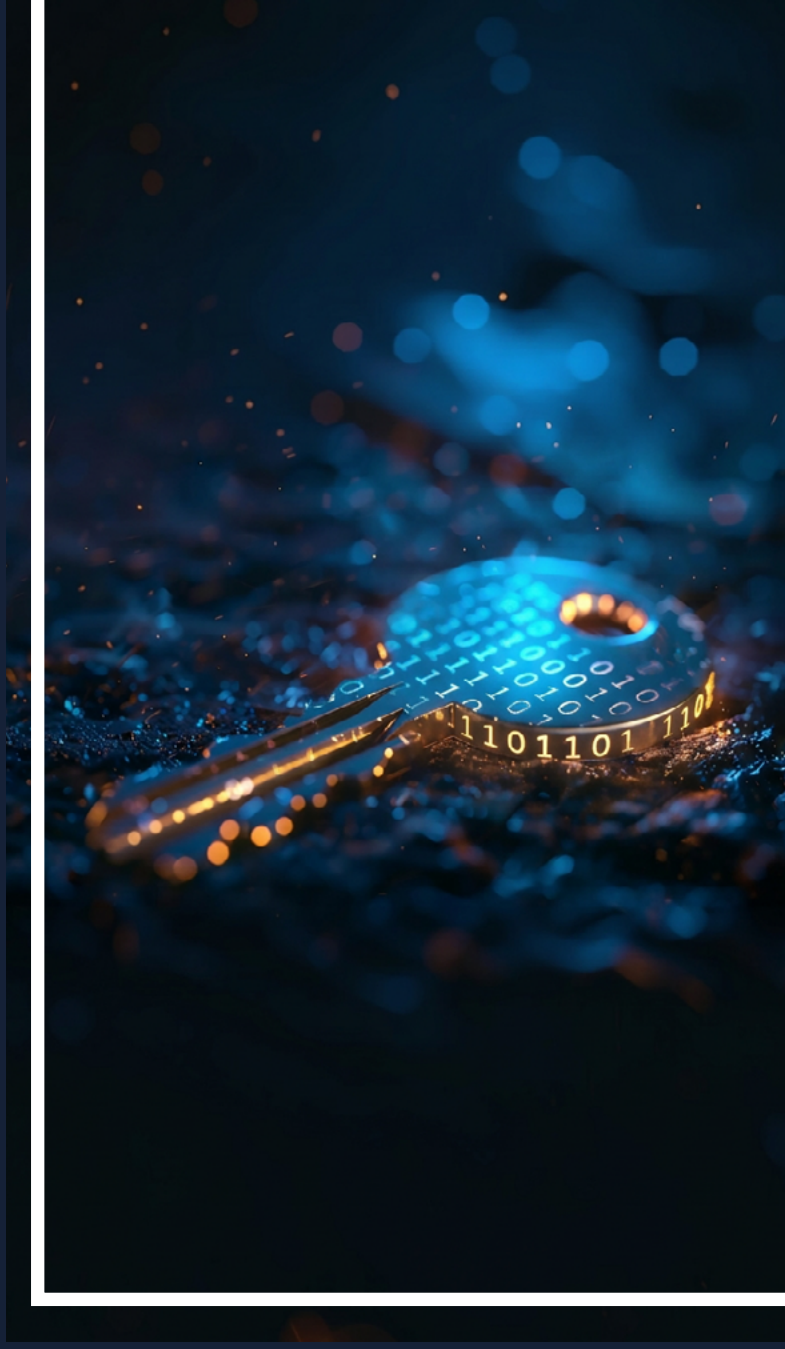


Hoja de ruta de la transición a criptografía postcuántica en España

NOVIEMBRE 2026

centro criptológico nacional

centro criptológico nacional

Edita:

CN-PYTEC
centro criptológico nacional

© Centro Criptológico Nacional, 2026
Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

Resumen ejecutivo **4**

1. Introducción **6**

1.1. Introducción al riesgo cuántico 8

1.2. Estructura del plan de transición 11

2. Etapa 1: Preparación para la transición postcuántica **14**

2.1. Definición de objetivos estratégicos y políticas criptográficas 15

2.2. Identificación de actores relevantes 17

2.2.1. Actores Externos 17

2.2.2. Actores Internos 18

2.3. Diagnóstico inicial e inventario de activos 19

2.3.1. Descubrimiento automatizado y formato CBOM 23

2.4. Análisis del riesgo cuántico y priorización de activos 26

2.4.1. Análisis de vulnerabilidad cuántica 27

2.4.2. Análisis de impacto 29

2.4.3. Análisis de esfuerzo estimado para la migración 32

2.4.4. Puntuación de riesgo cuántico y nivel de riesgo del sistema 33

2.5. Formación y concienciación 37

2.6 Gobernanza interna 39

3. Etapa 2: Planificación de la migración **40**

3.1. Planes de actualización 42

3.2. Estrategias de migración 45

3.3. Planes de migración, *backup* y *rollback* 47

4. Etapa 3: Ejecución de la migración **49**

4.1. Ejecución técnica de la migración 50

4.2. Seguimiento del proceso de migración 52

4.3. Implantación de mecanismos de cripto-agilidad 53

4.4. Seguimiento, indicadores, auditoría y mejora continua 58

5. Despliegue nacional, coordinación y calendario **59**

6. Acrónimos **61**

7. Bibliografía **63**

ANEXO I. Tabla de vulnerabilidad cuántica **67**

Resumen ejecutivo

Esta Hoja de Ruta establece un instrumento nacional de planificación, coordinación, seguimiento y revisión de la transición a la criptografía postcuántica en España, y se alinea con la Recomendación (UE) 2024/1101 de la Comisión, así como con *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, aprobado por el Grupo de Cooperación **NIS**, y se coordina con el Esquema Nacional de Seguridad.

El documento distingue dos planos complementarios. El primero es **nacional**: coordinación sectorial, calendario, indicadores, contratación pública, capacidad de evaluación y seguimiento. El segundo es **organizativo**: política criptográfica, inventario de activos y dependencias, análisis del riesgo cuántico, planificación, proyectos piloto, migración, pruebas, reversión y cripto-agilidad.

Esta Hoja de Ruta se proyecta sobre el conjunto del ecosistema público y privado, pero su exigibilidad depende del título jurídico aplicable. En el ámbito del Esquema Nacional de Seguridad, sus contenidos serán exigibles en la medida en que los recoja su normativa reguladora; en telecomunicaciones, servicios de confianza, entidades esenciales o importantes, infraestructuras críticas y sectores regulados, se incorporarán mediante la normativa y la supervisión sectorial; y para los restantes sujetos operan como referencia, fomento o adhesión voluntaria.

La preparación deberá iniciarse de inmediato. Antes del 31 de mayo de 2027 deberían estar establecidos la gobernanza, las políticas, el inventario inicial, la clasificación de los servicios o casos de uso incluidos en el alcance de la transición y se deberían haber planificado los proyectos piloto necesarios para los sistemas de riesgo alto y medio que se iniciarán en la medida de lo posible. La migración de los servicios o casos de uso de alto riesgo tiene como horizonte el 31 de diciembre de 2030. La transición de los sistemas de riesgo medio y, en la medida técnica y económicamente viable, de los de riesgo bajo, se desarrollará hasta el 31 de diciembre de 2035, sin perjuicio de la aceleración que exijan la evolución de la amenaza, los estándares o la normativa aplicable.

Resumen ejecutivo

La transición se gestionará en función del riesgo de los sistemas. La protección de la información de larga vida útil, el riesgo de captura y descifrado futuro, las actualizaciones de *software* y *firmware*, las infraestructuras de clave pública y los sistemas de identidad y firma, recibirán prioridad. En relación con los mecanismos criptográficos (incluidos algoritmos), parámetros, y requisitos de fortaleza para la transición, se mantendrán actualizados en las guías publicadas por el Centro Criptológico Nacional, con el alcance indicado en el **apartado 3.1**.

Esta Hoja de Ruta constituye la hoja de ruta nacional inicial de transición a la criptografía postcuántica, en el sentido previsto en la mencionada hoja de ruta coordinada del Grupo de Cooperación NIS. En su presente formulación, esta Hoja de Ruta no crea por sí misma obligaciones jurídicas, ya que las expresiones de carácter prescriptivo que contiene describen buenas prácticas o actuaciones recomendadas, salvo cuando reproduzcan una obligación directamente exigible conforme a la normativa identificada en cada caso. La estructura de gobernanza nacional de la transición, la distribución de funciones entre los órganos competentes y los instrumentos que, en su caso, hagan exigibles sus contenidos podrán establecerse mediante la normativa que se apruebe en la materia. Esta Hoja de Ruta se adaptará a dicha normativa, que prevalecerá sobre su contenido, y se entiende sin perjuicio de las competencias atribuidas a los departamentos ministeriales, organismos y autoridades sectoriales.

Se señala que la metodología de clasificación del riesgo cuántico del **apartado 2.4**, el calendario e hitos de esta Hoja de Ruta, los indicadores, el cuadro de mando nacional, y los formatos de seguimiento tienen carácter transitorio y se aplicarán como referencia hasta que la normativa que, en su caso, se apruebe establezca la gobernanza de la transición y, conforme a ella, los órganos competentes aprueben la metodología común, el calendario y los instrumentos de seguimiento, que sustituirán a los aquí recogidos. Las entidades adaptarán a dichos instrumentos, en los plazos que se establezcan, los inventarios, clasificaciones y planes elaborados conforme a esta Hoja de Ruta.



1. Introducción

Con el avance de la **computación cuántica**, la **criptografía se enfrenta a nuevos riesgos y desafíos**. La criptografía tradicional, especialmente la **criptografía de clave pública**, basada en problemas matemáticos complejos como la factorización de números enteros grandes (**RSA**) o el problema del logaritmo discreto (**DH**, **ECDH**, **DSA**, **ECC** y **ECDSA**), puede verse comprometida ante la aparición de un **ordenador cuántico criptográficamente relevante** (**CRQC** por sus siglas en inglés *Cryptographically Relevant Quantum Computer*), con capacidad suficiente para la ejecución de algoritmos cuánticos como por ejemplo los algoritmos de Shor.

Así mismo, la **criptografía simétrica**, junto con las funciones hash, también pueden ver mermada su seguridad con el desarrollo de un ordenador cuántico **CRQC**, al ejecutar el algoritmo de Grover. Sin embargo, el impacto es mucho menor, por lo que se recomienda aumentar la seguridad de los algoritmos simétricos y funciones hash siempre que sea posible.

Debido a esta amenaza, desde hace varios años, se está llevando a cabo un importante esfuerzo normativo por parte de las instituciones (p. ej. **NIST**, **ISO**, **IETF**, **ETSI**) para estandarizar nuevos algoritmos y criptosistemas resistentes a ataques llevados a cabo por un adversario que disponga de un ordenador **CRQC**. Estos nuevos algoritmos de clave pública se denominan **algoritmos postcuánticos**.



1. Introducción

Por ello, la amenaza de la computación cuántica hace indispensable una **transición planificada y ordenada hacia la implementación de algoritmos postcuánticos o esquemas híbridos** que combinen algoritmos tradicionales y postcuánticos. Esta transición debe ser capaz de preservar la fortaleza y la interoperabilidad de los sistemas actuales.

La estimación de la aparición del ordenador cuántico criptográficamente relevante ha ido variando con el tiempo. Inicialmente se esperaba su aparición en el año 2050. Sin embargo, con los desarrollos en computación cuántica, la fecha se ha ido adelantando y se prevé que esté disponible en la próxima década (entre 2030 y 2035).

Debido a los desafíos tecnológicos que implica la aparición de este ordenador, se hace necesario empezar la planificación ordenada y proactiva de los sistemas criptográficos e infraestructuras de clave pública (**PKI**) ante riesgos inminentes que puede representar su disponibilidad en el futuro. En concreto, existen dos **potenciales riesgos sobre los criptosistemas actuales**:

- **Almacena ahora y descifra luego (*Harvest now and decrypt later-HNDL*)**

  La información que necesitamos salvaguardar puede verse expuesta cuando se disponga de un ordenador **CRQC**, si no se comienza a proteger de manera adecuada.

- **Grandes tiempos de migración**

  No hay que subestimar los tiempos que puede llevar una migración de nuestros sistemas. Hay que comenzar a planificar todas sus fases: descubrimiento, adquisición, despliegue y puesta en marcha.

En el presente documento se analizarán las mejores prácticas para definir un plan de transición de los sistemas criptográficos hacia el uso de algoritmos postcuánticos o esquemas híbridos que combinen algoritmos tradicionales con algoritmos postcuánticos, estableciendo una hoja de ruta que abarque desde el diagnóstico inicial hasta la implementación y mantenimiento de las soluciones criptográficas.

En los siguientes subapartados se introducirá una aproximación para el cálculo del riesgo cuántico, basada en el teorema de Mosca, que ayuda a cuantificar el margen temporal disponible para abordar la transición.. Por último, se ofrecerá una estructura general del plan de migración, que defina las fases y los objetivos estratégicos para la adopción y uso general de algoritmos postcuánticos en sistemas criptográficos. Estas fases incluirán los siguientes aspectos: análisis de activos criptográficos, priorización de sistemas críticos, planificación, ejecución de la migración y mecanismos para su seguimiento y control.

1.1. Introducción al riesgo cuántico

Una primera introducción visual al riesgo cuántico se puede derivar del **teorema de Mosca**. Este presenta un esquema simple de visualización y tratamiento del riesgo cuántico propuesto por el investigador y profesor Michele Mosca de la universidad de Waterloo.

El teorema de Mosca aborda la problemática de cuándo deben abordar las organizaciones el plan de transición hacia algoritmos postcuánticos para protegerse de las amenazas que se pueden producir por ataques en los que se utilice un ordenador cuántico **CRQC**. Este esquema de gestión del riesgo puede servir como base a las organizaciones para identificar activos críticos en los que se deba iniciar el plan de transición.

