y negocio.

En este ámbito, el liderazgo del CISO exige anticipación más que reacción. El reto principal no reside en la fecha exacta en la que una capacidad cuántica madure hasta comprometer los algoritmos actuales, sino en el tiempo necesario para identificar dependencias criptográficas, planificar la migración y ejecutar los cambios de forma ordenada. Las prioridades de ejecución y las líneas de actuación concretas para el horizonte 2026 se desarrollan en el Capítulo 9.

La Alta Dirección, por su parte, no necesita dominar los detalles técnicos de la criptografía post-quantum, pero sí asumir su responsabilidad en la supervisión del riesgo. Esto implica dar prioridad al asunto, exigir información estructurada sobre el nivel de exposición, validar la coherencia del plan de transición y asegurar la asignación de los recursos necesarios. En riesgos de maduración lenta como este, la inacción no reduce el riesgo: lo traslada al futuro con mayor impacto y coste.

La madurez organizativa frente al desafío post-quantum depende, en última instancia, de la calidad de la relación entre el CISO y la Alta Dirección. Cuando existe alineamiento, mandato y continuidad ejecutiva, el riesgo PQC se integra de forma natural en el gobierno corporativo y deja de ser una preocupación técnica difusa para convertirse en una responsabilidad gestionada al máximo nivel.

[64] ISMS Forum. (2026). Libro Blanco del CISO: Evolución del rol, responsabilidades y gobierno de la seguridad. https://www.ismsforum.es/ficheros/descargas/lbdelciso1776574974.pdf

8.2. Comunicación efectiva del riesgo post-quantum al Board

La comunicación del riesgo post-quantum al Consejo de Administración no puede abordarse desde un enfoque técnico. El objetivo de este apartado no es volver a explicar la naturaleza de la computación cuántica ni detallar fundamentos criptográficos ya tratados en capítulos anteriores, sino traducir un riesgo estructural de largo plazo en términos comprensibles, supervisables y accionables para el Board.

En este contexto, la preparación post-quantum debe presentarse como un asunto de gobernanza, alineado con la gestión de riesgos sistémicos, la protección del valor a largo plazo y la responsabilidad fiduciaria del órgano de dirección.

La economía cuántica: contexto mínimo para la toma de decisiones

La denominada economía cuántica ha entrado en una fase de maduración acelerada que afecta directamente a sectores de misión crítica. Para el Consejo, no es relevante el detalle técnico, sino entender qué componentes de esta evolución tienen impacto directo en negocio y en horizontes temporales concretos.

Dimensión de la tecnología cuántica	Impacto en el negocio	Horizonte de madurez
Computación cuántica	**Optimización de carteras, simulación molecular, criptoanálisis.**	2027 - 2030+
Comunicación cuántica	**Transferencia segura de información, quantum key distribution (QKD).**	2024 – 2026 (adopción temprana)
Sensing cuántico	**Mediciones de alta precisión (gravedad, tiempo), diagnósticos médicos.**	2025 - 2028
Criptografía post-quantum	**Protección de datos frente a ataques cuánticos mediante algoritmos resistentes.**	2024 (estándares NIST) - 2029 (migración crítica)

Narrativa de riesgo para el Board: confidencialidad a largo plazo

Para una comunicación eficaz, el riesgo post-quantum debe vincularse directamente a la confidencialidad futura de activos estratégicos. No se trata de un riesgo hipotético: afecta a datos cuya pérdida de confidencialidad dentro de cinco, diez o veinte años tendría consecuencias irreversibles para la organización.

Desde la perspectiva del Board, el foco debe situarse en: propiedad intelectual, secretos industriales, información estratégica de negocio y datos personales o sanitarios con largos periodos de retención.

El mensaje clave es que la seguridad de la información no es estática, y que decisiones técnicas tomadas hoy condicionan la exposición futura de esos activos. Este enfoque permite al Consejo entender el riesgo post-quantum como una cuestión de ciclo de vida del dato y no como una apuesta tecnológica.

El caso de negocio: del coste técnico al ROI de resiliencia

La inversión en preparación post-quantum no debe presentarse únicamente como un coste de cumplimiento, sino como una inversión en resiliencia y reducción de deuda criptográfica. A nivel de dirección, el retorno debe entenderse como evitación de pérdidas futuras y mejora de la capacidad de adaptación.

Indicador de negocio	Impacto de la preparación PQC	Fuente de valor / ROI
Primas de ciberseguro	**Reducción de hasta un 50% en el incremento proyectado de primas.**	Evitación de costes por mayor postura de riesgo.
Cumplimiento regulatorio	**Evitación de multas de hasta el 2% de la facturación global (NIS2/GDPR).**	Continuidad operativa y legal.
Confianza del cliente	**Diferenciación competitiva mediante el sello de "Privacidad Post-quantum".**	Retención de clientes y nuevos mercados.
Resiliencia operativa	**Reducción del tiempo de inactividad por actualizaciones de certificados y claves.**	Eficiencia en procesos de IT y GRC.

Argumentario ejecutivo: mensajes clave para CEO y CFO

Para facilitar la comunicación en la próxima sesión del Consejo de Administración, se proponen los siguientes puntos de anclaje:

- **El "Día Q" no es una fecha, es una exposición presente:** Los adversarios ya están robando nuestros datos cifrados hoy (HNDL). Si la propiedad intelectual de la organización tiene un valor superior a cinco años, ya se está perdiendo valor frente a ataques futuros. La seguridad cuántica es una inversión en la protección de los ingresos futuros, no solo un gasto de IT.
- **Cumplimiento de DORA y NIS2[65] como seguro de continuidad:** Las multas por incumplimiento de resiliencia operativa y la responsabilidad personal de los directivos ya son una realidad legal. La preparación post-quantum es la evidencia más clara de una gestión de riesgos diligente y acorde con el "estado del arte".
- **La cripto-agilidad como ventaja competitiva:** No se migra sólo por miedo; sino con la idea de construir una infraestructura ágil que permitirá adoptar nuevas tecnologías y socios comerciales de manera segura. Ser "Quantum-Safe" será pronto un requisito para operar en sectores regulados y mercados globales.
- **Ahorro por evitación:** El coste del pánico vs. el coste del plan: Migrar ahora permite aprovechar los ciclos naturales de renovación tecnológica. Esperar a una vulnerabilidad crítica nos obligará a una migración de emergencia con costes exponenciales y riesgos operativos inaceptables (Efecto Y2Q).
- **Soledad del riesgo en la cadena de suministro:** Ninguna organización puede ser la única responsable de su seguridad. Debemos exigir transparencia cuántica a nuestros proveedores para evitar que un tercero vulnerable comprometa nuestra estabilidad sistémica.