En la siguiente figura podemos observar de forma gráfica el teorema de Mosca:

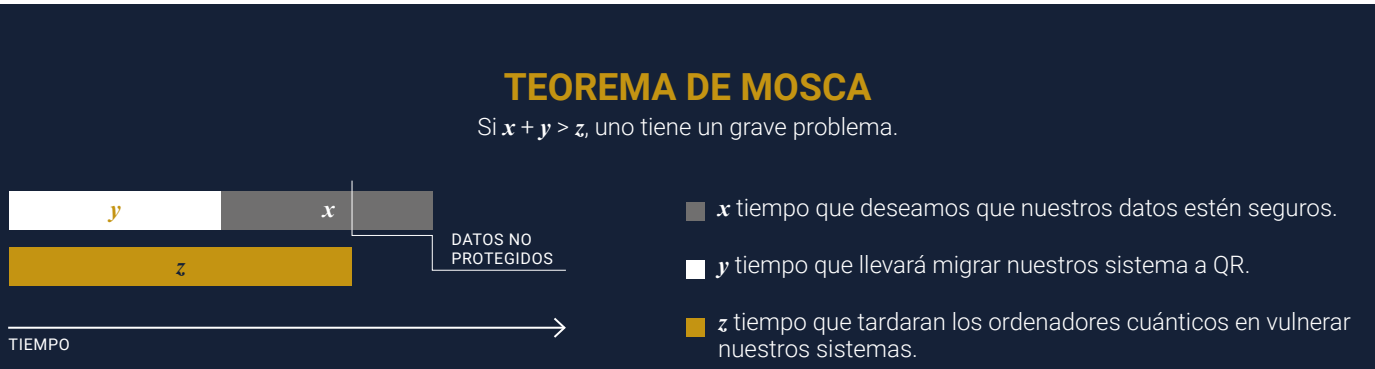


Ilustración 1. Teorema de Mosca

1. Introducción

El teorema de Mosca indica que las organizaciones deben preocuparse por el riesgo cuántico y empezar de inmediato con los planes de transición, si se cumple la siguiente condición:

$$X + Y > Z$$

Donde cada variable representa lo siguiente:

- **X: vida útil (*shelf-life time*):** Indica el tiempo de vida útil de la información generada y protegida mediante mecanismos tradicionales o los sistemas a proteger. Responde a la pregunta: ¿Cuánto tiempo debe permanecer segura la información? Debido a la posibilidad de ataques **HNDL**, se ha de tener en cuenta el tiempo de vida tanto de la información ya generada previamente como de la que se genere en la actualidad. Este valor es de especial relevancia en sistemas que cuyo ciclo de vida sea elevado, por ejemplo, certificados CA raíz con vigencia a 10-20 años, o en activos de información que deban mantenerse confidenciales durante largos periodos de tiempo, por ejemplo, información clasificada o evidencias digitales.
- **Y: tiempo de migración (*migration time*):** Indica el tiempo de ejecución del plan de transición y migración a la criptografía postcuántica. Responde a la pregunta: ¿Cuánto tiempo se tarda en realizar la migración a una solución postcuántica segura? Incluye para cada sistema o activo de información el tiempo desde que se inventaría y se analiza el riesgo cuántico, hasta que se ejecuta la migración y dicho activo pasa a disponer de protección cuántica. Se ha de tener en cuenta que el proceso de migración puede ser lento debido a su complejidad.
- **Z: cronograma de amenazas (*threat timeline*):** Indica el tiempo que tardarán los avances en computación cuántica en permitir la construcción de un ordenador cuántico criptográficamente relevante para la ejecución de ataques cuánticos. Responde a la pregunta: ¿Cuánto tiempo falta para que se construya un ordenador cuántico **CRQC**? Este valor es desconocido, ya que dependerá de los avances en el campo de la computación cuántica, tanto en la construcción de ordenadores cuánticos como en la mejora de los códigos de corrección de errores. Las estimaciones de cuándo puede estar disponible un ordenador cuántico **CRQC** varían entre los 5 y 15 años (2030-2040). El punto de inflexión a partir del que un ordenador **CRQC** se encuentre disponible para ataques cuánticos también se conoce habitualmente como ***Q-Day***.

1. Introducción



Existen algunas variaciones a este teorema que introducen el término "***Cripto-Procastinación***" como un elemento más en la suma y que se refiere a la postura de las organizaciones de retrasar o posponer el inicio del plan de transición y migración por diversos motivos, entre ellos la subestimación del riesgo o la complejidad y coste.

Del mismo modo, muchas organizaciones desconocen todos los sistemas y activos de información de los que disponen y que deben formar parte del plan de migración. Por ello **es indispensable la elaboración de un inventario de activos criptográficos que permita calcular el riesgo cuántico de toda la organización**.

Por tanto, una de las primeras conclusiones que se pueden extraer del teorema de Mosca es la necesidad de iniciar de inmediato el plan de transición postcuántica para que pueda ejecutarse de forma ordenada durante los próximos años y poder garantizar la seguridad una vez que llegue el *Q-day*.

1.2. Estructura del plan de transición

En este apartado, se definirá la estructura del plan de transición a criptografía postcuántica, dividiéndolo en tres fases o etapas.



ETAPA 1: Preparación para la migración postcuántica

2.1. Definición de objetivos estratétigos y políticas criptográficas

2.2. Identificación de actores relevantes

2.3. Diagnóstico inicial e inventario de activos

2.4. Análisis de riesgo cuántico y priorización de activos

2.5. Formación y concienciación

ETAPA 2: Planificación de la migración

3.1. Planes de actuación

3.2. Estrategias de migración

3.3. Planes de migración, *backup* y *rollback*

ETAPA 3: Ejecución de la migración

4.1. Ejecución técnica de la migración

4.2. Seguimiento del proceso de migración

4.3. Mecanismos de criptoagilidad

Ilustración 2. Etapas del plan de transición criptográfica

Etapa 1. Preparación para la transición postcuántica

La primera etapa se centra en establecer las **bases organizativas, estratégicas y técnicas** que permitan estar en la mejor disposición posible antes de acometer la planificación y ejecución del plan de migración. En este fase, se consideran las actividades que proporcionan un alto valor a la organización en términos de **gobernanza, visibilidad y resilencia**, independientemente de que la amenaza de un ordenador cuántico **CRQC** se llegue a materializar en el corto-medio plazo o incluso que no se llegase a materializar nunca.

Estas acciones se deben acometer para ser consciente de los riesgos y poder disponer de una visión precisa del estado de seguridad de los sistemas y activos criptográficos de la organización. Ignorar o posponer estos riesgos es incompatible con una gestión responsable de la seguridad.

Para ello es preciso:

- Definir los **objetivos estratégicos**.
- Revisar las **políticas criptográficas** de la organización.
- Identificar los **actores relevantes** del proceso.
- Realizar un **inventario de sistemas y activos criptográficos** junto con sus dependencias e interrelaciones, incluyendo también toda la cadena de suministro.
- Incluir **el riesgo cuántico en los análisis de riesgos**, con el objetivo de establecer una priorización de activos en base a su exposición y criticidad alineada con los objetivos estratégicos de la organización.
- Promover la **concienciación y formación** en materia criptográfica de forma que permita a la organización implementar los principios de cripto-agilidad (facilidad y rapidez con las que las organizaciones se pueden adaptar a cambios o nuevos riesgos relacionados con la criptografía) y resilencia a largo plazo, en línea con las políticas establecidas.

Etapa 2. Planificación de la migración

La segunda etapa del plan se orientará a establecer una planificación técnica y operacional de la migración. En ella, se recogen todos los resultados obtenidos de la etapa anterior, de forma que, en base a la priorización de activos, se detallen las **acciones concretas, ordenadas y calendarizadas**, estableciendo los **recursos necesarios**.

Para cada uno de los activos o grupo de activos identificados, se debe valorar el grado de madurez de las soluciones con capacidad postcuántica, así como el plan detallado de actualización o migración. Una vez se dispone del análisis de riesgo cuántico sobre el activo, así como las posibles soluciones de actualización o migración, se debe escoger una **estrategia de migración adecuada** para dicho activo y planificar su ejecución.

Junto con el plan técnico de migración, se deben definir planes de backup y vuelta atrás (***Rollback***), para garantizar la continuidad del servicio ante posibles fallos o incompatibilidades durante la transición. También es importante incluir

en el plan de migración la correcta **alineación con normativas aplicables y certificaciones**.

Durante todo este proceso se deben tener en cuenta mecanismos de cripto-agilidad, de forma que los sistemas y activos criptográficos puedan adaptarse rápidamente ante cambios, nuevas vulnerabilidades, etc. para mantener el nivel de protección y seguridad adecuado establecido en las políticas y objetivos estratégicos.

Etapa 3. Planificación de la migración

La última etapa del plan de transición se centra en la ejecución técnica del proceso de migración, el seguimiento del despliegue y el grado de avance y la implantación de mecanismos de monitorización continua del estado de la seguridad criptográfica, de forma que se pueda establecer un proceso iterativo donde se actualiza el análisis de riesgos y permita la implantación de un modelo de cripto-agilidad, donde los sistemas y activos se puedan adaptar rápidamente ante cambios.

En la siguiente imagen se recoge de forma visual y esquemática el proceso descrito anteriormente:

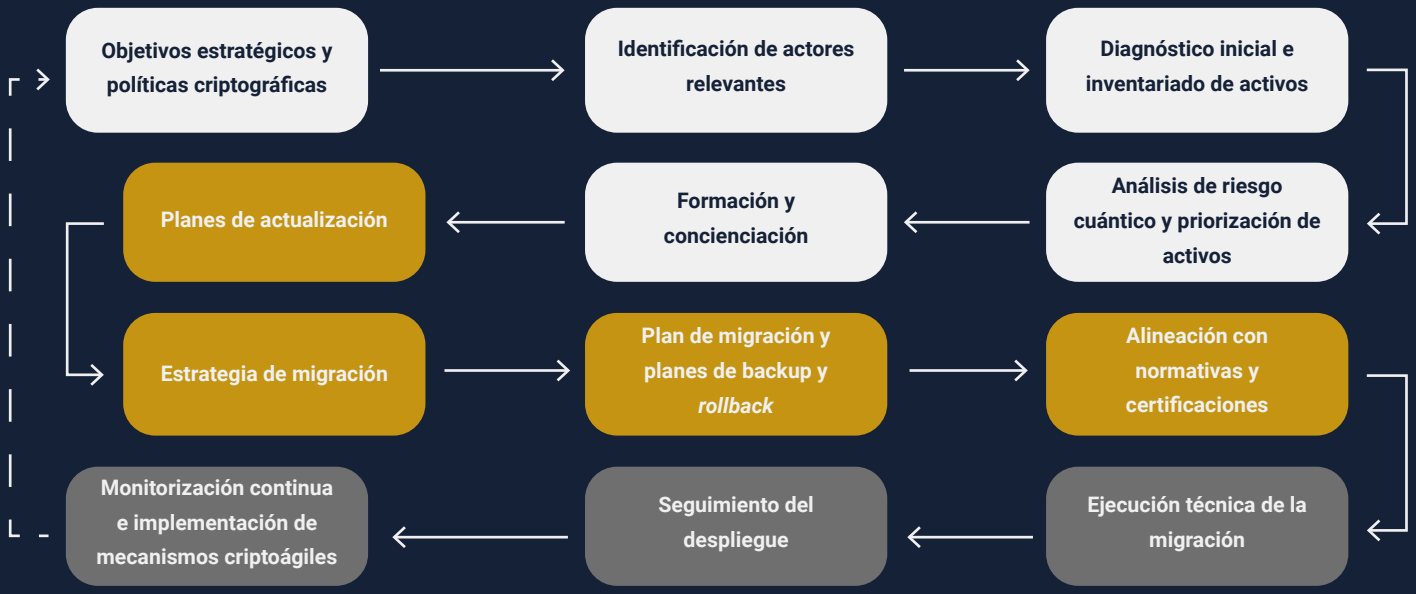


Ilustración 3. Estructura del plan de transición

A lo largo de los siguientes apartados, se analizará en detalle cada una de las etapas y acciones mencionadas anteriormente.

2. Etapa 1: Preparación para la transición postcuántica

En este apartado, analizaremos cada una de las acciones que componen la etapa 1 del plan de transición a criptografía postcuántica. Esta fase constituye la base sobre la que se construirá el resto del proceso de migración.

El objetivo de esta fase es obtener una **visión integral del estado de los activos** criptográficos de la organización, **definir las bases** estratégicas, organizativas y de gobernanza e **identificar riesgos y dependencias** críticas antes de abordar las acciones técnicas de migración, sustitución o integración de algoritmos postcuánticos.

Las actividades de esta etapa son: definición de objetivos estratégicos y políticas criptográficas, identificación de actores clave y grupos de interés, elaboración de un inventario de activos criptográficos y diagnóstico de situación actual, análisis del riesgo cuántico y priorización de activos y formación y concienciación de todos los perfiles implicados en el proceso.

2.1. Definición de objetivos estratégicos y políticas criptográficas

Las primeras acciones de la etapa de preparación para la migración postcuántica se basan en establecer un **marco de gobernanza** que sea la base sobre la que se sustente todo el proceso de transición cuántica.

Este marco de gobernanza debe establecer las **políticas organizativas** y marcos de trabajo con los que la organización oriente sus esfuerzos al cumplimiento de los **objetivos estratégicos** y a la realización de su visión y misión. Debe ser establecido por los órganos de **control estratégico de la organización** (consejo de administración, junta directiva, etc.) y debe definir la postura o **apetito frente al riesgo**. En este contexto, los riesgos asociados al avance de la computación cuántica pueden suponer un escollo para el cumplimiento de los objetivos estratégicos o incluso la continuidad de negocio.

La **incorporación del plan de transición cuántica en los objetivos estratégicos de la organización**, en lugar de tratarse como un plan independiente, asegura una correcta alineación de la organización y los actores implicados para una transición ordenada, habilita la asignación de recursos, incorpora la gestión del riesgo cuántico en los procesos organizativos de gestión del riesgo y cumplimiento legal y normativo; y permite adaptarse de forma criptográficamente ágil ante nuevos cambios o amenazas que pueden surgir.



Dentro de las políticas organizativas, se deben establecer las políticas criptográficas que deberían contener:

- **Gestión de inventario de activos criptográficos:** revisados de forma continua y que establezca mecanismos de mitigación del riesgo, prohibiendo o desaconsejando el uso de criptografía vulnerable en función del nivel de riesgo del activo.
- **Integrar el riesgo cuántico en los modelos de análisis de riesgos y continuidad de negocio:** contemplándolos, además, en los planes de continuidad de negocio. Esta integración permitirá la priorización en la migración y protección de activos críticos, así como procesos iterativos de gestión del riesgo y monitorización del grado de avance del plan de transición.
- **Inclusión de requisitos de protección postcuántica:** Las organizaciones deben revisar sus políticas, guías y estándares para incluir requisitos de protección postcuántica, ya sean internos o de cumplimiento normativo o de estándares y certificaciones. Asimismo, se promoverán mecanismos que permitan la cripto-agilidad en los productos o servicios prestados, habilitando mecanismos de actualización de algoritmos criptográficos, incorporación de cláusulas con proveedores de servicios, etc.
- **Gestión de riesgo en la cadena de suministro:** se deben reflejar los criterios de evaluación de proveedores externos en cuanto a madurez criptográfica postcuántica, así como sus capacidades de actualización o cripto-agilidad.
- **Establecimiento de procedimientos de gestión del ciclo de vida de claves criptográficas:** generación, distribución, almacenamiento, utilización y destrucción de las mismas.
- **Definición de algoritmos criptográficos y parametrización o fortaleza de claves:** establecer cuáles son los algoritmos criptográficos permitidos y su parametrización, como por ejemplo las longitudes de claves. La política criptográfica puede referenciar a otros estándares o normativas como referencia (**CCN-STIC 221**[1], **CCN-STIC 807**, **CCN-TEC 009 BP37**[2], etc.). Asimismo, se deben incluir el uso de protocolos criptográficos y las versiones mínimas permitidas.

2.2. Identificación de actores relevantes

El plan de transición debe involucrar a múltiples unidades organizativas y proveedores o entidades externas, de forma que el plan de transición sea completo y alineado con la industria.

En este apartado se enumerarán la tipología de actores, tanto externos como internos, relevantes en el proceso de transición a criptografía resistente a la amenaza cuántica y que cada organización deberá identificar según su ámbito geográfico, industria de aplicación o servicios prestados.

2.2.1. Actores externos

- **Organismos reguladores:** juegan un papel fundamental en la adopción y obligado cumplimiento de mecanismos de seguridad. Pueden ser organismos públicos, como la Unión Europea con normativas como el **DAS**, **CSA**, **CRA**, **RGPD**, **NIS2** o **DORA**, entre otras; u organismos privados o sectoriales como **PCI-DSS** (*Payment Card Industry Data Security Standard*).
- **Entidades de estandarización:** juegan un papel importante en el uso y aplicación de criptografía postcuántica. Algunos ejemplos relevantes son el **NIST** en la estandarización de algoritmos postcuánticos, **IETF**, **ISO**, **ETSI**, etc.
- **Entidades de certificación:** evalúan el correcto cumplimiento de estándares y normativa aplicable. Para muchas actividades empresariales y líneas de negocio es indispensable encontrarse debidamente certificado por una entidad certificadora reconocida. Un ejemplo es la certificación en **ENS**[3] nivel alto que evalúa el cumplimiento del Esquema Nacional de Seguridad, elaborado por el **CCN** en España. Las entidades deben ejecutar el plan de transición postcuántico para garantizar el cumplimiento de los estándares y normativas.
- **Proveedores externos:** la cadena de suministro es una parte fundamental de la seguridad de las organizaciones y ha crecido en complejidad debido a un amplio ecosistema de dependencias e interrelaciones. Para garantizar la seguridad integral, es indispensable que todos los proveedores externos se adecúen a las políticas criptográficas de la organización y se establezcan criterios de evaluación y acuerdos con proveedores que garanticen una correcta implementación de criptografía postcuántica en sus productos y servicios. Para facilitar esta labor, se podrá consultar en la **CCN-STIC 105 CPSTIC**[4] , aquellos

productos y servicios cualificados o aprobados que implementen criptografía resistente a la amenaza cuántica.