[65] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

Fuentes estratégicas para la Dirección

Mantener una referencia estructurada de fuentes permite respaldar decisiones presupuestarias y estratégicas:

Título de la fuente	Autor / organización	Relevancia para el Board
Quantum technology monitor 2025	McKinsey & Co.[66]	Cuantifica el valor económico ($100B) y el impacto por industrias específicas.
Embracing the quantum economy (2024)	World Economic Forum[67]	Define la "Brecha Cuántica" y ofrece una visión de liderazgo ético y estratégico.
Quantum-safe readiness index (QSRI)	IBM Institute for Business Value[68]	Proporciona un marco de 14 indicadores para medir la madurez frente a la industria.
Hype cycle for digital identity 2025	Gartner[69]	Sitúa la autenticación post-quantum como una tendencia crítica con madurez emergente.
Microsoft digital defense report 2025	Microsoft[70]	Conecta la amenaza cuántica con la evolución real de los ciberataques de naciones-estado.
NIS2 & DORA PQC compliance guide	CryptoNext / ENISA[71]	Traducción directa de los artículos legales a requisitos de implementación técnica.
Estrategia de tecnologías cuánticas de España	Gobierno de España[72]	Marco de referencia para la soberanía digital y el cumplimiento nacional.
Quantum readiness for leaders	WEF (Industry Series)[73]	Guías específicas para manufactura, salud y finanzas con casos de uso reales.
The year of quantum: from concept to reality	McKinsey (2025)[74]	Analiza el cambio de qubits físicos a lógicos y su impacto en la seguridad.
Economic impact of quantum attacks	Hudson Institute[75]	Estudio de impacto macroeconómico (pérdida de PIB de $2T-$3T) que resuena con CFOs.

[66] McKinsey & Company. (2025). Quantum Technology Monitor 2025: The year of quantum. From concept to reality.

[67] World Economic Forum. (2024). Embracing the quantum economy: A pathway for business leadership and ethical readiness. https://www.weforum.org/publications/embracing-the-quantum-economy-a-pathway-for-business-leaders

[68] IBM Institute for Business Value. (2025). The quantum-safe readiness index: Measuring organizational preparedness for the post-quantum era. IBM Corporation. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-quantum-safe-readiness

[69] Gartner, Inc. (2025). Hype cycle for digital identity, 2025. Gartner. https://www.gartner.com/en/documents/6718134

[70] Microsoft. (2025). Microsoft digital defense report 2025. Microsoft Corporation. https://www.microsoft.com/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

[71] CryptoNext Security. (2025). DORA and NIS2: European requirements for post-quantum cryptography. CryptoNext Security. https://www.cryptonext-security.com/en/blog/dora-and-nis2-european-requirements-for-post-quantum-cryptography/

[72] Ministerio para la Transformación Digital y de la Función Pública. (2025). Estrategia de tecnologías cuánticas de España 2025–2030. Gobierno de España. https://espanadigital.gob.es/estrategia-de-tecnologias-cuanticas-de-espana

[73] World Economic Forum. (2024). Quantum readiness for leaders: Industry series.

[74] McKinsey & Company. (2025). The year of quantum: From concept to reality in 2025. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

[75] Butler, A. W., & Herman, A. (2023). Prosperity at risk: The quantum computer threat to the U.S. financial system. Hudson Institute. https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system

One pager para el Board (estructura recomendada)

Un informe de situación eficaz para el Consejo debe ser conciso, visual y orientado a la acción. A continuación, se detalla la estructura ideal:

1. Resumen ejecutivo (the bottom line)

- **Estado de alerta:** "Riesgo Sistémico Identificado". La computación cuántica compromete la confidencialidad a largo plazo de nuestros activos core (IP, Datos de Clientes)
- **Urgencia:** cumplimiento obligatorio de DORA/NIS2 para 2025. Riesgo HNDL activo sobre datos con retención superior a 5 años

2. Métricas clave de preparación (dashboard)

- **Inventario CBOM:** 45% completado (Objetivo 202[JP53.1]6: 100%)
- **Exposición de datos críticos:** 1.2 Terabytes identificados bajo riesgo HNDL
- **Madurez de proveedores:** 2 de 5 socios estratégicos han confirmado preparación PQC

3. Hitos del proyecto (Roadmap 2026)

- **Fase 1 (Descubrimiento):** finalización del inventario de certificados y claves (Q1 2026)
- **Fase 2 (Observabilidad):** evaluación de impacto de latencia y pruebas de compatibilidad híbrida (Q2 2026)
- **Fase 3 (Remediación):** inicio de migración de sistemas críticos de cara al cliente (Q4 2027)

4. Riesgos y dependencias

- **Talento:** brecha del 30% en perfiles con formación en criptografía avanzada
- **Proveedores:** dependencia de la actualización de firmas PQC por parte del proveedor de Cloud principal

5. Petición de decisión (The call to action)

- Aprobación de la partida presupuestaria para el "Centro de Excelencia Criptográfica"
- Inclusión de la "Cláusula de Preparación Cuántica" en todas las renovaciones de contratos de TIC de Nivel 1

Para el Consejo de Administración, el riesgo post-quantum no es un debate tecnológico sino una prueba de madurez del gobierno corporativo. Las organizaciones que actúan con antelación reducen incertidumbre, evitan decisiones precipitadas y preservan su capacidad de generar valor en un contexto de cambio estructural.

La transición post-quantum es, en esencia, una transformación de la infraestructura de confianza. Quienes lideren este proceso no solo mitigarán un riesgo futuro, sino que fortalecerán su posición como custodios fiables de la información en la economía digital que viene.

8.3. Alineamiento con el ERM y frameworks de gestión de riesgos

El alineamiento entre la Gestión de Riesgos Empresariales (Enterprise Risk Management, ERM) y un framework de gestión de riesgos en criptografía post-quantum (PQC) es un elemento crítico para integrar de forma efectiva los riesgos derivados de la transición criptográfica dentro de la estrategia global de la organización, en coherencia con los principios metodológicos y métricas ya definidos en el capítulo 5.1.

Este alineamiento no debe limitarse a la incorporación de un nuevo riesgo tecnológico aislado. Implica reconocer la criptografía como un riesgo sistémico y transversal, con impacto a largo plazo, e integrar los riesgos, amenazas y controles asociados a PQC dentro del framework corporativo de gestión de riesgos (ERM), así como en marcos ya consolidados de gestión del riesgo tecnológico, como NIST Cybersecurity Framework 2.0 o ISO 31000.

Integración de PQC en el ciclo ERM

Un primer paso en la integración de PQC en el ciclo Enterprise Risk Management (ERM) consiste en incorporar los riesgos asociados a PQC dentro de las categorías de riesgo ya existentes en el ERM, asegurando coherencia con el lenguaje y la estructura corporativa. Para ello, se pueden llevar a cabo las siguientes fases:

A) Identificación y contextualización

Es clave definir escenarios de riesgo PQC que conecten directamente con el impacto en el negocio. Entre ellos:

- Estratégicos: pérdida de ventaja competitiva o exposición futura de información sensible.
- Operacionales: fallos o interrupciones en sistemas debido a la obsolescencia criptográfica.
- Legales / Compliance: incumplimiento de futuras regulaciones o estándares de seguridad.
- Reputacionales: exposición de datos cifrados en la actualidad bajo el paradigma “harvest now, decrypt later”.

B) Priorización estratégica

El marco ERM debe utilizarse para priorizar la migración a PQC, especialmente en aquellos sistemas que gestionan información con larga vida útil o alta sensibilidad, maximizando así la eficiencia en la asignación de recursos.

C) Inventario y evaluación

Es necesario establecer una visión clara del riesgo mediante:

- Inventario de activos criptográficos CBOM
- Evaluación estructurada del riesgo mediante metodologías específicas como PQC-RA (Post-Quantum Cryptographic Risk Assessment)

Elementos clave para un framework conjunto ERM–PQC

Para una integración efectiva, la gestión del riesgo PQC debe articularse como un modelo conjunto que combine gobernanza, evaluación, seguimiento y mejora continua, evitando su tratamiento como un riesgo técnico aislado.

Gobernanza y cultura

- Definir roles y responsabilidades claras en la gestión de riesgos PQC.
- Integrar PQC dentro de la cultura de gestión de riesgos de la organización.

Conexión entre CISO, CRO y negocio

- Asegurar la coordinación entre áreas tecnológicas, de riesgos y de negocio.
- Elevar PQC a nivel estratégico, evitando su aislamiento en el ámbito técnico.

Evaluación y tratamiento del riesgo

- Aplicar metodologías homogéneas de evaluación de riesgos.
- Definir planes de tratamiento alineados con ERM: eliminar, mitigar, transferir o aceptar.

Seguimiento, reporting y mejora continua

- Integración natural del riesgo PQC en el ciclo ERM, de forma que:
  - la auditoría valide la eficacia del modelo,
  - el reporting proporcione visibilidad ejecutiva,
  - y la mejora continua permita su adaptación ante cambios tecnológicos y regulatorios.
- Revisión periódica del inventario criptográfico (CBOM), escenarios de riesgo y hojas de ruta de migración.
- Incorporación sistemática de lecciones aprendidas procedentes de auditorías, evaluaciones internas o ejercicios de simulación.

Alineamiento con el apetito de riesgo

- Definir explícitamente niveles de tolerancia al riesgo PQC.
- Incorporar estos límites dentro del Risk Appetite Framework corporativo.

Integración en la gestión de terceros (Third Party Risk Management)

- Evaluar el grado de preparación de proveedores en materia de PQC.
- Incluir requisitos de crypto-agility y planes de migración en contratos y procesos de due diligence.

La integración de PQC en el ERM permite transformar un riesgo tecnológico emergente en un riesgo gestionado de forma estructurada, medible y alineada con la estrategia corporativa, facilitando la toma de decisiones informadas y anticipándose a futuras exigencias regulatorias y de mercado

8.4. Auditoría, reporting y mejora continua

La integración de los riesgos asociados a PQC dentro del marco ERM debe complementarse con un enfoque sólido de auditoría, reporting y mejora continua, que garantice no solo la adecuación inicial del framework, sino también su evolución en un contexto tecnológico y regulatorio dinámico.

Dado el carácter emergente de PQC y la incertidumbre asociada a su adopción, este ámbito resulta clave para asegurar la resiliencia a largo plazo y la capacidad de adaptación de la organización.

Auditoría del riesgo PQC

La función de auditoría interna/ externa debe incorporar progresivamente el riesgo PQC dentro de su alcance, evaluando tanto el diseño como la efectividad de los controles implantados.

Entre los principales focos de auditoría destacan:

- **Gobernanza:** revisión de roles, responsabilidades y estructuras de decisión en torno a PQC.
- **Inventario criptográfico:** validación de la completitud, integridad y actualización del CBOM.
- **Evaluación de riesgos:** consistencia metodológica en la identificación, medición y priorización de riesgos PQC.
- **Planes de migración:** priorización, grado de avance, cobertura y adecuación de las hojas de ruta hacia algoritmos post-quantum.
- **Crypto-agility:** capacidad real de los sistemas para adaptarse a cambios criptográficos sin disrupciones significativas.
- **Gestión de terceros:** evaluación del riesgo PQC en proveedores críticos.

La auditoría debe considerar estándares y buenas prácticas emergentes, alineándose con marcos como NIST, ISO 27001 o futuras guías regulatorias específicas en PQC.

Reporting y comunicación

El reporting debe permitir trasladar la complejidad técnica de PQC a un lenguaje comprensible y accionable para la Alta Dirección y el Consejo.

Se recomienda:

- Integrar los riesgos PQC dentro de los informes periódicos de ERM.
- Utilizar indicadores clave de riesgo (KRIs) específicos, tales como:
  - % de activos críticos con criptografía vulnerable.
  - % de sistemas con capacidades de crypto-agility.
  - Nivel de avance en la migración a PQC.
  - Exposición a datos con larga vida útil no protegidos adecuadamente.[JP53.1]
- Incorporar escenarios de riesgo en los informes para ilustrar impactos potenciales.
- Establecer una narrativa clara sobre:
  - Nivel de exposición actual.
  - Evolución del riesgo.
  - Necesidades de inversión y priorización.

El objetivo es facilitar una toma de decisiones informada, alineada con el apetito de riesgo y la estrategia corporativa.

9. Recomendaciones y Roadmap de Implantación

Los capítulos anteriores han analizado el impacto del escenario post-quantum desde el punto de vista regulatorio, de riesgo y de madurez organizativa. Este capítulo no introduce nuevos conceptos, sino que sintetiza ese análisis en una hoja de ruta práctica para la toma de decisiones.

El foco no es explicar por qué existe el riesgo, sino qué decisiones deben tomarse y en qué horizonte temporal para llegar a 2030 y 2035 sin migraciones improvisadas ni exposición regulatoria innecesaria.

9.1. Qué deben hacer los CISOs en 2026

A partir de 2026, la preparación frente al escenario post-quantum deja de ser una cuestión exploratoria y pasa a formar parte del mínimo exigible de diligencia en la gestión de la ciberseguridad. Independientemente del sector o del nivel de madurez de partida, existen cinco prioridades que todo CISO debería poder justificar ante auditores, reguladores y órganos de gobierno.

Visibilidad criptográfica como prerrequisito

El primer paso no es migrar, sino saber qué existe y qué se protege. Resulta imprescindible disponer de un inventario de algoritmos, claves y certificados que permita identificar dependencias de criptografía vulnerable, especialmente en activos que gestionan datos con horizontes largos de confidencialidad o que soportan funciones críticas de negocio. Sin esta visibilidad, cualquier hoja de ruta carece de base defendible.

Gobernanza del riesgo cuántico integrada en el ERM

El riesgo post-quantum no debe gestionarse como un riesgo técnico aislado. Debe integrarse en el marco de gestión de riesgos corporativo existente, utilizando criterios comprensibles para la dirección: impacto, probabilidad, horizonte temporal y apetito de riesgo. Esto permite priorizar inversiones, evitar alarmismo y situar la transición PQC al mismo nivel que otros riesgos estratégicos.

Definición de una estrategia formal de transición

La expectativa regulatoria no es el despliegue inmediato de nuevos algoritmos, sino la existencia de una estrategia documentada, basada en riesgo y aprobada a nivel directivo. Dicha estrategia debe definir principios (uso de estándares, enfoque híbrido, cripto agilidad), prioridades y hitos temporales alineados con los ciclos de vida tecnológicos y regulatorios.

Activación de capacidades mínimas de cripto agilidad

Incluso sin migraciones masivas, el CISO debe empezar a reducir dependencias rígidas de algoritmos concretos. Esto incluye exigir configurabilidad criptográfica en nuevos desarrollos, evitar soluciones propietarias no estandarizadas y revisar contratos y adquisiciones desde una óptica de capacidad de evolución futura.