- **Grupos de trabajo y comunidad científica:** la colaboración con grupos de trabajo o investigación permite compartir conocimiento, estar informado de los últimos avances tecnológicos y poder invertir de forma efectiva en investigación, desarrollo e innovación (**I+D+i**). La colaboración impulsa el desarrollo de la industria y la confianza en los avances tecnológicos, de suma importancia en el ámbito de la criptografía.
- **Clientes y/o usuarios finales:** estos también deben estar adecuadamente identificados, con el objetivo de ofrecerles productos y servicios seguros, haciendo uso de criptografía postcuántica, así como comunicarles de forma efectiva cómo esta contribuye a la protección de los activos de información gestionados.

---

[1] *Guías CCN-STIC:* https://www.ccn-cert.cni.es/es/guias.html

[2] *Recomendaciones para una transición postcuántica segura:* https://www.ccn.cni.es/es/menu-pytec-es/pildoras-tecnologicas-pytec

[3] *Esquema Nacional de Seguridad:* https://ens.ccn.cni.es/es/

[4] *Catálogo de Productos y Servicios TIC del CCN:* https://cpstic.ccn.cni.es/es/

2.2.2. Actores internos

A continuación, se ofrece una propuesta para la definición de roles y responsabilidades que deberá adaptarse en cada institución:

- **Comité de dirección postcuántico:** formado por órganos de gobierno como el consejo de administración o la junta directiva. Define el marco de gobernanza y establece los objetivos estratégicos de la organización y la tolerancia al riesgo. Aprueba las políticas de seguridad y la asignación de recursos. Para que el plan de transición cuántico sea efectivo, debe ser respaldado por los órganos de gobierno e incluido en las políticas criptográficas y presupuestos.
- **Oficina de Programa PQC:** liderada por la figura del **CISO** o **CIO**, es la encargadoa de definir las políticas criptográficas de la organización, validar los planes de actualización de diferentes protocolos y sistemas y establecer directrices o guías de aplicación para la migración postcuántica. Asimismo, lidera el análisis de riesgos de la organización, estableciendo una priorización de activos según su criticidad, y monitoriza el estado de cumplimiento y grado de alineación con las políticas criptográficas. Verificará que las políticas criptográficas se

encuentren alineadas con los requisitos legales, regulatorios y contractuales de aplicación para cada caso.

Equipo técnico especializado: engloba los diferentes equipos y unidades que operan sus líneas de negocio específicas y que gestionan sus propias operaciones y recursos. Cada equipo técnico puede constituirse con múltiples técnicos especializados en arquitectura, desarrollo, sistemas e infraestructuras, operaciones, etc. El equipo técnico especializado debe conocer los productos y servicios ofrecidos y el nivel de riesgo asociado y alinearse con las políticas de seguridad organizativas para planear y ejecutar el plan de migración postcuántico.

Responsables de dominio/aplicación: serán los encargados de ejecutar los planes de migración en cada uno de los productos y servicios impactados en su ámbito, siguiendo las directrices y guías de implantación definidas por la oficina de programa **PQC**.

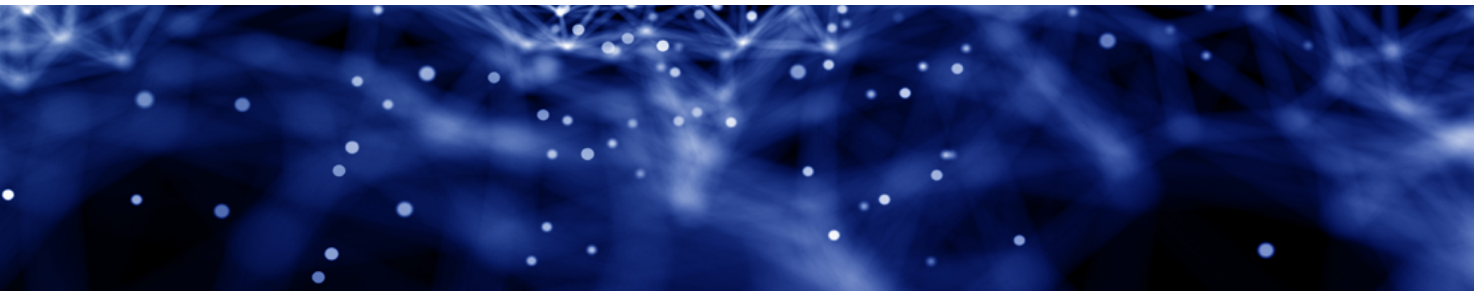
2.3 Diagnóstico inicial e inventario de activos

Una vez iniciado el plan de transición a la criptografía postcuántica, establecidos los objetivos estratégicos y las políticas criptográficas, e identificados los principales actores relevantes del proceso; el siguiente paso consiste en realizar un **diagnóstico inicial de la situación actual de la organización en materia de criptografía**.

Estas acciones tienen como objetivo recopilar toda la información necesaria para establecer un inventario de activos criptográficos, también denominado **CBOM (*Cryptographic Bill Of Materials*)**, así como un mapa de dependencias, que permita posteriormente elaborar un análisis de riesgos y evaluar de forma efectiva el riesgo cuántico al que se enfrentan los activos. De este modo, se podrá establecer una priorización para la ejecución del plan de migración.

A efectos de inventario criptográfico y diagnóstico inicial, se entiende por **activo criptográfico** cualquier elemento, *hardware* o *software*, que intervenga en la protección, generación, gestión, aplicación o soporte de mecanismos criptográficos dentro de la organización. A grandes rasgos, se puede establecer la siguiente taxonomía:

- **Datos protegidos mediante criptografía:** activos de información digital cuya confidencialidad, integridad y/o autenticidad dependen del uso de criptografía. Incluye tanto datos en reposo (p. ej. cifrado en disco, bases de datos cifradas, ficheros firmados digitalmente, etc.) como datos en tránsito (comunicaciones **TLS**, **SSH**, **IPsec**, etc.).
- **Productos, componentes y servicios que aplican criptografía:** se trata de los activos, productos y servicios, ya sean *hardware*, *firmware* o *software*, que aplican criptografía mediante el uso de protocolos criptográficos, algoritmos y bibliotecas criptográficas, módulos criptográficos, etc. Asimismo, en este grupo de activos se han de tener en cuenta las propias claves criptográficas y certificados digitales. En este grupo se encuentran sistemas de gestión de claves (**KMS**), módulos de seguridad *Hardware* (**HSM**), infraestructuras de clave pública (**PKI**), bibliotecas criptográficas (p. ej. OpenSSL, BouncyCastle, etc.), protocolos (p. ej. **TLS1.3**, **SSH**, **IKEv2**, etc.) y cualquier otro servicio que haga uso de criptografía, así como las claves criptográficas utilizadas.
- **Proveedores externos:** terceras partes que pertenecen a la cadena de suministro y que facilitan o gestionan componentes, productos o servicios donde se utiliza criptografía. Puede comprender desde hiperescalares cloud, entidades de certificación o infraestructuras de clave pública externas, proveedores de servicios cualificados, servicios de almacenamiento cifrado o cualquier plataforma SaaS o PaaS con la que se establezcan comunicaciones cifradas. Las políticas de seguridad deben incluir criterios de evaluación criptográfica de los proveedores, que incluyan requisitos de soporte a algoritmos postcuánticos, de cripto-agilidad y garantizar el cumplimiento a través de acuerdos con los proveedores de servicios.



2. Etapa 1: Preparación para la transición postcuántica

La creación y mantenimiento del inventario de activos criptográficos es una de las tareas más complejas y laboriosas a las que se enfrentan las organizaciones en la etapa inicial, debido a la gran cantidad de activos criptográficos con los que puede llegar a contar. Es indispensable contar con un inventario completo y que muestre una **visión realista del estado de ciberseguridad de la organización**, con el objetivo de identificar si dichos activos son vulnerables a ataques cuánticos y a qué riesgo se enfrentan para poder tomar una decisión de la estrategia a considerar.

La utilidad del inventario de activos criptográficos va más allá del plan de transición, ya que puede ayudar a identificar otras vulnerabilidades, como uso de protocolos o versiones inseguras. Por ello, la creación y mantenimiento de este inventario de activos criptográficos debe ser algo definido a nivel global en las políticas de seguridad de la organización.

Para cada activo criptográfico, se deben extraer una serie de datos, que pueden variar en función de la tipología del activo. A grandes rasgos deben ser suficientes para identificar el riesgo criptográfico y el grado de protección frente a amenazas del que dispone dicho activo. A modo de referencia se pueden extraer algunos datos como:

- **Tipología del activo:** define si el activo es un producto, protocolo, biblioteca, datos (en reposo, en tránsito o en uso), claves criptográficas o certificados digitales.
- **Localización del activo:** ubicación física y/o lógica del activo criptográfico.
- **Valor de los datos:** define las dimensiones de seguridad más importantes para el activo: confidencialidad, integridad, autenticidad o disponibilidad.
- **Clasificación del activo:** clasificación de seguridad del activo (Secreto, Reservado, Confidencial, Difusión Limitada o Público; o equivalentes).
- **Algoritmos criptográficos y fortaleza de claves:** algoritmos criptográficos utilizados y longitud o fortaleza de las claves utilizadas. Por ejemplo, **AES** con claves de 256 bits, **RSA** módulo 4096 o las CIPHER_SUITES permitidas en **TLS**.
- **Versiones de protocolos y bibliotecas criptográficas:** determinadas versiones de protocolos y bibliotecas criptográficas pueden contener vulnerabilidades de seguridad si no se actualizan debidamente. Por ello, se debe anotar en el inventario la versión de la biblioteca criptográfica utilizada (p.ej. OpenSSL o BouncyCastle) y la versión del protocolo utilizado (p. ej **TLS 1.3**).

Junto con el inventario de activos criptográficos, es necesario definir el mapa de dependencias, que permitirá establecer las interrelaciones entre los activos criptográficos del inventario y agruparlos en base a dependencias comunes. Por ejemplo, el mapa de dependencias puede indicar los activos criptográficos que dependen de un proveedor externo, de una misma infraestructura **PKI**, de una biblioteca criptográfica, etc.

Debido a la complejidad de la tarea de creación y mantenimiento del inventario de activos criptográficos y la heterogeneidad de las organizaciones, **cada organización debe definir la estrategia que mejor se adapte a sus características**. De forma genérica, se puede establecer el siguiente marco metodológico:

1) **Definición del objetivo de la tarea de inventariado:** los objetivos pueden ser cumplimiento normativo, descubrimiento inicial, actualización u otros motivos.

2) **Definición del alcance:** determina que tipo de activos criptográficos son incluidos en la tarea de creación o mantenimiento de inventario.

3) **Definición de metodología:** puede ser un descubrimiento de activos criptográficos automatizado o semiautomatizado mediante análisis de tráfico, escaneo de puertos y sistemas, análisis de almacenamiento, análisis de código, etc. o puede ser un proceso manual en el que cada equipo o unidad de negocio identifica sus activos criptográficos. En este punto se seleccionan las herramientas adecuadas para llevar a cabo el inventario y se dividen las tareas entre los miembros de la organización.

4) **Definición de análisis de datos:** determina la información requerida para cada activo de información.

5) **Definición de reportes:** determina cómo la información recolectada se inventaria, almacena y actualiza para su análisis. Define el formato y la estructura de datos.

6) **Definición de política de actualización:** determina cómo y cada cuánto tiempo el inventario debe ser revisado y actualizado, asegurando que sigue reflejando una visión actual de los activos de la organización. Incluye los mecanismos de alta de nuevos activos criptográficos, modificación o baja de activos.

2.3.1. Descubrimiento automatizado y formato CBOM

Debido a la gran cantidad de activos criptográficos con los que puede contar una organización y la complejidad de la tarea de inventariado de los mismos, una de las áreas más importantes es la de creación de procesos automatizados o semiautomatizados de descubrimiento de activos criptográficos y generación y mantenimiento del inventario.

Una de las iniciativas en este ámbito, la lleva a cabo el **NIST** a través del **NCCoE** (*National Cybersecurity Center of Excellence*) con la publicación de las publicaciones especiales **NIST SP 1800-38**, que consta de tres documentos identificados como A, B y C.

En estos documentos se analiza el proceso de descubrimiento de activos criptográficos y algoritmos vulnerables; se define el formato de inventario **CBOM** de forma que sea procesable por sistemas y se incluyen pruebas con herramientas de diferentes proveedores tecnológicos.

Estos documentos identifican tres posibles escenarios en donde se pueden utilizar herramientas automatizadas o semiautomatizadas de descubrimiento de activos criptográficos:

- **Desarrollo de *Software*:** el empleo de bibliotecas criptográficas facilita a los desarrolladores de *software* el uso de primitivas criptográficas en las aplicaciones, desde creación de claves, hasta cifrado o firma digital. Algunas de las bibliotecas criptográficas más utilizadas son OpenSSL, BouncyCastle, Libsodium, Crypto++, wolfCrypt.



Sin embargo, el uso de bibliotecas criptográficas maduras no implica el uso correcto de las mismas. Un mal uso puede suponer vulnerabilidades de seguridad, como por ejemplo uso de algoritmos obsoletos, uso de modos o parametrizaciones débiles o incorrectas, reutilización de claves o vectores de inicialización, uso de claves o secretos en código, etc.

En este ámbito, la utilización de **analizadores de código estáticos o dinámicos** es de uso extendido y recomendado en el sector. Estos analizadores pueden detectar vulnerabilidades en el código por empleo incorrecto de las bibliotecas criptográficas o el uso de versiones obsoletas de la biblioteca. Asimismo, pueden permitir el análisis e inventariado de uso de criptografía en las aplicacionexs de una organización. Es recomendable que estos analizadores se incorporen en **procesos de integración y despliegue continuo (CI/CD)**, de forma que se puedan detectar vulnerabilidades introducidas en código nuevo y tener un seguimiento continuo e inventariado en tiempo real del estado del uso de criptografía en las aplicaciones de la organización.

- **Sistemas y aplicaciones:** estos hacen uso de criptografía de forma habitual, ya sea para el establecimiento de comunicaciones cifradas, cifrado de datos en reposo, firma digital, arranque seguro, etc. Los documentos del **NIST** establecen una clasificación entre ejecutables y no ejecutables.

  Los ficheros ejecutables incluyen *software*, *hardware*, *firmware* y bibliotecas criptográficas. Es habitual en estaciones de trabajo y servidores encontrar dependencias base de bibliotecas criptográficas en el propio sistema operativo. Los ficheros no ejecutables son objetos de sistema operativo referenciados por las aplicaciones y el *software*. Los activos criptográficos de ficheros no ejecutables pueden ser claves, certificados o almacenes de claves (p. ej. **PKCS#12**, **JKS**, etc.).

  En este ámbito, se pueden ejecutar **analizadores de almacenamiento** para detectar ficheros ejecutables y no ejecutables que deban considerarse en el inventario de activos criptográficos.

- **Tráfico de red:** es posible escanearlo mediante **analizadores de tráfico o *sniffers***. Permiten escanear una red y detectar qué algoritmos criptográficos se están usando y entre qué sistemas se establecen las comunicaciones. Es importante identificar cada protocolo de red utilizado y verificar si se está utilizando un protocolo seguro criptográficamente. Asimismo, se deben considerar todos los niveles de comunicación de la capa OSI a la hora de analizar el tráfico de red. Otras herramientas que se pueden utilizar son los escáneres de puertos para detectar el uso de protocolos criptográficos vulnerables por parte de las aplicaciones.