Pilotos selectivos en casos de mayor exposición

La experiencia operativa no se adquiere con planes, sino con pruebas controladas. Iniciar pilotos en casos de uso bien acotados, protección de datos de larga vida, canales expuestos a redes públicas, firma de software o identidad, permite anticipar impactos técnicos y organizativos sin asumir riesgos desproporcionados.

Estas prioridades constituyen acciones de *no regret*: refuerzan la postura de seguridad actual y preparan a la organización para escenarios futuros sin comprometer la estabilidad operativa.

9.2. Prioridades a corto, medio y largo plazo

La transición a la criptografía post-quantum es un proceso de largo recorrido, condicionado por los ciclos de vida tecnológicos y por hitos regulatorios ya definidos. Para evitar enfoques reactivos o descoordinados, resulta clave estructurarla en horizontes temporales claros, alineados con los objetivos de reducción progresiva del riesgo.

2026 - 2027

Corto plazo:
Preparación y visibilidad

Objetivo: comprender la exposición real de la organización.

En esta fase se establecen los cimientos del programa. El foco no está en migrar, sino en conocer y ordenar:

- Inventario criptográfico de sistemas, algoritmos, claves y certificados.
- Clasificación de datos según horizonte de confidencialidad.
- Identificación de dependencias críticas (proveedores, HSM, librerías, PKI).
- Definición y aprobación de la estrategia de transición PQC.
- Inicio de pilotos controlados en casos seleccionados.

Este periodo es crítico: las decisiones tomadas aquí condicionan el coste, el ritmo y la viabilidad de todas las fases posteriores.

2028–2030

Medio plazo:
Migración de alto riesgo

Objetivo: reducir el riesgo material antes de los hitos regulatorios clave.

En línea con el roadmap europeo, los casos de uso de mayor exposición deben estar protegidos antes de 2030. Las prioridades se concentran en:

- Migración de sistemas críticos y datos de larga retención.
- Despliegue de esquemas híbridos como solución transitoria.
- Evolución de infraestructuras de identidad y PKI.
- Alineamiento efectivo con proveedores estratégicos.

Esta fase marca el paso del análisis a la reducción tangible del riesgo.

2031–2035

Largo plazo:
Transformación completa

Objetivo: consolidar un entorno estructuralmente *quantum-safe*.

En este horizonte, la transición deja de ser un programa específico y pasa a integrarse en la arquitectura estándar:

- Retirada progresiva de algoritmos clásicos vulnerables.
- Adopción generalizada de estándares PQC.
- Integración de la cripto agilidad en la arquitectura empresarial.
- Revisión continua de la postura criptográfica y del riesgo residual.

Para 2035, la adopción de PQC debe ser la norma y no la excepción.

9.3. Quick wins y acciones inmediatas

Además de la planificación a medio y largo plazo, existen acciones de impacto inmediato que permiten avanzar de forma tangible en la preparación post-quantum sin esperar a grandes proyectos ni inversiones estructurales. Estas actuaciones generan tracción interna, reducen incertidumbre y facilitan la toma de decisiones posteriores.

Sensibilización y alineamiento interno

Uno de los principales bloqueos en la transición PQC no es técnico, sino organizativo. Iniciar sesiones de sensibilización dirigidas a equipos técnicos, responsables de negocio, jurídico y compras permite establecer un lenguaje común y evitar que la computación cuántica se perciba como un problema lejano o puramente académico.

Inventario criptográfico mínimo viable

No es necesario alcanzar desde el primer momento un inventario exhaustivo. Un enfoque pragmático consiste en construir un inventario inicial centrado en sistemas críticos, datos de larga retención y canales expuestos. Este inventario mínimo ya permite identificar puntos de riesgo relevantes y priorizar esfuerzos posteriores.

Protección temprana de datos de larga vida

Identificar conjuntos de datos cuya confidencialidad debe mantenerse más allá de la próxima década y evaluar cómo se están protegiendo hoy es una de las acciones con mayor retorno. En muchos casos, bastan medidas transitorias, como el uso de esquemas híbridos o la reducción de la vida útil de certificados, para reducir de forma significativa la exposición al riesgo HNDL.

Evaluación del estado de preparación de proveedores

La dependencia de terceros es una de las principales fuentes de riesgo residual. Solicitar a proveedores críticos información básica sobre su hoja de ruta PQC, su soporte de estándares y su capacidad de evolución criptográfica permite detectar dependencias problemáticas con antelación y evitar situaciones de bloqueo futuro.

Incorporación de criterios PQC en decisiones corrientes

Finalmente, uno de los quick wins más eficaces consiste en introducir criterios relacionados con cripto agilidad y preparación post-quantum en procesos ya existentes: adquisiciones, renovaciones de contrato, diseño de nuevas aplicaciones o revisiones de arquitectura. Esto evita generar deuda criptográfica adicional mientras se define la estrategia global.

Estas acciones no sustituyen a una hoja de ruta estructurada, pero permiten avanzar desde el primer momento y demostrar un enfoque proactivo y gobernado de la transición.

9.4. Hoja de ruta para la transición PQC: el camino realista

La transición a PQC no es lineal ni homogénea. Debe abordarse como un proceso progresivo, basado en riesgo y compatible con entornos híbridos, evitando enfoques disruptivos que comprometan la operación.

Un modelo de cinco fases permite estructurar la transición de forma ordenada y defendible:

Fase 1: Descubrimiento y evaluación • Inventario criptográfico. • Análisis de exposición y dependencias. • Identificación de sistemas y datos críticos. **Resultado:** visión clara y compartida del riesgo.	**Fase 2: Estrategia y planificación** • Definición del roadmap de transición. • Priorización de casos de uso. • Alineamiento con marcos regulatorios. **Resultado:** plan estructurado, aprobado y trazable.
Fase 3: Pilotos y validación • Despliegue de soluciones híbridas. • Pruebas de rendimiento y compatibilidad. • Validación operativa. **Resultado:** reducción de incertidumbre y aprendizaje práctico.	**Fase 4: Migración progresiva** • Migración priorizada de sistemas críticos. • Coordinación con proveedores y terceros. • Despliegue controlado por oleadas. **Resultado:** reducción efectiva del riesgo post-quantum.
Fase 5: Operación y mejora continua • Monitorización del entorno criptográfico. • Adaptación a nuevos estándares y amenazas. • Evolución permanente de la cripto agilidad. **Resultado:** organización preparada para futuras transiciones tecnológicas.	

Este enfoque permite avanzar con control, absorber la complejidad de los entornos reales y llegar a los hitos de 2030 y 2035 sin migraciones forzadas ni pérdida de confianza.

10. Conclusiones: hacia una resiliencia cuántica sostenible

Como hemos visto a lo largo del presente documento, la transición hacia la criptografía post-quantum es, día de hoy, un imperativo estratégico de negocio. Las organizaciones deben asumir que la amenaza cuántica, más que un evento futuro, es un riesgo operativo presente que exige una respuesta inmediata y estructurada.

Las principales conclusiones que extraemos a la hora de abordar esta transición son las siguientes:

1. El riesgo depende de la vida útil de la información, no sólo de la disponibilidad de la tecnología. El mayor peligro actual es la estrategia HNDL. Los datos sensibles capturados hoy por actores maliciosos serán descifrados en cuanto la computación cuántica sea una realidad. Por tanto, la urgencia de la migración no depende de cuándo aparecerá un ordenador cuántico criptográficamente relevante, sino de cuánto tiempo deben permanecer protegidos los datos de la organización. Si la vida útil de la información supera el horizonte de aparición de esta tecnología, el riesgo ya se ha materializado.

2. La gobernanza es clave. La transición PQC es, ante todo, un desafío de gobernanza y gestión de activos. La tecnología por sí sola no garantiza la seguridad; se requiere , idealmente, tener la mayor visibilidad posible a través de un Cryptography Bill of Materials. Es necesario que las organizaciones conozcan qué algoritmos, claves y certificados utilizan, y en qué sistemas residen, para poder priorizar su migración. La clave del éxito radica en integrar el riesgo cuántico en el marco de Enterprise Risk Management, tratando la "deuda criptográfica" con la misma seriedad que la deuda financiera.

3. La cripto-agilidad como principio rector. La incertidumbre sobre la evolución de los estándares y las amenazas obliga a adoptar la "cripto-agilidad" como pilar fundamental de la arquitectura tecnológica. Los sistemas deben diseñarse para ser modulares, permitiendo el reemplazo de algoritmos sin necesidad de rediseñar toda la infraestructura. El enfoque de "cripto-como-código" y la adopción de esquemas híbridos (clásico + PQC) son las estrategias más realistas para garantizar la seguridad sin comprometer la continuidad operativa durante el largo periodo de transición.

4. El cumplimiento normativo como catalizador. Regulaciones como NIS2 y DORA han transformado la criptografía de un control técnico aislado a una obligación de gobernanza sujeta a supervisión. Los hitos europeos (2026 para estrategias nacionales, 2030 para sistemas críticos y 2035 para adopción general) proporcionan una hoja de ruta que las organizaciones deben utilizar para justificar inversiones y priorizar recursos. El cumplimiento ya no es el destino, sino el catalizador que permite convertir la preparación cuántica en un programa de gestión estructurado.

5. La cadena de suministro como punto crítico de fallo. Ninguna organización es una isla en la era post-quantum. La seguridad de la cadena de suministro es un vector de riesgo sistémico. La capacidad de una organización para protegerse, por tanto, depende directamente de la preparación de sus proveedores tecnológicos. Exigir transparencia, hojas de ruta de migración y cláusulas de seguridad cuántica en los contratos es una medida de protección indispensable frente a la posible obsolescencia de terceros.

6. La oportunidad de la ventaja competitiva. Más allá de la mitigación de riesgos, la preparación proactiva ofrece una oportunidad de diferenciación en el mercado. Las organizaciones que lideren la transición serán percibidas como custodios más fiables de la información, fortaleciendo la confianza de clientes y stakeholders. La transición PQC es una palanca para modernizar procesos, automatizar la gestión de identidades y optimizar la resiliencia operativa.

La transición a la criptografía post-quantum es un maratón, no un sprint. La hoja de ruta debe ser realista:

- **Corto plazo (2026-2027):** Centrarse en el descubrimiento, inventario (CBOM) y sensibilización.
- **Medio plazo (2028-2030):** Migración priorizada de sistemas críticos y despliegue de soluciones híbridas.
- **Largo plazo (2031-2035):** Consolidación de entornos quantum-safe y retirada de algoritmos heredados.

En conclusión, el éxito en la era post-quantum no se medirá por la rapidez de una migración masiva, sino por la capacidad de la organización para gestionar su postura criptográfica de forma dinámica, defendible y alineada con sus objetivos estratégicos. La inacción es la decisión más costosa; la preparación, la inversión más rentable para garantizar la confianza digital en las próximas décadas.

ANEXO

Ejercicios prácticos y Playbooks

Simulación de escenarios de crisis post-quantum

La simulación de crisis no debe ser tratada únicamente como un ejercicio hipotético si no que debe utilizarse como una herramienta estratégica de resiliencia organizacional.

Un ejercicio de mesa (o tabletop exercise) es un taller de simulación donde los participantes discuten su respuesta a un escenario de crisis específico.

A diferencia de incidentes clásicos (ransomware, brechas de datos o denegaciones de servicio), las crisis post-quantum se caracterizan por su asimetría temporal: los efectos más dañinos pueden materializarse años después del ataque inicial. Esto obliga a replantear los ejercicios de crisis desde una lógica distinta, orientada no solo a la contención inmediata, sino a la protección de la confianza futura.

La simulación permite a las organizaciones poner a prueba su capacidad para gestionar escenarios donde:

- Los algoritmos criptográficos históricos dejan de ser confiables.
- La confidencialidad de los datos se ve comprometida.
- La integridad de datos pasados es cuestionada retroactivamente.
- La migración criptográfica debe realizarse bajo presión operativa, regulatoria y reputacional.

Se debe realizar ejercicios de crisis extrapolados al dominio post-quantum bajo el principio de cripto-agilidad. El objetivo no es únicamente ensayar una respuesta técnica, sino evaluar la capacidad del sistema para cambiar de paradigma en los tres pilares básicos: humano, organizativo y tecnológico.

Fase 1. Preparación e Identificación

Como ya se ha comentado en capítulos anteriores, la organización debe disponer de una CBOM actualizada, que permita identificar algoritmos utilizados, dependencias criptográficas y el ciclo de vida y longevidad requerida en los datos protegidos.

Fase 2. Diseño del Escenario e Inyecciones

En los ejercicios de crisis, las inyecciones (injects) son eventos diseñados para forzar decisiones bajo presión. En un contexto PQC, estas deben romper supuestos profundamente arraigados.

Ejemplos de injects de alto impacto incluyen:

- **Fallo de Confianza Criptográfica:** anuncio de que una autoridad criptográfica adversaria ha demostrado capacidad práctica para debilitar firmas RSA/ECC, invalidando certificados históricos.
- **Degradación Operativa por PQC:** introducción de latencia, fallos de handshake TLS o incompatibilidades debido al tamaño de claves y firmas en algoritmos post-quantum e híbridos.
- **Exposición Retroactiva de Datos:** confirmación de que datasets cifrados años atrás, como datos personales, propiedad intelectual o información industrial, han sido descifrados.
- **Presión Regulatoria y Contractual:** notificación de reguladores, auditores o clientes estratégicos exigiendo pruebas de integridad histórica y continuidad de cumplimiento.

Un error común, ampliamente documentado en ejercicios de crisis, es diseñar escenarios demasiado técnicos o benévolos. En ejercicios post-quantum, el realismo exige introducir fricción organizativa, ambigüedad y conflicto de prioridades, tal como ocurre en incidentes reales.