Debido a las múltiples tipologías de activos criptográficos y herramientas de descubrimiento, se hace indispensable el uso de un estándar a la hora de definir el inventario o **CBOM**, de forma que su procesamiento pueda ser gestionado por máquinas de forma automática o semiautomática. En la actualidad, el formato definido por **CycloneDX**, que forma parte del proyecto OWASP, es la especificación más utilizada para la construcción de **CBOM** en formato procesable. Este formato es un estándar ECMA en la versión 1.6 (**ECMA-424**) e incluye la criptografía utilizada, metadatos identificativos y dependencias.

Un **CBOM** puede proporcionar descripciones muy detalladas de activos criptográficos de distintos tipos: protocolos y algoritmos criptográficos, claves criptográficas, datos cifrados, certificados digitales, firmas digitales, hashes, vectores de inicialización, *tokens*, credenciales, etc. En la siguiente imagen se representa la estructura de definición de activos criptográficos en **CBOM**:

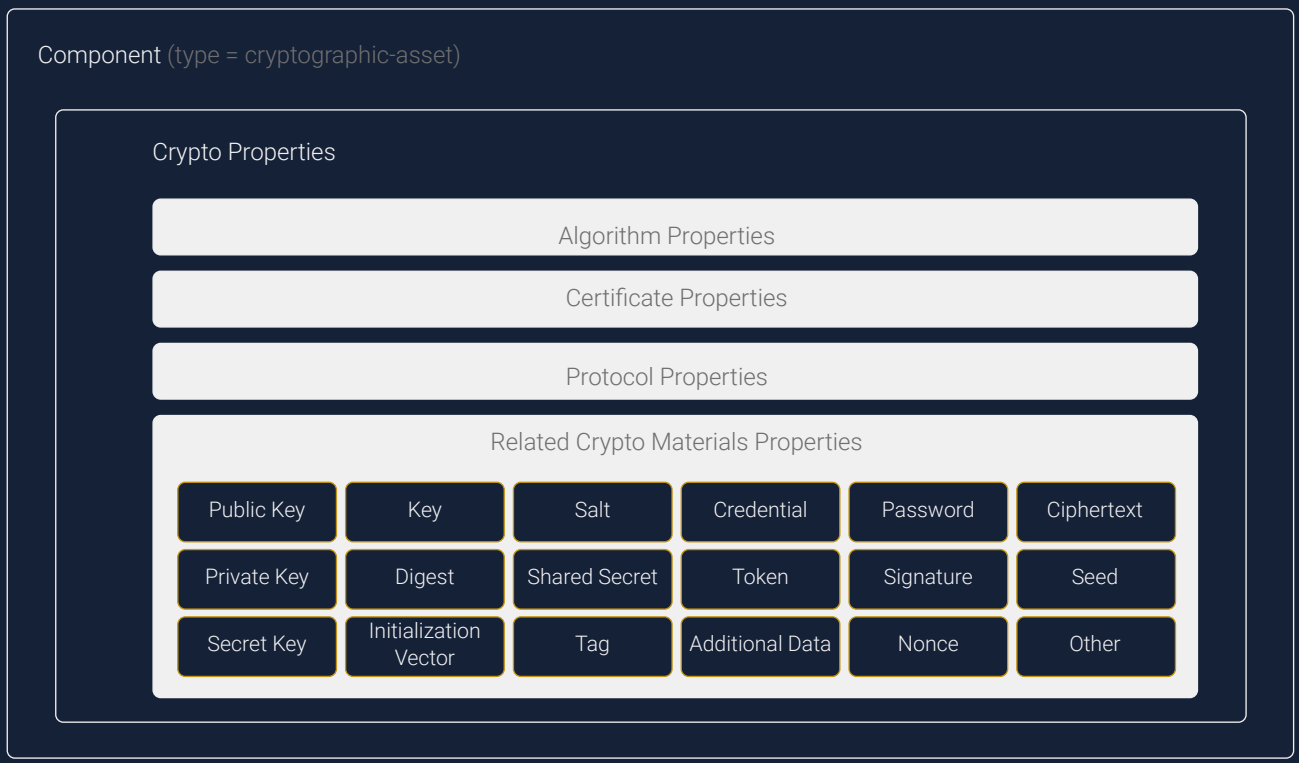


Ilustración 4. Estructura y tipos de activos CBOM CycloneDX

Cabe destacar que aunque el uso de herramientas automatizadas o semiautomatizadas sea de gran utilidad, se debe compaginar con el análisis manual para comprobar los resultados obtenidos y complementar con los activos criptográficos que quedan fuera del alcance de las herramientas o con información de contexto adicional, como las interdependencias. Por ejemplo, en las claves y otros activos criptográficos contenidos en *hardware* seguro como **HSM** o **TPM** o en soluciones de gestión de claves **KMS** o infraestructuras **PKI**.

2.4. Análisis del riesgo cuántico y priorización de activos

Los criterios de clasificación del riesgo cuántico y su correspondencia con los niveles alto, medio y bajo que recoge este apartado tienen carácter transitorio y orientativo, en los términos indicados en el resumen ejecutivo.

Una vez elaborado el inventario de activos criptográficos y que la organización haya logrado una mayor visibilidad sobre la criptografía utilizada, el siguiente paso es el de evaluar el riesgo cuántico sobre dichos activos, con el objetivo de poder establecer una priorización de activos sobre los que aplicar salvaguardas e implementaciones postcuánticas en primer lugar.

En este apartado se establece una metodología de análisis del riesgo cuántico sobre los activos criptográficos basada en tres aspectos fundamentales:

- **Análisis de vulnerabilidad cuántica:** valora la fortaleza de los algoritmos criptográficos utilizados frente a ataques conocidos en la actualidad que puedan ser llevados a cabo por un ordenador cuántico **CRQC**.

- **Análisis de impacto:** valora el impacto que tendría la ruptura de la criptografía de los activos criptográficos. Se basa en las consecuencias de la vulneración de activos de información en cualesquiera de las dimensiones de seguridad,clasificando dichos activos por orden de importancia, en cuanto al impacto sobre la confidencialidad, integridad o autenticidad.
- **Tiempo y esfuerzo estimado de la migración postcuántica:** estimación de tiempo y/o esfuerzo requerido para llevar a cabo la migración a criptografía postcuántica. Las estimaciones se pueden basar en los retos conocidos de llevar a cabo la migración debido a su complejidad o a migraciones ejecutadas con anterioridad. El análisis de tiempos y esfuerzos es necesario a la hora de valorar la priorización en la migración de activos debido a la posibilidad de ejecución de ataques **HNDL** por parte de atacantes.

A continuación, se establecerán unas guías para la evaluación de las tres dimensiones del análisis de riesgo cuántico citadas. Asimismo, con posterioridad, se establecerá un procedimiento para otorgar una puntuación de riesgo para los activos criptográficos en base a los valores obtenidos en cada dimensión.

2.4.1. Análisis de vulnerabilidad cuántica

Este **debe valorar la resistencia de los algoritmos criptográ icos** frente a ataques cuánticos, es decir, llevados a cabo por un ordenador cuántico **CRQC** utilizando los ataques conocidos en la actualidad, por ejemplo, mediante la ejecución de los algoritmos de Shor para criptografía asimétrica o de clave pública.

También deben considerarse las vulnerabilidades de los algoritmos derivadas de ataques no cuánticos. Muchos algoritmos postcuánticos son relativamente recientes y no han estado expuestos a criptoanálisis durante periodos prolongados. Por tanto, una exposición más prolongada a criptoanálisis podría revelar nuevas vulnerabilidades en estos algoritmos.

Asimismo, es importante tener en cuenta que muchos protocolos criptográficos utilizan una combinación de algoritmos criptográficos. Por ejemplo, **TLS** utiliza cipher suites que se componen de algoritmos criptográficos para intercambio de claves (p. ej. **ECDH**), autenticación (p. ej. **RSA**), cifrado (p. ej. **AES GCM**) y *hashing*

o MAC (p. ej. **SHA-256**). En estos casos, hay que diferenciar si los múltiples algoritmos criptográficos se utilizan en una construcción híbrida o no. En el caso de que se utilice una construcción híbrida, la vulnerabilidad cuántica será la mínima otorgada por el algoritmo más robusto utilizado en la construcción híbrida. En el caso de que no se utilice una construcción híbrida, la vulnerabilidad cuántica será la máxima otorgada por el algoritmo más débil utilizado.

A continuación, se establece una **clasificación de puntuación sobre la vulnerabilidad cuántica de los algoritmos**:

PUNTUACIÓN	DESCRIPCIÓN
0	El algoritmo utilizado no presenta vulnerabilidades prácticas conocidas frente a ataques cuánticos o tradicionales. No requiere migración en base al estado actual del conocimiento.
1	El algoritmo no se encuentra en peligro todavía de ser roto por completo por un ataque de un ordenador cuántico **CRQC**, pero puede disminuir su seguridad y requerir atención en el futuro. Por ejemplo, existen ataques cuánticos frente a la criptografía simétrica, que reducen la seguridad a la mitad. Se recomienda utilizar longitudes de clave mayores, pero se deben priorizar las migraciones de algoritmos criptográficos que serán rotos por completo por ataques cuánticos.
2	El algoritmo utilizado no es seguro frente a ataques cuánticos o tradicionales. Necesita ser migrado a una alternativa postcuántica segura.

Tabla 1. Puntuaciones vulnerabilidad cuántica.

En el **Anexo I: Tabla de vulnerabilidad cuántica** se incluye una tabla con varios algoritmos criptográficos conocidos y la puntuación de vulnerabilidad cuántica asignada.

2.4.2. Análisis del impacto

El análisis de impacto pretende cuantificar las consecuencias para la organización en el caso de que la criptografía que utiliza se vea rota.

La organización debe realizar un **análisis del impacto de compromiso de sus activos de información en alguna o todas las dimensiones de seguridad: disponibilidad, confidencialidad, integridad, trazabilidad o autenticidad**. Se deben tener en cuenta desde aspectos normativos y regulatorios hasta aspectos relacionados con la reputación de la organización. Por ejemplo, una organización puede tener un impacto económico directo si se ve expuesto su sistema de licenciamiento; o si se exponen datos personales de usuarios o clientes puede suponer una multa administrativa y un impacto reputacional sobre la marca de la organización.

Asimismo, otro aspecto a tener en cuenta a la hora de analizar el impacto es el de identificar si existen atacantes que, cuando existan ordenadores cuánticos **CRQC**, tengan como objetivo a la organización y sus activos criptográficos o de información. Por un lado, se deben analizar las posibilidades de que exista un ordenador **CRQC** en un horizonte temporal determinado (de 5 o 10 años), en base a los desarrollos y avance actual de la computación cuántica. Por otro lado, cuando exista este ordenador, tendrá un coste demasiado elevado como para que lo pueda utilizar cualquier atacante. Por tanto, durante los primeros años y hasta que se extienda un uso más generalizado de *Quantum as a Service* (**QaaS**), los posibles atacantes pueden ser actores estatales, cuyo objetivo sean las infraestructuras críticas de los países o secretos oficiales.



A continuación, se establece una **clasificación de puntuación sobre el impacto de los ataques cuánticos sobre activos criptográficos**:

PUNTUACIÓN	DESCRIPCIÓN
1	No hay impacto significativo que requiera atención, o el impacto es bajo. Puede ser por varias causas: • La sensibilidad del sistema o activo criptográfico no es elevada. • La posibilidad de materialización de la amenaza antes de 10 años es muy baja y la protección de la información o sistema no requiere un ciclo de vida tan extenso. • No existen intereses realistas por parte de un atacante cuyo objetivo pueda ser el activo criptográfico en el corto-medio plazo. • Existen medidas de protección complementarias.
2	Existe un impacto significativo y un interés realista por parte de potenciales atacantes, pero no en el corto plazo. Por ejemplo: • Existe un atacante con interés realista en el activo criptográfico que tiene acceso a poder interceptar los datos y poder descifrarlos cuando esté disponible un ordenador **CRQC**, pero los datos no tendrán elavada relevancia o impacto en el horizonte temporal planteado (10-20 años). • El compromiso del sistema no se puede llevar a cabo de manera retroactiva. Es decir, el riesgo se materializará cuando exista un ordenador **CRQC**. Por ejemplo, ataques sobre firmas digitales en sistemas de autenticación, instalación de actualizaciones, etc.
3	El impacto es muy elevado y necesita ser mitigado de forma inmediata. Por ejemplo: • Existe un atacante con interés realista en el activo criptográfico que tiene acceso a poder interceptar los datos y poder descifrarlos cuando esté disponible un ordenador **CRQC**. • Los datos interceptados siguen siendo sensibles en el horizonte temporal cuando esté disponible un ordenador **CRQC**. Es decir, el compromiso de dichos activos tiene impacto significativo en el negocio o en las personas dentro de 10-20 años. • Algunos ejemplos: secretos de Estado, propiedad intelectual, contratos confidenciales, datos de carácter personal sensibles, etc.

Tabla 2. Puntuaciones del impacto de los ataques cuánticos.

Un ejemplo de análisis de impacto, asumiendo que existe un atacante con intereses realistas cuando exista un ordenador cuántico **CRQC**, podría ser el siguiente:

- **Impacto sobre confidencialidad:** activos criptográficos o de información sobre los que prima mantener la confidencialidad, puede tratarse de comunicaciones (información en tránsito) o datos cifrados almacenados (información en reposo).
  - **¿El potencial atacante tiene acceso a la información cifrada?** Ya sea mediante intercepción de las comunicaciones o acceso a los medios de almacenamiento cifrados.
    - NO: **puntuación de impacto 1**. Existen medidas de protección adicionales, como segmentación de redes.
    - SI: ¿La confidencialidad de la información se debe mantener más de 10 años?, es decir, cuál es el impacto de revelación de la información una vez pasados 10 años.
      * Si la información sigue siendo sensible pasado el horizonte temporal: **puntuación de impacto 3**. Existe un alto riesgo de ataques **HNDL**.
      * Si la información ya no es sensible pasado el horizonte temporal: **puntuación de impacto 2**. Existe un alto riesgo de ataques **HNDL**, pero para cuando se materialice la amenaza el impacto es menor o no significativo.
- **Impacto sobre integridad:** activos criptográficos o de información sobre los que prima mantener la integridad, puede tratarse de actualizaciones de *software*, cadena de custodia de activos criptográficos, etc. En estos casos, el impacto es elevado desde el momento que se materialice la amenaza de un ordenador cuántico **CRQC**. **Puntuación de impacto 2**.
- **Impacto sobre autenticidad:** sistemas o activos criptográficos que hacen uso de criptografía para autenticar o establecer identidades. Es el caso de los algoritmos criptográficos de firma digital.
  - ¿La firma digital debe seguir siendo válida pasados 10 años?
    - En caso negativo: **puntuación de impacto 1**. Existe riesgo únicamente a partir de la materialización de la amenaza de un ordenador cuántico **CRQC**.
    - En caso afirmativo: **puntuación de impacto 2**. Riesgo alto de ataques materializados cuando exista un ordenador cuántico **CRQC**.
  - Otros mecanismos de autenticidad y/o autenticación. Valorar con **puntuación de impacto 1 o 2**, en función del activo, su criticidad y el tiempo de validez de la autenticación. El riesgo existe únicamente a partir de la materialización de la amenaza de un ordenador cuántico **CRQC**.

2.4.3 Análisis de esfuerzo estimado para la migración

Por último, se debe valorar el **esfuerzo en tiempo y recursos para la realización de migración** de los activos criptográficos a criptografía postcuántica. En cualquier proyecto y migración, es esencial el cálculo de tiempos y esfuerzos económicos y humanos necesarios para la ejecución del mismo; sin embargo, en el en caso de la migración a criptografía postcuántica, es indispensable, ya que como se vio en el teorema de Mosca, **el tiempo de migración y la vida útil de la información son dos aspectos fundamentales a tener en cuenta a la hora de valorar el riesgo cuántico**. A mayor tiempo de migración y/o vida útil de la información, mayor es la probabilidad de que los activos criptográficos puedan ser afectados por ataques de tipo **HNDL**.

A continuación, se establece una **clasificación de puntuación sobre el esfuerzo en tiempos de realización de la migración a criptografía postcuántica**:

PUNTUACIÓN	DESCRIPCIÓN
1	No se esperan mayores inconvenientes en la migración y se puede completar la migración a una alternativa segura resistente a la amenaza cuántica en menos de dos años.
2	La migración no es trivial, pero no se esperan factores bloqueantes. Se puede completar en menos de 6-8 años.
3	La migración será dificultosa y se puede extender en el tiempo a causa de múltiples factores, por ejemplo: • Multitud de interdependencias o proveedores externos. • Falta de prioridad sobre el activo criptográfico • Componentes heredados (*legacy*) En este caso, la migración se espera que no esté completa antes de 6-8 años.

Tabla 3. Puntuaciones sobre el esfuerzo en tiempos de realización de la migración.

Los tiempos de migración de los activos criptográficos pueden variar enormemente en función de la organización y de los tipos de activos criptográficos. Algunos de estos factores pueden ser: la madurez de la organización, dependencias externas en estándares o regulaciones, dependencias de proveedores externos, dependencias de módulos *hardware*, activos con capacidades limitadas *hardware* o *software*, código no mantenido, etc.

2.4.4. Puntuación de riesgo cuántico y nivel de riesgo del sistema

Por último, las tres puntuaciones obtenidas anteriormente se deben combinar en una **puntuación global de riesgo cuántico**. Una vez se haya calculado el riesgo cuántico las organizaciones deben establecer una **priorización de activos** y empezar a planificar el proceso de migración. Se debe tener en cuenta que, en función de la tolerancia al riesgo o apetito de riesgo de la organización, éstas pueden decidir si acometer con mayor o menor urgencia las tareas de migración, en especial para los activos de menor riesgo.

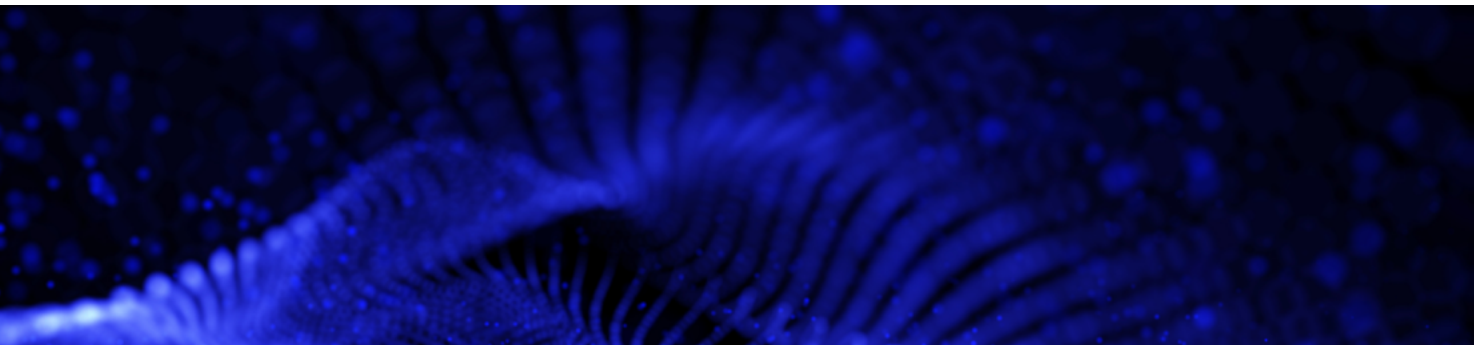
A continuación, se establece una **clasificación de puntuación del riesgo cuántico** con su significado correspondiente:

PUNTUACIÓN	DESCRIPCIÓN
0 (Sin Riesgo)	No se identifica riesgo cuántico relevante.
1 (Riesgo Bajo)	Puede existir riesgo cuántico en el largo plazo, pero no es prioritario atenderlo.
2 (Riesgo Medio)	Existe riesgo cuántico y se necesitan tareas de migración, pero la criptografía actual es segura hasta la materialización de la amenaza de un ordenador cuántico **CRQC** o las tareas de migración se esperan que sean rápidas y sencillas.
3 (Riesgo Alto)	Existe riesgo cuántico y se necesita priorizar la migración de estos activos en el corto plazo debido a su impacto o tiempo elevado de migración.
4 (Riesgo Grave)	Existe riesgo cuántico en la actualidad debido a ataques **HNDL** y requieren atención inmediata. El impacto es muy elevado y el tiempo de vida útil de la información o el tiempo de migración son muy elevados y se espera que la amenaza se materialice antes.

Tabla 4. Puntuaciones riesgo cuántico.

A continuación, se establece una guía para el cálculo del riesgo cuántico en base a los valores obtenidos en las dimensiones de vulnerabilidad, impacto y esfuerzo de migración:

- **Vulnerabilidad 0:** Si no existe vulnerabilidad, no existe riesgo. Puntuación de riesgo 0.
- **Vulnerabilidad 1:** De forma general no existe riesgo cuántico en el corto plazo, aunque se pueden tomar medidas para incrementar la seguridad y fortaleza frente a ataques cuánticos. Puntuación de riesgo 1, excepto:
  - Valoración de impacto 3 y valoración de esfuerzo de migración mayor o igual que 2: **Puntuación de riesgo 2**.
- **Vulnerabilidad 2:** Los algoritmos criptográficos son vulnerables. Se debe valorar el impacto y esfuerzo de migración:
  - Valoración de impacto 1: **Puntuación de riesgo 1**, excepto si el esfuerzo de migración tiene puntuación 3, que se le asigna **puntuación de riesgo 2**.
  - Valoración de impacto 2: **Puntuación de riesgo 2**, excepto si el esfuerzo de migración tiene puntuación 3, que se le asigna **puntuación de riesgo 3**.
  - Valoración de impacto 3: **Puntuación de riesgo 4**, excepto si el esfuerzo de migración tiene puntuación 1, que se le asigna **puntuación de riesgo 3**.



En la siguiente tabla se puede observar de manera visual un mapa de calor que recoge las valoraciones de riesgo cuántico establecidas en el párrafo anterior en función de las dimensiones de vulnerabilidad, impacto y esfuerzo de migración.

VULNERABILIDAD	IMPACTO	ESFUERZO DE MIGRACIÓN	RIESGO CUÁNTICO
0	N/A	N/A	0
1	1	N/A	1
1	2	N/A	1
1	3	1	1
1	3	2	2
1	3	3	2
2	1	1	1
2	1	2	1
2	1	3	2
2	2	1	2
2	2	2	2
2	2	3	3
2	3	1	3
2	3	2	4
2	3	3	4

Tabla 5. Mapa de calor de riesgo cuántico.



Cabe destacar que el proceso de análisis de riesgo cuántico otorga una visión sobre la situación actual frente a riesgo de los activos criptográficos. **Estos análisis deben ser iterativos e irse actualizando periódicamente para reflejar la situación fidedigna de la organización**. Por ejemplo, a medida que se ejecutan las tareas de migración, la vulnerabilidad de los activos criptográficos se reducirá y por tanto su riesgo; o puede que sea necesario revisar el impacto o los tiempos de migración debido a nuevos avances tecnológicos, eficiencias, etc.

La determinación del nivel de riesgo del sistema (alto, medio o bajo), se basará en la puntuación obtenida para el riesgo cuántico. De esta manera, el sistema se clasificará en un nivel de riesgo y se priorizará la migración en función de dicha clasificación.

RIESGO CUÁNTICO	NIVEL DE RIESGO DEL SISTEMA
1	Bajo
2	Medio
3-4	Alto

Tabla 6. Nivel de riesgo del sistema.

2.5. Formación y concienciación

Otra de las acciones importantes a realizar en esta primera etapa es la de formación y concienciación. La preparación para la migración a la criptografía postcuántica exige que toda **la organización se encuentre debidamente alineada con los objetivos estratégicos y políticas criptográficas y se comprendan los riesgos de la computación cuántica** sobre los activos criptográficos actuales, así como la necesidad de planificar y abordar la migración.

Estas actividades formativas y de concienciación deben abordar a todos los actores relevantes, tanto internos como externos. En el caso de los actores internos, se debe abordar desde los equipos directivos hasta los técnicos de cada una de las áreas de negocio. Para ser efectiva, **la formación y concienciación debe estar enfocada al ámbito de responsabilidad de cada uno de los actores** y al impacto que supondrá sobre su actividad diaria. Por ejemplo, los órganos de gobierno deben comprender los riesgos, dependencias y costes para poder tomar decisiones alineadas con los objetivos estratégicos de la organización. En cambio, los equipos técnicos deben disponer de conocimientos y procesos adecuados para la ejecución de la migración y posterior operación de sistemas que hacen uso de criptográfia postcuántica.



Por otro lado, es importante mantener una **comunicación directa y constante con los actores externos**, para asegurar la alineación de los objetivos. Por ejemplo, se debe trasladar a los **proveedores** las siguientes necesidades:

- Incorporar criptografía postcuántica para cumplir con las políticas criptográficas organizativas y su correspondiente habilitación
- Mantener el cumplimiento normativo y regulatorio con las normas de aplicación
- Mantener certificaciones que incluyan nuevos requisitos de seguridad postcuántica.

También es importante impulsar la colaboración y el intercambio de conocimiento entre organizaciones. Por último, se debe **comunicar a clientes y usuarios** los cambios aplicados y cómo éstos redundan en una mejora sobre la seguridad de sus datos y aplicaciones.

Por último, las organizaciones deben interiorizar que el proceso de migración postcuántica no es un proceso puntual, sino que debe dar lugar a un **ciclo continuo de monitorización tecnológica y criptográfica**, que debe desembocar en procesos de gestión de riesgo continuos, vigilancia de aparición de nuevas vulnerabilidades y seguimiento de cambios normativos o de certificación. Este proceso continuo permitirá que la organización pueda implementar mecanismos de agilidad criptográfica en los sistemas y activos criptográficos para responder a futuras amenazas o revisiones de algoritmos y/o estándares.

2.6. Gobernanza interna

Cada entidad deberá integrar la transición en su sistema de gobernanza de la seguridad. La dirección competente aprobará la política criptográfica, asignará recursos y aceptará, cuando proceda, los riesgos residuales. El Responsable de la Seguridad propondrá y supervisará las medidas; el Responsable del Sistema dirigirá la implantación; y los Responsables de la Información y de los Servicios participarán en la priorización y aceptación de los resultados.

El plan institucional de transición será formalmente aprobado, contará con presupuesto, hitos, indicadores y responsables, y se integrará con los procesos de análisis de riesgos, continuidad, contratación, gestión de cambios, arquitectura y auditoría.

Las entidades del ámbito de aplicación del **ENS** vincularán su organización interna con las medidas aplicables correspondientes. La información de seguimiento que deba comunicarse se remitirá a la autoridad competente conforme al marco aplicable.



3. Etapa 2: Planificación de la migración

En la segunda etapa, nos centraremos en las tareas específicas relacionadas con la planificación de las acciones de migración para cada activo criptográfico.

Se presupone que la organización ha ejecutado o avanzado en las tareas definidas en el apartado de preparación para la migración postcuántica y tiene un diagnóstico de la situación actual, al menos para los activos criptográficos más críticos. Este diagnóstico incluye el inventario de activos y la clasificación según el análisis de riesgo cuántico, que servirá como punto de partida para elaborar los planes de migración.

En esta etapa, se analizarán las **opciones de actualización a criptografía postcuántica y su grado de madurez** para los activos criptográficos en el alcance del análisis, que en una primera instancia se tratará de los activos criptográficos más críticos y posteriormente se irán desarrollando sobre aquellos con una menor clasificación de riesgo. Para cada uno de ellos, se debe escoger una **estrategia de migración** o de implementación de salvaguardas para tratar o mitigar el riesgo cuántico.

Con la estrategia de migración escogida para el activo criptográfico y el plan de actualización, se elaboran los **planes de migración**, estableciendo tiempos, recursos y procedimientos detallados. Estos planes deben incluir también planes de respaldo (*backup*) y vuelta atrás (*rollback*) para poder anticiparse a posibles contingencias durante el proceso de migración.

Por último, las organizaciones, productos y servicios sujetos a normativas, estándares y/o regulaciones, deben trabajar para garantizar el cumplimiento normativo y de certificación de la solución de la criptografía postcuántica con los nuevos requisitos o auditorías que se puedan requerir.

Deberán iniciarse los proyectos piloto con carácter previo a la migración con el fin de comprobar la viabilidad de la solución. Estos pilotos y los despliegues finales deberán tener en cuenta fechas concretas que se determinan en función del nivel de riesgo del sistema. De esta manera, se deberá considerar el calendario indicado en la siguiente tabla.

Los plazos siguientes constituyen horizontes de planificación y su exigibilidad derivará, en su caso, de la normativa aplicable en cada ámbito. Respecto de las entidades sujetas a normativa sectorial y de las entidades esenciales e importantes, su graduación por riesgo, sector y viabilidad técnica y económica se establecerá mediante el instrumento sectorial correspondiente. Para los restantes sujetos constituyen referencia.

FECHA	HITOS A COMPLETAR
Antes del 31.05.2027	Inventarios iniciales de activos criptográficos Clasificación de casos de uso y pilotos planificados e iniciados en la medida de lo posible para sistemas de riesgo alto y medio
Antes del 31.12.2030	Migración completada para los sistemas de riesgo alto
Antes del 31.12.2035	Migración completada para los sistemas de riesgo medio y, en la medida de lo posible, para riesgo bajo

Tabla 7. Calendario de referencia para la transición.

La planificación deberá traducir la clasificación del riesgo en un listado priorizado de sistemas que requieren migración, a los que se les asignarán proyectos piloto. Los proyectos asociados a sistemas de riesgo alto y medio deberán planificarse e iniciarse en la medida de lo posible antes del 31 de mayo de 2027. Cada piloto deberá documentar, como mínimo, la arquitectura, objetivo, el mecanismo criptográfico empleado, la interoperabilidad, el rendimiento, la evaluación, los riesgos residuales, el plan de respaldo, el plan de reversión y los criterios de paso a producción.

3.1. Planes de actualización

Resulta fundamental la revisión o **establecimiento de los planes de actualización o alternativas seguras** desde el punto de vista de la criptografía postcuántica para un activo criptográfico determinado. Es preciso, valorar las alternativas disponibles para la implementación de salvaguardas que ayuden a tratar o mitigar el riesgo cuántico. Esta valoración debe tener en cuenta tanto los aspectos técnicos como organizativos y legales o normativos, así como el grado de madurez de la solución postcuántica. En aquellos organismos que les sea de aplicación el Esquema Nacional de Seguridad, a la hora de realizar la selección de soluciones, deberán tener en cuenta los requisitos de certificación, y técnicos que le sean de aplicación. Fuera del ámbito competencial del Centro Criptológico Nacional, los mecanismos y parámetros que este determine tendrán carácter de referencia técnica.

A continuación, se establecen varias dimensiones a tener en cuenta a la hora de valorar los planes de actualización a criptografía postcuántica para cada uno de los activos criptográficos:

- **Análisis de soluciones:** En esta dimensión se valoran las soluciones de la criptografía postcuántica disponibles para aplicar sobre el activo criptográfico. **Para un mismo activo puede ser necesario valorar múltiples soluciones**, ya sean complementarias o excluyentes.Por ejemplo, si el activo hace uso de algoritmos tradicionales vulnerables para intercambio de claves y para autenticación, se debe proveer una solución postcuántica para ambos algoritmos. En este sentido, se deben evaluar múltiples cuestiones, por ejemplo: ¿Existen soluciones de criptografía postcuántica para el activo criptográfico? ¿Qué algoritmo criptográfico postcuántico utiliza la solución propuesta? ¿Se hace uso de un esquema híbrido postcuántico o de un algoritmo postcuántico en modo individual o *standalone*?