Fase 3. Ejecución

Durante la ejecución del ejercicio, se evalúa el funcionamiento de equipo de crisis como sistema socio-técnico, no como un equipo puramente técnico. Aspectos críticos para validar:

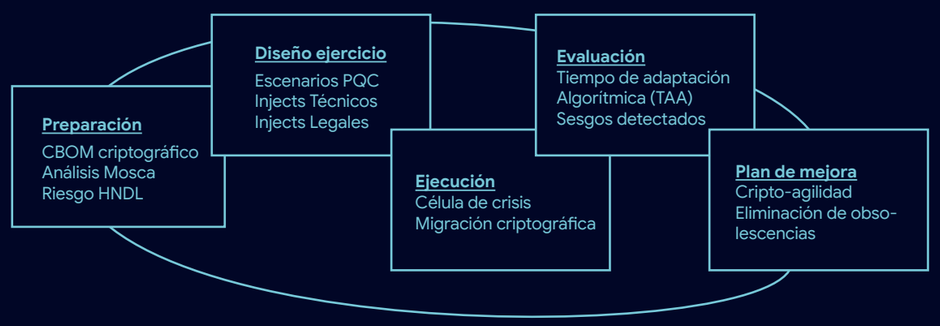
- **Aislamiento y contención criptográfica:** capacidad para identificar sistemas cuya seguridad depende de algoritmos obsoletos y limitar su exposición sin detener el negocio.
- **Activación de un plan de migración:** ejecución coordinada de mecanismos de transición hacia algoritmos post-quantum o híbridos.
- **Gestión de la confianza:** coordinación entre áreas técnicas, legales, comunicación y cumplimiento para explicar qué datos siguen siendo confiables y por qué.
- **Toma de decisiones bajo Incertidumbre:** la principal tensión no es técnica, sino estratégica: cuándo migrar, qué aceptar como riesgo residual y cómo justificarlo.

Fase 4. Evaluación

En ejercicios, la recuperación del servicio no es un indicador suficiente de éxito. Una métrica clave es el Tiempo de Adaptación Algorítmica (TAA) definido como la capacidad de modificar primitivas criptográficas sin rediseñar la arquitectura ni comprometer la continuidad del negocio.

La evaluación posterior debe identificar:

- Dependencias rígidas que impiden la migración.
- Obsolescencia técnica (HSM, firmware, dispositivos OT).
- Brechas entre estrategia de cripto-agilidad y capacidad real.
- Sesgos detectados durante el ejercicio (exceso de confianza, sub-reacción o bloqueo decisional), ampliamente descritos en la literatura de simulación de crisis.



Como conclusión, un ejercicio post-quantum se considera exitoso no cuando todo funciona, sino cuando revela fallos estructurales antes de que lo haga un adversario.

Las organizaciones con datos críticos de larga vida útil deberían realizar al menos un ejercicio tabletop anual centrado exclusivamente en la caída del cifrado asimétrico, involucrando no solo a TI y seguridad, sino también a legal, cumplimiento y alta dirección.

Ejercicios de mesa y lecciones aprendidas

El objetivo de un tabletop no es solucionar el problema en tiempo real, sino probar la eficacia de los planes, políticas y la comunicación de la organización.

Objetivos Clave:

- **Validar la Hoja de Ruta PQC:** poner a prueba el plan de migración frente a eventos inesperados.
- **Identificar Gaps:** descubrir puntos ciegos en el inventario, la gobernanza o la capacidad de respuesta.
- **Mejorar la Comunicación:** asegurar que existe un flujo de comunicación claro entre los equipos técnicos, legales, de negocio y la alta dirección.
- **Aumentar la Concienciación:** educar a los líderes de negocio sobre el impacto real de la amenaza cuántica.

Participantes Esenciales:

Un table top de PQC debe ser multifuncional. La lista de participantes debería incluir:

- **CISO y Equipo de Ciberseguridad:** lideran la respuesta al incidente.
- **CIO y Equipo de TI/Operaciones:** responsables de la infraestructura y los sistemas heredados.
- **Líderes de Desarrollo de Aplicaciones:** propietarios de los sistemas que necesitan ser actualizados.
- **Equipo Legal y de Cumplimiento:** para evaluar el impacto regulatorio (DORA, NIS2) y contractual.
- **Equipo de Comunicación Corporativa:** para gestionar la comunicación interna y externa.
- **Líderes de Unidades de Negocio:** para entender y decidir sobre el impacto en las operaciones.
- **Equipo de Gestión de Riesgos:** para contextualizar el evento dentro del marco de riesgo empresarial.

Escenarios Prácticos para un table top

Aquí tienes varios escenarios realistas que una organización debería simular:

Escenario 1: El "Día Q" Acelerado

Situación: Una noticia de última hora, confirmada por fuentes fiables (por ejemplo, una agencia gubernamental), anuncia un avance disruptivo en la computación cuántica. Se estima que un CRQC estará operativo en 18 meses, no en 10 años.

Preguntas a Discutir:

- ¿Cómo se valida esta información? ¿Quién toma la decisión de activar el plan de emergencia?
- ¿Cómo se acelera nuestra hoja de ruta de migración? ¿Qué proyectos se priorizan y cuáles se pausan?
- ¿Tenemos el presupuesto y los recursos para esta aceleración?
- ¿Cómo se comunica esto al Consejo de Administración y a los inversores?

Escenario 2: Vulnerabilidad en un Estándar PQC

Situación: Un grupo de investigadores publica una vulnerabilidad seria en uno de los algoritmos PQC recién estandarizados por el NIST (por ejemplo, ML-KEM/Kyber), que ya se ha implementado en un piloto de VPN corporativa.

Preguntas a Discutir:

- ¿Cómo se detecta dónde se ha desplegado este algoritmo? ¿Está el inventario (CBOM) lo suficientemente detallado?
- ¿Se cuenta con la "cripto-agilidad" necesaria para cambiar a un algoritmo alternativo (por ejemplo, uno de los candidatos de la ronda 4 del NIST)?
- ¿Cuál es el proceso técnico para desplegar el parche o el nuevo algoritmo? ¿Está automatizado?
- ¿Cómo se gestiona el riesgo mientras se implementa la solución?

Escenario 3: Fallo en la Cadena de Suministro

Situación: Un proveedor crítico de software (por ejemplo, el proveedor de nuestro sistema ERP o de una librería de pagos) anuncia que no cumplirá con los plazos para ser resistente a la cuántica y que su soporte para PQC se retrasa indefinidamente.

Preguntas a Discutir:

- ¿Qué sistemas y procesos de negocio dependen de este proveedor? ¿Cuál es el impacto financiero de esta dependencia?
- ¿Qué dice nuestro contrato sobre los requisitos de seguridad y las penalizaciones? ¿Está el equipo legal preparado?
- ¿Se han dentificado proveedores alternativos? ¿Cuál es el coste y el tiempo para migrar a otra solución?
- ¿Es posible aislar el sistema vulnerable usando gateways o proxies criptográficos como medida de mitigación temporal?

Escenario 4: El Piloto Híbrido Falla en Producción

Situación: Tras implementar un modo híbrido (Clásico + PQC) en una aplicación de cara al cliente, se detecta un aumento masivo de la latencia que provoca caídas del servicio y quejas de los clientes.

Preguntas a Discutir:

- ¿Cuál es el procedimiento de rollback para desactivar el modo híbrido de forma segura y rápida?
- ¿Cómo se realiza el análisis de causa raíz? ¿Fueron las pruebas de rendimiento previas insuficientes?
- ¿Cómo se comunica el problema a los clientes y a los equipos internos?
- ¿Qué impacto tiene este fallo en la confianza del equipo y de la dirección en el programa PQC? ¿Cómo se reajusta el plan?