  Las soluciones pueden ser muy diferentes en función de la naturaleza del activo. A continuación se indican algunos ejemplos:

  - **Desarrollo propio:** si depende de una solución propia, es necesario analizar la adaptabilidad de la misma para el uso de criptografía postcuántica. En muchos casos, esto implica la adaptación del código fuente. En este sentido, la aplicación de criptografía suele implementarse mediante la utilización de **bibliotecas criptográficas**. Es necesario analizar si la solución viene dada por el uso de primitivas criptográficas proporcionadas por la misma biblioteca, si es necesario actualizar su versión o si dicha biblioteca no tiene soporte para primitivas postcuánticas, si se debe migrar y hacer uso de una biblioteca criptográfica diferente que sí tenga dicho soporte.

- **Dependencias externas:** si el activo o sistema criptográfico depende de soluciones externas, ya sean comerciales o de código abierto se debe analizar con el proveedor su adaptabilidad y soporte para criptografía postcuántica. El abanico de soluciones externas puede ser muy amplio, desde módulos **HSM**, soluciones SaaS, componentes de red. En algunos casos, será necesaria una **actualización de *software* o *firmware***, junto con una correcta **gestión de la configuración**.

- **Análisis de madurez:** se deben evaluar múltiples cuestiones, por ejemplo: ¿El algoritmo o construcción criptográfica postcuántica se encuentra estandarizado? ¿La solución va en línea con las prácticas de la industria en materia de criptografía postcuántica? ¿La solución es suficientemente madura para su puesta en producción? Las respuestas a estas preguntas pueden ser variadas. El **NIST** ha estandarizado el uso de los principales algoritmos postcuánticos de encapsulamiento de claves (**ML-KEM**) y firma digital (**ML-DSA** y **SLH-DSA**); sin embargo, en la actualidad el uso de estos algoritmos en determinados protocolos criptográficos como **TLS** o **SSH**, se encuentra en muchos casos en estado de borrador o draft en organizaciones de estandarización relevantes como el **IETF**.

- **Análisis de idoneidad:** Una vez analizadas las soluciones y su grado de madurez, se debe analizar la idoneidad de la solución en el contexto actual del activo o sistema criptográfico. En este sentido, se deben evaluar múltiples cuestiones, por ejemplo: ¿Se puede implantar la solución con las limitaciones *software*/*hardware* presentes si las hubiese? ¿Cómo afectará al rendimiento? ¿La solución propuesta garantiza la compatibilidad hacía atrás si es necesario?

- **Análisis de conformidad:** Por último, se debe analizar si la solución propuesta se encuentra en línea con las normativas o regulaciones de aplicación. Si el activo criptográfico se encuentra sujeto a certificación y auditoría, se debe garantizar que la solución de la criptografía postcuántica utilizada cumple los requisitos marcados.

Para cada activo criptográfico puede darse el caso de que no existan soluciones de actualización de la criptografía postcuántica o que existan varias alternativas. Si existen varias alternativas se deben valorar para escoger la más conveniente para el activo criptográfico determinado y su contexto de aplicación. Asimismo, aunque se deba valorar cada activo de forma individualizada, una misma solución o plan de actualización puede ser de aplicación a múltiples activos criptográficos que reúnan características comunes.

A continuación, se recogen algunos posibles ejemplos de planes de actualización de activos criptográficos:

- **Servidores Linux que utilizan el protocolo SSH provisto a través de la biblioteca OpenSSH:** si el servidor utiliza una versión de OpenSSH inferior a la 9.0, entonces debe migrar a una versión igual o superior a la 9.0. OpenSSH introdujo el soporte a la construcción híbrida de intercambio de claves *sntrup761x25519-sha512* en la versión 9.0 (abril de 2022), siendo el algoritmo de intercambio de claves utilizado por defecto. A partir de la versión 9.9, OpenSSH introdujo la construcción híbrida de intercambio de claves *mlkem768x25519-sha256*, siendo el algoritmo por defecto a partir de la versión 10 (abril 2025). OpenSSH es un estándar de facto en lo referente a implementación del protocolo **SSH** en sistemas Linux y Unix, por lo que su adopción es muy extendida y se podría considerar como una solución madura. El plan de actualización debe recoger la configuración adecuada para el activo criptográfico.

- Desarrollos propios que hacen uso de criptografía a través de la **biblioteca criptográfica** BouncyCastle: si los desarrollos utilizan las implementaciones de criptografía de la biblioteca criptográfica BouncyCastle con versiones que no soportan criptografía postcuántica (Java < 1.79 o .NET < 2.5.0), se debe actualizar a versiones posteriores que cuenten con dicho soporte. Una vez actualizada la biblioteca criptográfica, se debe adaptar el desarrollo para hacer uso de soluciones de criptografía postcuántica.

- Uso de ***proxy* inverso TLS**. Muchas aplicaciones o arquitecturas de seguridad hacen uso de *proxies* inversos que actúan como terminador de conexiones **TLS**. Algunos de los proxies más conocidos son *Nginx* o *Apache HTTP server*. Estos proxies hacen uso principalmente de la biblioteca criptográfica OpenSSL para la implementación de los algoritmos criptográficos y el protocolo **TLS**. OpenSSL añadió el soporte a algoritmos criptográficos postcuánticos en la versión 3.5. Otra alternativa para hacer uso de algoritmos postcuánticos en versiones de openSSL entre la 3.0 y la 3.4 es la de hacer uso del proveedor criptográfico *oqs-provider*. Por lo tanto, en función del activo criptográfico se podría optar por la alternativa de actualizar la versión de openSSL a la versión 3.5; o bien la de utilizar una versión inferior con el proveedor *oqs-provider*. El uso de algoritmos postcuánticos no viene habilitado por defecto en los proxies como Nginx o Apache, es necesario asegurarse que se encuentran compilados contra una versión de OpenSSL con soporte a algoritmos postcuánticos y realizar los cambios de configuración pertinentes para su habilitación. Los pasos necesarios deben ser recogidos en el plan de actualización.



3.2. Estrategias de migración

A partir del análisis de riesgo cuántico y las alternativas de migración, se debe determinar cuál es la estrategia más adecuada para llevar a cabo sobre el activo.

La elección de una estrategia u otra dependerá en gran medida de cada organización y su tolerancia al riesgo. Dependerá del impacto que pueda suponer el compromiso de dichos activos, del tiempo y esfuerzo requerido para su migración y de los planes de actualización disponibles, así como su grado de madurez e idoneidad para abordar el proceso de migración con garantías operativas y de seguridad, y las restricciones técnicas o regulatorias involucradas.

A continuación, se muestran algunas estrategias de migración a criptografía postcuántica o tratamiento de riesgo:

- **Migrar:** se decide adaptar o evolucionar el uso de la criptografía del activo criptográfico, ya sea mediante el empleo de algoritmos postcuánticos o esquemas híbridos; tal y como se establezca en el plan de actualización escogido. La elección del plan de actualización no tiene carácter definitivo, una organización podría escoger la aplicación de un esquema híbrido en el corto plazo y reevaluar el activo en el medio plazo para aplicar el uso único de algoritmos postcuánticos.
- **Posponer la migración:** se decide migrar el activo criptográfico hacia la criptografía postcuántica, pero el riesgo percibido o la priorización de activos hace que dichas tareas no se acometan con carácter inmediato. No se debe confundir la elección de esta estrategia con la Cripto-Procrastinación, en esta estrategia se toma la decisión consciente de abordar la migración más adelante, asumiendo cierto nivel de riesgo. Se deben establecer fechas aproximadas para las tareas de migración o la reevaluación del activo. Asimismo, si se produce algún cambio significativo que impacte en el estado del activo, riesgo o plan de actualización, se debe proceder a dicha reevaluación y ratificar o cambiar la estrategia de migración.
- **Reemplazar:** se decide reemplazar el activo o sistema criptográfico vulnerable por otro con soporte a criptografía postcuántica.
- **Retirar:** si el activo ya no es importante o existe otra alternativa, la organización puede optar por retirar dicho activo, eliminando de esta forma el riesgo. Podría ser el caso de sistemas heredados (*legacy*) o dispositivos IoT/OT sin actualizaciones disponibles.

- **Agotar el tiempo de vida útil:** si el tiempo de vida útil del activo es corto, la organización puede optar por agotar su tiempo de vida útil y una vez se haya agotado ese tiempo, proceder a su retirada o reemplazo. Por ejemplo, podría ser el caso de sistemas no expuestos a ataques **HNDL** que se espera que agoten su tiempo de vida útil antes de la aparición de ordenadores cuánticos **CRQC**.
- **Mitigar el riesgo con acciones complementarias:** la organización puede tomar medidas complementarias que no impliquen una migración postcuántica del activo criptográfico pero que reduzcan el nivel de exposición del mismo y por tanto de su nivel de riesgo. Tras la aplicación de dichas medidas, el activo seguirá siendo vulnerable a ataques cuánticos, pero la organización puede decidir tolerar ese riesgo residual. Un ejemplo sería el de aislamiento del activo mediante segmentación de redes de seguridad, migrando el activo desde una red pública (i.e. Internet) a una red privada.
- **Tolerar el riesgo:** la organización puede decidir no tomar medidas adicionales y tolerar el riesgo de ataques cuánticos. De nuevo, no debe confundirse con Cripto-Procrastinación. En este caso la organización ha realizado el análisis de riesgos correspondiente, es consciente de los riesgos y decide deliberadamente en base a un análisis coste-beneficio no tomar medidas de tratamiento del riesgo. Asimismo, si existen cambios significativos, la organización podría reevaluar el activo y optar por una estrategia de migración o tratamiento del riesgo diferente. No obstante, cuando conforme al régimen jurídico aplicable, la posposición o la tolerancia del riesgo constituya una excepción a una obligación exigible, se someterá al régimen de excepciones previsto en la normativa aplicable y, en los casos de uso de riesgo alto, a la aceptación expresa de la autoridad competente cuando así proceda.

Una vez decidida la estrategia a llevar a cabo, se debe plasmar en el plan de migración concreto, como se verá a continuación.

3.3. Planes de migración, *backup* y *rollback*

Los planes de migración deben contemplar mecanismos de respaldo y copia de seguridad (*backup*) y vuelta atrás (*rollback*).

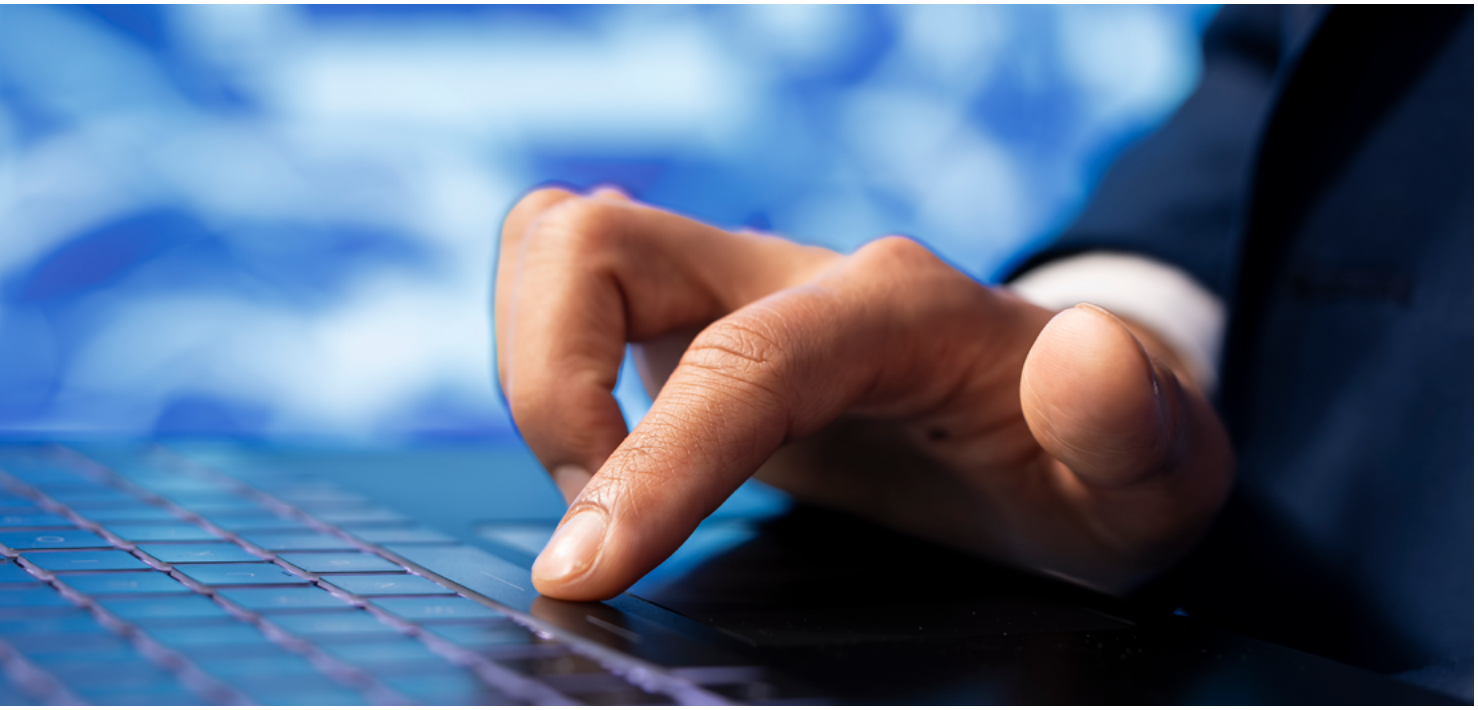
Un plan de migración detallado debe contener al menos los siguientes apartados:

- **Fechas de ejecución** de las tareas de migración y estimación de tiempos. Si es un sistema o activo productivo, se deben definir las ventanas de actualización y el tiempo máximo tolerable de parada.
- **Procesos administrativos y de negocio.** Estos procesos deben designar un responsable de la migración del activo criptográfico y un equipo responsable de la ejecución de las tareas técnicas. Para ello, es indispensable la **asignación de un presupuesto que contemple los recursos tanto humanos como materiales** necesarios para la migración.
- **Análisis de dependencias.** A partir del mapa de dependencias de activos criptográficos elaborado durante la fase de inventariado, se debe establecer un orden de migración entre los distintos activos interrelacionados. Antes de ejecutar el plan de actualización, se debe asegurar que los activos que suponen una dependencia de éste ya han sido migrados.
- **Plan de actualización detallado** en función de la estrategia de migración escogida. Se recogerán las tareas técnicas definidas paso por paso. El plan de actualización podría contar con varias fases. Por ejemplo, una primera fase con un esquema híbrido para, en una fase posterior, utilizar únicamente algoritmos postcuánticos.
- **Plan de *backup*.** Se debe establecer un plan de copias de seguridad, de forma que se disponga de una instantánea actualizada del estado del activo o sistema criptográfico justo antes de proceder con las tareas de ejecución de la migración.



- **Plan de *Rollback*.** En el caso de encontrarse dificultades durante el proceso de migración, tales como exceder el tiempo permitido para la ventana de actualización, errores durante el proceso de actualización, fallos de interoperabilidad, etc. se debe contar con un plan de vuelta atrás que permita retornar el activo criptográfico al último estado correcto conocido. El plan de vuelta atrás puede consistir en la restauración de una copia de seguridad o en la reversión de los pasos de migración ejecutados.
- **Plan de pruebas y aceptación.** Última fase de pruebas destinada a asegurar que la solución aplicada sigue cumpliendo con los requisitos funcionales, operativos y de seguridad del activo criptográfico, así como las posibles interdependencias con otros activos o sistemas. Estas pruebas deben concluir en la aceptación del activo con la solución de criptografía postcuántica para su puesta en producción.

Al finalizar la elaboración del plan de migración, se contará con procedimientos documentados y asignados para poder proceder a la ejecución de las tareas de migración de manera segura, ordenada y verificable, minimizando riesgos y asegurando la continuidad operativa de los procesos de negocio.



4. Etapa 3: Ejecución de la migración

La última etapa consiste en la ejecución del plan de migración elaborado durante la etapa anterior. En esta fase, la organización ya tendrá un conocimiento completo del inventario de activos criptográficos y su exposición al riesgo cuántico, así como las alternativas de actualización y el plan de migración concreto, con su presupuesto, procedimientos detallados y planes de *backup* y *rollback*.

En esta etapa la organización ya ha ganado una madurez suficiente en lo relativo a criptografía postcuántica y todos los actores relevantes están debidamente formados y concienciados y se encuentran alineados con los objetivos estratégicos de la organización y las políticas criptográficas definidas.

Las acciones realizadas en esta etapa son la ejecución de las tareas técnicas relacionadas con la migración de los activos criptográficos, el seguimiento de dichas ejecuciones y la retroalimentación del resultado y, por último, la implementación de procesos de monitorización continua y mecanismos para favorecer la cripto-agilidad.

4.1. Ejecución técnica de la migración

Las acciones a realizar en la ejecución técnica de la migración comprenden desde la ejecución del plan de *backup* hasta la realización de pruebas y, en caso de error o fallos, puede ser necesaria la ejecución del plan de *rollback*.

Las tareas técnicas del plan de migración pueden ser de muy diversa índole, como por ejemplo la actualización de bibliotecas criptográficas, cambios de configuraciones, cambios en código fuente, sustitución de dispositivos *hardware*, aislamiento y segmentación de redes sobre los activos, etc.

A continuación, se establece un diagrama de flujo con los pasos requeridos para la ejecución técnica de la migración.

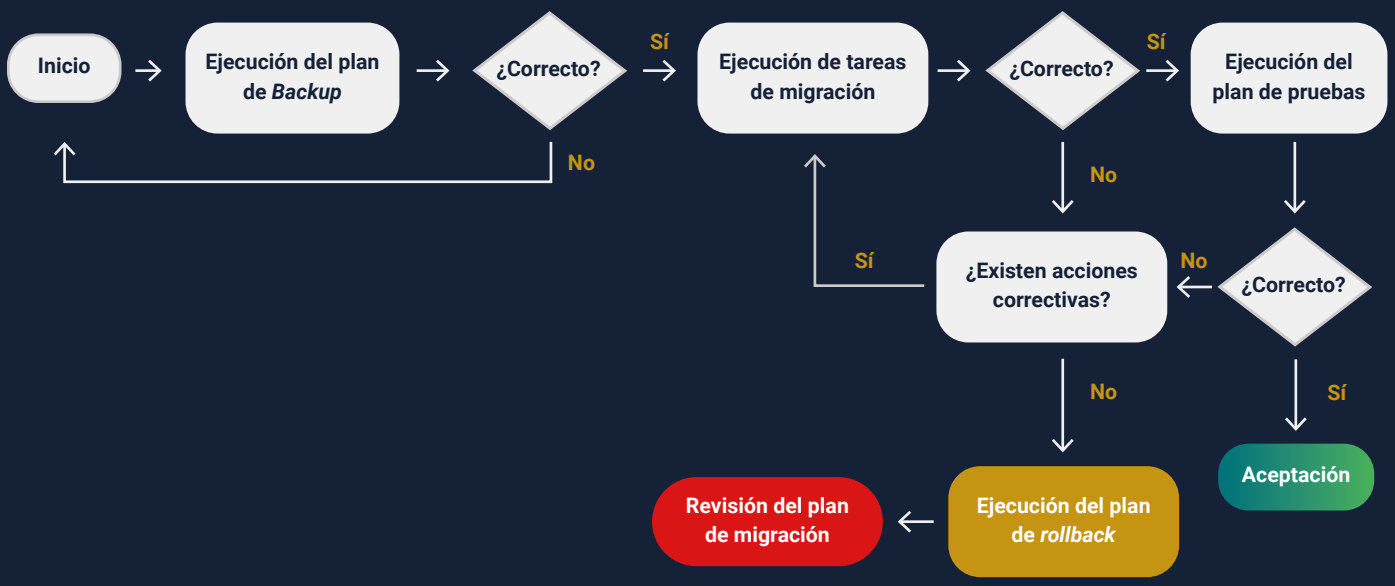


Ilustración 5. **Diagrama de flujo pasos migración.**

4. Etapa 3: Ejecución de la migración

En primer lugar, como ya se ha indicado, se inicia la **ejecución del plan de *backup***, con el objetivo de disponer de una instantánea del último estado correcto conocido del sistema o activo criptográfico. Si el plan de *backup* fallase, no se sigue adelante con el resto de tareas hasta que se pueda ejecutar correctamente.

Con el plan de *backup* realizado, iniciamos la **realización de las tareas de migración** descritas en el plan de actualización del activo criptográfico. En caso de fallo, el equipo debe evaluar el fallo y tomar una decisión. Si existiesen medidas correctivas para dicho fallo, se aplican y se sigue adelante con el resto de tareas hasta que todas se completen de forma satisfactoria. Si se desconociese la naturaleza del fallo o no existieran medidas correctivas o estas requirieran más tiempo del disponible en la ventana de actualización, entonces el equipo debe proceder con el **plan de *rollback*** para devolver el activo a su último estado correcto. Se debe revisar el plan de migración para tener en cuenta el fallo observado y volver a reintentarlo en una iteración posterior.

Si las tareas de migración se han realizado correctamente, entonces se debe ejecutar el **plan de pruebas** que contiene pruebas funcionales, operativas y de seguridad; con el fin de validar el resultado de la migración y aceptar el sistema o activo criptográfico para su puesta en producción.

Si alguna de las pruebas falla, el equipo debe valorar si es debido a algún fallo en el proceso o si existe alguna medida correctiva. Si existiesen medidas correctivas, se aplicarían y se volvería a ejecutar el plan de pruebas hasta que arroje un resultado satisfactorio. En caso de no existir medidas correctivas, el equipo debe aplicar el plan de *rollback* y proceder a la revisión del plan de migración para tener en cuenta la prueba fallida y cómo solucionar el problema. El plan de migración revisado se volvería a reintentar en una iteración posterior.

Si todas las pruebas son satisfactorias, entonces se acepta el sistema o activo criptográfico en producción.

4.2. Seguimiento del proceso de migración

Las tareas de seguimiento del proceso de migración constituyen un elemento esencial para garantizar que la transición hacia criptografía postcuántica se ejecuta conforme al plan de migración, respetando los tiempos y recursos asignados. Este seguimiento debe garantizar que los resultados del proceso de migración se enmarquen en el proceso global de control y gobernanza de la organización, retroalimentando otros procesos, con el objetivo de mantener una visión actualizada y completa de los activos criptográficos, alineada con los objetivos estratégicos y las políticas criptográficas.

La ejecución de las tareas y procedimientos técnicos del plan de migración puede tener dos posibles resultados:

- **Ejecución satisfactoria.** En ese caso, se debe realizar un informe en el que se expliquen detalladamente los pasos realizados y el resultado obtenido, así como las pruebas de validación y aceptación de la solución. Este informe debe retroalimentar otros procesos del plan de transición a criptografía postcuántica que hemos visto anteriormente, como el inventario de activos criptográficos y el análisis de riesgo cuántico.

  Tras completar la migración, se debe **actualizar el inventario de activos criptográficos** para reflejar las nuevas primitivas criptográficas postcuánticas o híbridas utilizadas, así como la tipología y características del material criptográfico empleado, sin incorporar en ningún caso valores de claves ni otro material criptográfico secreto o clasificado y, en su caso, las versiones actualizadas de las librerías criptográficas empleadas. Además, en la siguiente iteración del **análisis de riesgos, deberá reevaluarse el estado del activo criptográfico, los riesgos asociados** (incluido el riesgo cuántico), calcular el riesgo residual y decidir si este es aceptable o si requiere medidas adicionales.

- **Migración no satisfactoria.** En ese caso, el seguimiento del proyecto debe documentar los errores, fallos u obstáculos encontrados durante el proceso de migración. Se debe evaluar el porqué de dichos obstáculos y plantear soluciones que formarán parte de un **proceso de lecciones aprendidas, que retroalimenten el plan de migración y el plan de actualización**. Una vez adaptados los procesos, se replanifica para volver a reintentar la migración.

Finalmente, se debe mantener una comunicación con todos los actores relevantes del proceso para mantenerlos informados sobre el grado de avance del plan de migración.

4.3. Implantación de mecanismos de cripto-agilidad

Una vez concluido el proceso de migración a criptografía postcuántica, las organizaciones deben aspirar a incrementar su grado de madurez y control sobre sus activos criptográficos, añadiendo mecanismos de cripto-agilidad en sus procesos de mejora continua.

Para ello, no basta con adoptar tecnología concreta, sino que es necesario alinear **soluciones técnicas, procesos y políticas** que permitan un **uso eficiente y flexible de la criptografía**. Esto facilitará que los sistemas y activos criptográficos puedan actualizarse, modificarse o reemplazarse con un impacto reducido en la organización, por ejemplo, mediante cambios de configuración o tiempos de parada mínimos. Más allá de la transición postcuántica, la cripto-agilidad constituye una buena práctica para el mantenimiento general de la criptografía, al favorecer la identificación de vulnerabilidades y la resolución de incidentes de forma más eficiente.

La cripto-agilidad tiene, por tanto, especial relevancia porque la mayoría de algoritmos postcuánticos son relativamente nuevos y podrían requerir sustitución si se descubren nuevas vulnerabilidades o si futuras normas y estándares establecen requisitos distintos a los inicialmente adoptados por la organización.

A continuación, veremos algunas de las principales formas de la cripto-agilidad y qué procedimientos u obstáculos se pueden encontrar:

- **Agilidad de migración:** consiste en la capacidar de cambiar el uso de un algoritmo o primitiva criptográfica por otra. Es el caso de migración de criptografía tradicional a criptografía postcuántica. Durante este proceso de migración es importante asegurar que el uso de los nuevos algoritmos criptográficos es soportado por todos los componentes o depedencias del activo o sistema criptográfico, para evitar problemas de interoperabilidad.

  El uso de procedimientos de negociación de algoritmos o el soporte de múltiples algoritmos de forma simultánea y excluyente (construcciones no híbridas), pueden ayudar a mejorar la interoperabilidad e incrementar la agilidad de migración; sin embargo, también pueden introducir nuevos riesgos de ataques de degradación (*downgrade*), donde un atacante podría escoger de forma deliberada el uso de un algoritmo menos seguro.



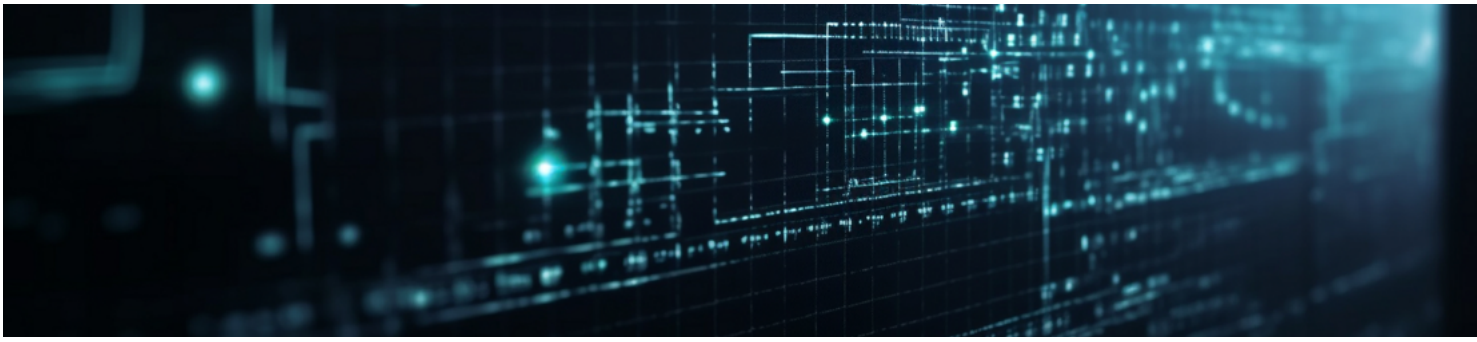
Asimismo, el uso de dispositivos *hardware* limitados o con problemas de compatibilidad puede ser un obstáculo para conseguir la agilidad de migración. El uso de nueva criptografía puede suponer retos a evaluar, como el uso de tamaños de clave mayores, necesidades incrementadas de procesamiento y almacenamiento o la incompatibilidad de mecanismos de aceleración *hardware*.

- **Agilidad de cumplimiento:** supone la adaptabilidad de la criptografía y sistemas para el cumplimiento regulatorio, normativo o de estándares. Requiere un seguimiento y control de los cambios introducidos en dichos estándares o normativas para poder adaptarse de forma ágil a su cumplimiento. Asimismo, para sistemas que den servicio en múltiples jurisdicciones, es posible que se requiera el uso de diferente criptografía o parametrizaciones en función de la región donde se presta el servicio.
- **Agilidad de implementación:** se refiere a la capacidad y simplicidad de cambios en las implementaciones de los algoritmos criptográficos en las aplicaciones desarrolladas. Puede ser el caso de abstracciones que separen la invocación del método criptográfico de su implementación, de esta forma se puede cambiar de forma ágil la implementación o incluso la biblioteca criptográfica que provea dicha implementación. Asimismo, se puede establecer un mecanismo de configuración para la elección de la implementación de la primitiva criptográfica, para poder aplicar cambios sin necesidad de modificar el código fuente. En este sentido, herramientas enmarcadas en el flujo CI/CD de SecDevOps pueden ayudar a detectar usos incorrectos o vulnerabilidades de la criptografía.

- **Agilidad de plataformas:** se refiere a la capacidad de integración de las implementaciones criptográficas en diferentes plataformas. Es de especial relevancia en las organizaciones que proveen implementaciones criptográficas a clientes. Estas deberían ser capaces de ejecutarse en diferentes dispositivos con independencia del *hardware* o *software* que utilicen. Por ejemplo, un proveedor de implementaciones criptográficas debería proveer alternativas o soluciones para el uso de la criptografía en plataformas de 32 y 64 bits, ARM o AMD, sistemas Unix o Windows, etc.
- **Otras formas de agilidad:**
  - **Agilidad de fortaleza criptográfica o de contexto:** se basa en cambiar de forma dinámica las parametrizaciones de seguridad de los algoritmos o primitivas criptográficas. Puede ser de utilidad en contextos donde estándares o normativas te indican los parámetros de seguridad a utilizar en función del contexto, grado de confidencialidad de la información, etc.
  - **Agilidad de retirada:** capacidad de retirar de producción de forma ordenada algoritmos o criptografía obsoleta o vulnerable.
  - **Agilidad de composición:** capacidad de establecer esquemas o construcciones híbridas que combinen múltiples algoritmos criptográficos de forma dinámica.

Para poder llegar a implementar las formas de cripto-agilidad mencionadas, se deben implementar una serie de **mecanismos** en tres dimensiones: tecnologías y procedimientos técnicos, procesos de negocio y políticas criptográficas:

- **Tecnologías y procedimientos técnicos.** A nivel técnico, se pueden implementar varias medidas para mejorar la cripto-agilidad de la organización. El primer paso es conocer qué criptografía se utiliza en la organización y dónde. El uso de herramientas de gestión de inventarios criptográficas ayudan a poder monitorizar y detectar vulnerabilidades en los activos criptográficos para proceder a su actualización. Asimismo, un inventario completo de activos criptográficos incluirá un mapa de dependencias que será de utilidad a la hora de detectar y prevenir posibles problemas de interoperabilidad entre componentes.