Lecciones Aprendidas Clave de la Industria

Aunque muchas organizaciones están en las primeras fases, ya están surgiendo patrones claros y lecciones aprendidas de los pilotos y la planificación estratégica.

1. El Inventario es el Cimiento (y es más Difícil de lo que Parece).

Las organizaciones subestiman sistemáticamente la omnipresencia de la criptografía en sus sistemas. No se trata solo de certificados web, sino de SSH, firmas de código, bases de datos, sistemas embebidos, etc. El descubrimiento manual es imposible; se necesitan herramientas automatizadas.

2. La "Cripto-Agilidad" no es un Eslogan, es una Necesidad Técnica.

La incapacidad para cambiar rápidamente de algoritmos es el principal obstáculo técnico. Las organizaciones con criptografía "hardcoded" (codificada directamente en la aplicación) se enfrentan a un esfuerzo de remediación masivo. La adopción de "cripto-como-código" y el uso de bibliotecas modulares es fundamental.

3. Los Sistemas Heredados (Legacy) son el Mayor Obstáculo.

No se puede parchear fácilmente un mainframe de 20 años o un sistema de control industrial. La sustitución es a menudo inviable. Las soluciones realistas pasan por la abstracción criptográfica, utilizando gateways o proxies que gestionen la criptografía PQC en nombre del sistema heredado.

4. El Rendimiento Importa, Especialmente en el "Borde".

Los algoritmos PQC tienen claves y firmas más grandes, lo que puede aumentar la latencia y el consumo de CPU. Si bien esto puede ser manejable en un centro de datos, es un desafío crítico para dispositivos con recursos limitados como terminales de pago, dispositivos IoT o smart meters. Las pruebas de rendimiento en estos dispositivos son cruciales.

5. La Cadena de Suministro es el Mayor Punto Ciego.

Una organización puede tener una estrategia PQC perfecta, pero si un proveedor de software o hardware no está preparado, hereda ese riesgo. La preparación cuántica debe ser un criterio clave en la selección y gestión de proveedores. Exigir hojas de ruta PQC y CBOMs a los proveedores se está convirtiendo en una práctica estándar.

6. La Gobernanza y la Comunicación son Clave para el Éxito.

La migración a PQC no es solo un problema del CISO. Es un riesgo empresarial que debe ser entendido y financiado por la alta dirección. Crear un equipo multifuncional, comunicar el riesgo en términos financieros (como la "Deuda Criptográfica") y reportar el progreso a través de dashboards claros es esencial para mantener el impulso y los recursos necesarios para un proyecto que durará varios años.

Plantillas de runbooks y checklists para CISOs

Plantilla 1: Checklist Estratégico PQC para el CISO

Este checklist está diseñado para que el CISO pueda supervisar el estado del programa de preparación cuántica, asegurarse de que se cubren todas las áreas críticas y reportar el progreso al Consejo de Administración y a otros líderes ejecutivos.

Fase 1: Descubrimiento y Evaluación de Riesgos

- ☑ Inventario Criptográfico (CBOM): ¿se ha completado un inventario exhaustivo de todos los activos criptográficos (algoritmos, claves, certificados, librerías)? ¿Está automatizado este proceso?
- ☑ Identificación de Vulnerabilidades: ¿se han identificado y etiquetado todos los sistemas que utilizan criptografía vulnerable a ataques cuánticos (RSA, ECC, etc.)?
- ☑ Clasificación de Datos: ¿se han clasificado los datos protegidos por estos sistemas según su "vida útil" o "horizonte de confidencialidad"?
- ☑ Análisis de Riesgo Cuántico: ¿se ha calculado un "Quantum Risk Score" para los activos críticos para priorizar la migración?
- ☑ Cuantificación Financiera: ¿se ha estimado la "Deuda Criptográfica" de la organización para comunicar el riesgo en términos financieros al negocio?
- ☑ Evaluación de la Cripto-Agilidad: ¿se ha evaluado la capacidad actual de la organización para cambiar algoritmos criptográficos? ¿Se sabe dónde hay criptografía "hard-coded"?

Fase 2: Estrategia y Gobernanza

- ☑ Estrategia Formal y Hoja de Ruta: ¿existe una estrategia PQC formal y aprobada, con una hoja de ruta plurianual y un presupuesto asignado?
- ☑ Modelo de Gobierno: ¿se ha establecido un comité o grupo de trabajo multifuncional (por ejemplo, "Grupo de Amenazas Cuánticas") con un responsable ejecutivo claro?
- ☑ Roles y Responsabilidades: ¿se han definido roles clave como el "Ingeniero PQC" o el "Arquitecto de Criptografía"?
- ☑ Políticas y Estándares: ¿se han actualizado las políticas de seguridad, desarrollo seguro (SDL) y gestión de proveedores para incluir requisitos de PQC?
- ☑ Comunicación al Consejo: ¿existe un plan de comunicación para informar regularmente al Consejo de Administración sobre el estado del riesgo cuántico y el progreso del programa?

Fase 3: Planificación y Pruebas

- ☑ Selección de Pilotos: ¿se han identificado los sistemas y aplicaciones candidatos para los primeros proyectos piloto de PQC (idealmente, en modo híbrido)?
- ☑ Definición de Métricas de Éxito: ¿se han definido los KPIs para los pilotos (por ejemplo, impacto en el rendimiento, latencia, interoperabilidad)?
- ☑ Análisis de Proveedores: ¿se está evaluando la preparación PQC de nuestros proveedores de tecnología críticos (hardware, software, nube)?
- ☑ *Table top*: ¿se ha planificado y ejecutado al menos un table top con los escenarios de riesgo PQC más probables?
- ☑ Plan de Formación: ¿existe un plan para formar a los equipos técnicos y de desarrollo en los nuevos algoritmos y protocolos PQC?

Fase 4: Migración y Despliegue

- ☑ Plan de Migración por Fases: ¿existe un plan detallado para el despliegue de PQC, priorizando los sistemas con mayor "Quantum Risk Score"?
- ☑ Plan de Rollback: para cada migración, ¿existe un plan de reversión probado en caso de fallo o impacto inaceptable en el negocio?
- ☑ Plan de Comunicación: ¿hay un plan para comunicar los cambios a las partes interesadas internas y, si aplica, a los clientes?
- ☑ Automatización del Despliegue: ¿se están utilizando principios de "Cripto-como-Código" para automatizar el despliegue de los nuevos estándares?

Fase 5: Operación y Mejora Continua

- ☑ Monitorización Continua: ¿están los sistemas de monitorización (SIEM, etc.) configurados para detectar problemas relacionados con la nueva criptografía?
- ☑ Actualización del Inventario: ¿se actualiza el inventario criptográfico de forma continua a medida que se realizan los cambios?
- ☑ Vigilancia de Amenazas: ¿hay un proceso para mantenerse informado sobre nuevas vulnerabilidades en los algoritmos PQC y los avances en la computación cuántica?
- ☑ Revisión de la Estrategia: ¿se revisa y actualiza la hoja de ruta PQC anualmente o cuando hay cambios significativos en el panorama de amenazas?

Plantilla 2: Runbook Operativo de Respuesta a Incidentes PQC

Este runbook detalla los pasos a seguir por el equipo de respuesta a incidentes ante un escenario específico.

ID del Runbook: *PQC-IR-001*

Título: Respuesta a Vulnerabilidad Crítica en Algoritmo PQC Estandarizado

Escenario:

Se ha publicado una vulnerabilidad crítica (CVSS 9.0+) que afecta a un algoritmo de firma PQC estandarizado por el NIST (por ejemplo, ML-DSA/Dilithium). La vulnerabilidad permite la falsificación de firmas digitales. La organización utiliza este algoritmo para firmar actualizaciones de software y en algunos protocolos de autenticación.

Objetivos:

- Identificar todos los sistemas afectados en menos de 4 horas.
- Contener la amenaza y aplicar mitigaciones temporales en menos de 12 horas.
- Desplegar un algoritmo alternativo seguro en todos los sistemas afectados en menos de 72 horas.
- Comunicar de forma clara y oportuna a todas las partes interesadas.

Roles y Responsabilidades:

- Comandante del Incidente (CISO/Director de Ciberseguridad): liderazgo general y comunicación ejecutiva.
- Líder Técnico (Arquitecto de Criptografía): dirige el análisis técnico y la remediación.
- Equipo de Operaciones de Seguridad (SOC): monitorización y detección.
- Equipo de Desarrollo (DevOps/DevSecOps): implementación de cambios en el código y los pipelines.
- Equipo Legal y de Cumplimiento: evaluación del impacto regulatorio.
- Líder de Comunicación: gestión de las comunicaciones internas y externas.

Fases del Proceso de Respuesta

Fase 1: Detección y Triaje (T+0 a T+1 hora)

Alerta: el equipo de inteligencia de amenazas o el SOC recibe la alerta sobre la nueva vulnerabilidad.

Validación: el Líder Técnico valida la veracidad y aplicabilidad de la vulnerabilidad a nuestro entorno.

Activación del Equipo de Respuesta: el Comandante del Incidente activa formalmente el equipo de respuesta a incidentes.

Evaluación de Impacto Inicial: se realiza una evaluación rápida del impacto potencial en el negocio. Se establece el nivel de severidad del incidente.

Fase 2: Contención y Análisis (T+1 a T+4 horas)

Consulta al Inventario Criptográfico (CBOM): el Líder Técnico consulta la herramienta de inventario (por ejemplo, SandboxAQ, Keyfactor) para generar una lista de todos los sistemas, aplicaciones y librerías que utilizan el algoritmo vulnerable.

Análisis de Exposición: se determina qué sistemas están expuestos a Internet y cuáles son internos.

Mitigación Temporal:

Si es posible, se aplican reglas de firewall o WAF para bloquear patrones de ataque conocidos.

Se considera la desactivación temporal de los servicios no críticos que dependen del algoritmo vulnerable.

Se aumenta el nivel de monitorización sobre los sistemas afectados

Fase 3: Remediación (T+4 a T+72 horas)

- [x] Selección de Algoritmo Alternativo: el Líder Técnico, en consulta con el comité de gobierno PQC, selecciona un algoritmo de firma alternativo aprobado (por ejemplo, otro estándar del NIST o un candidato de reserva).
- [x] Actualización de la Política como Código:
  - [x] El equipo de DevOps actualiza la política en Open Policy Agent (OPA) para prohibir el algoritmo vulnerable y permitir el nuevo.
  - [x] El cambio se versiona en Git.
- [x] Despliegue Automatizado (vía CI/CD):
  - [x] Se modifica el código de las aplicaciones modernas para usar el nuevo algoritmo.
  - [x] El pipeline de CI/CD se activa, las pruebas de regresión se ejecutan automáticamente.
- [x] OPA valida que la nueva configuración cumple con la política actualizada.
- [x] El cambio se despliega en un entorno de staging para una validación final.
- [x] Tras la aprobación, se despliega en producción.
- [x] Remediación Manual (Sistemas Heredados):
  - [x] Se activa el plan específico para los sistemas legacy que no pueden ser actualizados automáticamente.
  - [x] Esto puede implicar contactar al proveedor, aplicar un parche manual o actualizar la configuración de un gateway criptográfico.

Plantilla 2: Runbook Operativo de Respuesta a Incidentes PQC

Este runbook detalla los pasos a seguir por el equipo de respuesta a incidentes ante un escenario específico.

Fase 4: Recuperación y Verificación (T+72 horas en adelante)

- ☑ Escaneo de Verificación: se realiza un nuevo escaneo con la herramienta de inventario para confirmar que no quedan instancias del algoritmo vulnerable.
- ☑ Monitorización Post-Cambio: el SOC monitoriza los sistemas actualizados para detectar cualquier comportamiento anómalo o impacto en el rendimiento.
- ☑ Declaración de Cierre del Incidente: el comandante del Incidente declara formalmente el cierre del incidente una vez que todos los sistemas están parcheados y estables.

Fase 5: Post-Incidente y Lecciones Aprendidas

- ☑ Reunión de Lecciones Aprendidas: se convoca una reunión con todos los participantes en un plazo de 5 días hábiles.
- ☑ Análisis de Causa Raíz: ¿Qué funcionó? ¿Qué no funcionó? ¿Fue el inventario preciso? ¿Falló la automatización en algún punto?
- ☑ Actualización del Runbook: se actualiza este runbook con las lecciones aprendidas.
- ☑ Informe Ejecutivo: se prepara un informe para la alta dirección resumiendo el incidente, la respuesta y las mejoras a implementar.

Modelos de políticas y procedimientos

En la actualidad, no se han identificado modelos de políticas empresariales de uso de o posición ante tecnologías cuánticas que estén públicamente disponibles. Sí están disponibles las estrategias y políticas nacionales de diversos países y áreas de influencia, que se exponen a continuación.

- **Estrategia nacional de USA, articulada mediante su Cámara de Comercio:** https://www.uschamber.com/assets/documents/2024319-C_TEC-Quantum-principles-Final-1.pdf
- **Estrategia Cuántica de la Unión Europea:** https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- **Estrategia Cuántica de España:** https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion_ministro/2025/04/2025-04-24/EstrategiaTecnologiasCuanticas_compressed_24_04.pdf

No se ha localizado una fuente fiable de la estrategia cuántica de la República Popular China, que también es un actor relevante en el campo.

Herramientas y recursos recomendados

- https://openquantumsafe.org/. Proyecto open source para la transición a la criptografía resistente a cuántica
- https://csrc.nist.gov/Projects/post-quantum-cryptography-. Página principal del NIST respecto de sus iniciativas en PQC.
- https://www.thalesaleniaspace.com/en/press-releases/arranca-el-desarrollo-del-primer-sistema-geoestacionario-de-distribucion-de-clave/es. Sistema geoestacionario de distribución de clave cuántica por satélite liderado por Thales Alenia Space.
- https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Página donde NIST publica los resultados de la evaluación de resistencia a las capacidades cuánticas de algoritmos criptográficos. En 2022 fueron todos algoritmos simétricos.
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Página donde NIST publica los esquemas candidatos a criptografía cuántica que son aprobados. Se publicarán a futuro más esquemas aquí
- https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals. Página en la que NIST recoge nuevos esquemas candidatos, para su evaluación.

isms forum

CSC
CYBER SECURITY CENTRE

Riesgos y Oportunidades del Post-Quantum en Ciberseguridad

Guía para CISOs