Otras herramientas que son de gran utilidad para la mejora de la cripto-agilidad de la organización son las herramientas de gestión y automatizacion de procesos relacionados con claves criptográficas y certificados digitales. Estas soluciones pueden ser de tipo **KMS**, **PKI** o **HSM** y permiten automatizar la creación, rotación, uso, distribución y revocación de las claves criptográficas y certificados digitales.

Durante el desarrollo de **aplicaciones propias** se pueden aplicar múltiples herramientas o estrategias que favorezcan la cripto-agilidad de la organización. Por ejemplo, mediante el uso de capas de abstracción que separan la invocación de un algoritmo o primitiva criptográfica de su implementación, gestión de la configuración o el uso de escáneres de vulnerabilidades de código que permiten detectar vulnerabilidades criptográficas o usos incorrectos de la misma. Muchos de estos controles se pueden automatizar en procesos CI/CD para un control continuo del código fuente.

- **Procesos de negocio.** Es indispensable que se incluya la cripto-agilidad en este punto. Una correcta definición y documentación de procesos favorece la alineación de todos los actores relevantes involucrados y el cumplimiento de los objetivos estratégicos de la organización, traduciéndose en una mayor eficiencia operativa.

  Algunos de los procesos de negocio donde se pueden incluir formas de cripto-agilidad son los siguientes:

  - **Procesos de adquisición de activos (*software* y *hardware*).** Se pueden incluir requisitos o cláusulas con proveedores de servicios en las que se garantice la actualización de los componentes criptográficos. Asimismo, se pueden requerir evidencias de pruebas específicas sobre la criptografía utilizada y los mecanismos de cripto-agilidad incorporados. Para los componentes *hardware*, se debe garantizar que puedan soportar diferentes algoritmos criptográficos o que puedan ser actualizables de forma sencilla en el futuro, por ejemplo mediante actualizaciones remotas u OTA (*Over the Air*).
  - **Procesos de gestión de cambios.** Controlan cómo se aplican cambios en los sistemas y activos de la organización de forma controlada y eficiente. Incorporar la cripto-agilidad en esta gestión involucra la descripción del cambio criptográfico, quién es el responsable de dicho cambio y cómo se ha de llevar a cabo. Dicho proceso debe ser debidamente autorizado y una vez ejecutado, deben establecerse mecanismos para retroalimentar la actualización del inventario criptográfico y el análisis de riesgo con el nuevo estado del activo.

- **Proceso de desarrollo y publicacion de *software*.** Supone proporcionar los recursos necesarios para incluir fases de pruebas rigurosas que validen que no se produzcan problemas de interoperabilidad u otras vulnerabilidades.
- **Proceso de gestión de incidentes.** Deben existir procesos que permitan la monitorización del uso de criptografía en la organización y procedimientos claros de actuación definidos en caso de que se produzca un incidente de seguridad.

- **Políticas criptográficas.** Para asegurar una aplicación homogénea y eficiente de mecanismos de cripto-agilidad a lo largo de la organización, estos requisitos deberían estar contenidos en las políticas criptográficas. Estas pueden contener la obligación de creación y mantenimiento del inventario de activos criptográficos, asignación de perfiles responsables de monitorización y mantenimiento criptográfico, obligatoriedad de realización de planes de pruebas criptográficas, requisitos en los procedimientos de adquisición, etc.

  Por otro lado, deben ser lo suficientemente flexibles para no suponer un obstáculo a la cripto-agilidad. Por ejemplo, si la política criptográfica especifica determinados algoritmos y parametrizaciones y se descrubre una vulnerabilidad o hay un cambio normativo que suponga la necesidad de cambio de dichos algoritmos, se debería actualizar la política criptográfica antes de proceder a los cambios en los sistemas y activos criptográficos.

Para las organizaciones, el análisis de qué mecanismos o qué nivel de cripto-agilidad necesitan puede suponer un reto. Este análisis debe basarse en el tipo de organización y la naturaleza de los activos criptográficos, de la tolerancia al riesgo de la organización y de qué forma de cripto-agilidad es requerida.

Por ejemplo, para una organización que requiere agilidad de cumplimiento normativo y de estándares en las publicaciones de un producto *software* o *hardware* que produce, los cambios no tienen que aplicarse en cuestión de minutos, sino que pueden demorar semanas o meses en función del ciclo de actualizaciones del producto y la complejidad de implementación de los cambios. En cambio, una organización que requiere agilidad de migración para la protección de activos críticos de información puede requerir tiempos mucho más rápidos en el caso de que se descubra una vulnerabilidad.

Asimismo, en función del análisis de riesgo de los activos, las organizaciones podrían decidir aplicar mecanismos de cripto-agilidad para los nuevos desarrollos o adquisiciones de productos *software* y *hardware*; mientras que se mantendría un enfoque más conservador en los productos más antiguos o legacy. Esto se debe a que **la incorporación de estos mecanismos de cripto-agilidad se realiza desde la fase de diseño,** enmarcado en el paradigma de *Security-by-design*, en lugar de aplicarlos con posterioridad.



4.4. Seguimiento, indicadores, auditoría y mejora continua

El seguimiento deberá operar en tres niveles: entidad, sector y ámbito nacional. Cada **entidad** mantendrá indicadores sobre inventario, clasificación de riesgos, pilotos, migraciones, excepciones, adquisiciones, cobertura de mecanismos postcuánticos y riesgos residuales. Las autoridades **sectoriales** agregarán la información conforme a sus competencias. En el **ámbito nacional**, el **CCN** elaborará formatos y criterios técnicos comunes para facilitar la consolidación, comparación y seguimiento de la transición. El Centro Criptológico Nacional consolidará únicamente la información técnica agregada que le sea facilitada por las autoridades competentes o por los mecanismos previstos para el ámbito **ENS**.

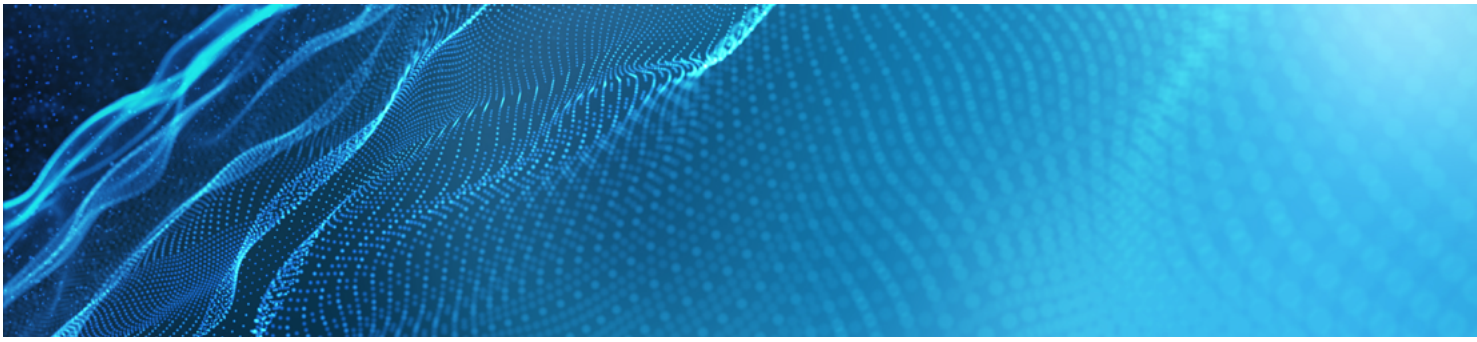
El cuadro de mando nacional será aprobado por el órgano que apruebe esta Hoja de Ruta o, en su caso, por el que determine la normativa aplicable. Incluirá, al menos, porcentaje de activos inventariados, porcentaje de casos de uso clasificados, cobertura de información de larga vida útil, número y resultado de pilotos, avance de migraciones de alto y medio riesgo, porcentaje de adquisiciones cripto-ágiles, disponibilidad de productos evaluados, excepciones abiertas y cerradas, formación impartida y principales dependencias o bloqueos.

La Hoja de Ruta será revisada al menos anualmente y, de forma extraordinaria, cuando se produzcan avances relevantes en computación cuántica, cambios en los estándares, vulnerabilidades graves o decisiones de la Unión Europea que exijan acelerar la transición y, en todo caso, cuando se apruebe normativa que regule la transición o su gobernanza, para adaptarla a ella. Las modificaciones que afecten al alcance, a los hitos, a los criterios de clasificación del riesgo o a la gobernanza seguirán el mismo cauce que su aprobación. El Centro Criptológico Nacional podrá actualizar las tablas técnicas, las referencias y los anexos, dando cuenta de ello al órgano que haya aprobado la Hoja de Ruta.

5. Despliegue nacional, coordinación y calendario

La coordinación nacional de la transición se ejercerá conforme al marco competencial vigente, sin perjuicio de que la normativa que, en su caso, se apruebe establezca su estructura de gobernanza, los órganos responsables y sus funciones.

La hoja de ruta del Grupo de Cooperación NIS establece, para los Estados miembros, la implementación de los primeros pasos antes del **31 de diciembre de 2026,** entre los que figuran: el establecimiento de la hoja de ruta nacional y el inicio de la planificación y de los proyectos piloto correspondientes a los casos de uso de riesgo alto y medio.



5. Despliegue nacional, coordinación y calendario

Hasta el **31 de diciembre de 2030** se priorizará la migración de los servicios o casos de uso de alto riesgo. En la evaluación del riesgo se considerarán con carácter prioritario los sistemas esenciales, la información de larga vida útil, las infraestructuras de clave pública, los sistemas de identidad y firma electrónica, las comunicaciones sensibles y los mecanismos de actualización de *software* y *firmware*. Hasta el **31 de diciembre de 2035** se abordará la migración de los sistemas de riesgo medio y, en la medida técnica y económicamente viable, de los sistemas de riesgo bajo.

Los plazos tienen el carácter transitorio indicado en el resumen ejecutivo, son horizontes máximos de planificación y podrán anticiparse. La evolución tecnológica no deberá utilizarse como motivo para retrasar el inventario, la evaluación del riesgo, la cripto-agilidad, la contratación preparada para la transición ni los pilotos técnicamente maduros.

En la contratación pública relativa a sistemas que incorporen funciones criptográficas, se recomienda que los pliegos incorporen, según proceda, prescripciones técnicas, criterios de adjudicación, o condiciones especiales de ejecución relativas a cripto-agilidad, capacidad de actualización, soporte de mecanismos postcuánticos o híbridos, inventario criptográfico del producto, hoja de ruta del proveedor, interoperabilidad, soporte, fin de vida, notificación de vulnerabilidades y evidencias de evaluación o certificación.

La capacidad nacional de evaluación se apoyará en el Organismo de Certificación del **CCN**, el **CPSTIC** y una red de laboratorios técnicamente coordinada por el **CCN**. Esta coordinación se entenderá, sin perjuicio de las competencias que correspondan a otros organismos en materia de acreditación, certificación europea, evaluación de la conformidad y vigilancia de mercado.

6. Acrónimos

ACRÓNIMO	SIGNIFICADO
AES	Advanced Encryption Standard
CBOM	Cryptographic Bill Of Materials
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad TIC del Centro Criptológico Nacional
CRQC	Cryptographically Relevant Quantum Computer (Ordenador cuántico criptográficamente relevante)
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
ETSI	European Telecommunications Standards Institute
HNDL	Harvest now and decrypt later (Almacena ahora y descifra luego)
HSM	Hardware Security Module (Módulo de seguridad Hardware)
IETF	Internet Engineering Task Force
KMS	Key Management System (Sistema de gestión de claves)
ML-DSA	Module-Lattice-based Digital Signature Algorithm
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism
NIST	National Institute of Standards and Technology

6. Acrónimos

ACRÓNIMO	SIGNIFICADO
NCCoE	National Cybersecurity Center of Excellence
PKI	Public Key Infrastructure (Infraestructura de clave pública)
PQC	Post-Quantum Cryptography (Criptografía postcuántica)
RSA	Rivest-Shamir-Adleman
SLH-DSA	Stateless Hash-based Digital Signature Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
TPM	Trusted Platform Module



7. Bibliografía

[REF 001] **Mosca Michele (2015).** *Cybersecurity in an era with quantum computers: will we be ready?* https://eprint.iacr.org/2015/1075.pdf

[REF 002] **NIST Internal Report (2024).** *Transition to Post-Quantum Cryptography Standards* https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[REF 003] **The White House (2022).** *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[REF 004] **IETF PQUIP WG (2025).** *Post-Quantum Cryptography for Engineers* https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14

[REF 005] **IETF UTA WG (2025).** *Post-Quantum Cryptography Recommendations for TLS-based Applications* https://datatracker.ietf.org/doc/html/draft-ietf-uta-pqc-app-00

[REF 006] **ETSI CYBER (2020). ETSI TR 103 619 V1.1.1.** *Migration strategies and recommendations to Quantum Safe schemes* https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[REF 007] **ETSI CYBER (2024). ETSI TR 104 016 V1.1.** *A Repeatable Framework for Quantum-Safe Migrations* https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf

[REF 008] **EU NIS CG PQC Workstream (2025).** *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography* https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

7. Referencias

[REF 009] **National Cyber Security Centre (2025).** *Timelines for migration to post-quantum cryptography.* https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[REF 010] **Australian Signals Directorate (2025).** *Planning for post-quantum cryptography* https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography

[REF 011] **Canadian Centre for Cyber Security (2025).** *Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)* https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[REF 012] **TNO, CWI, y AIVD (2024).** *The PQC Migration Handbook. 2ª ed.* https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

[REF 013] **NIST National Cybersecurity Center of Excellence (2023).** *NIST SP 1800-38 (Initial Preliminary Draft). Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography* https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)

[REF 014] **CycloneDX – The OWASP Foundation (2025).** *Authoritative Guide to CBOM. 2ª ed.* https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf

[REF 015] **IETF Network Working Group (2001).** *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* https://www.ietf.org/rfc/rfc3161.txt

[REF 016] **IETF PKIX WG (2010).** *ESSCertIDv2 Update for RFC 3161* https://datatracker.ietf.org/doc/html/rfc5816

[REF 017] **ETSI ESI (2023).** *ETSI EN 319 421 V1.2.1. Policy and Security Requirements for Trust Service Providers issuing Time-Stamps* https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf

[REF 018] **ETSI ESI (2016).** *Time-stamping protocol and time-stamp token profiles* https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

[REF 019] **Comisión Europea (2024).** *Recomendación (UE) 2024/1101, de 11 de abril de 2024, sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica.* https://ec.europa.eu/newsroom/dae/redirection/document/104248

7. Referencias

[REF 020] **NIS Cooperation Group (2025).** *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.* https://ec.europa.eu/newsroom/dae/redirection/document/117507

[REF 021] **Países Bajos: AIVD, CWI y TNO (2024).** *The PQC Migration Handbook, 2.ª edición; y NCSC-NL, documentación de preparación de programas de migración cuántica.* https://english.aivd.nl/site/binaries/site-content/collections/documents/2024/12/3/the-pqc-migration-handbook/The+PQC+Migration+Handbook+.pdf

[REF 022] **Francia: ANSSI (2026).** *Feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026-2027; recomendaciones y posicionamientos técnicos sobre transición postcuántica y criptoagilidad.* https://www.sgdsn.gouv.fr/files/files/Publications/Feuille%20de%20route%20S%C3%A9curit%C3%A9%20num%C3%A9rique%20de%20l%27Etat%202026-2027.pdf

[REF 023] **Finlandia: National Cyber Security Centre Finland (2025).** *Criterios del grupo criptográfico nacional para evaluaciones de productos PQC aplicables desde el 1 de enero de 2026.* https://www.kyberturvallisuuskeskus.fi/fi/uutiset/suomen-kansallisen-kryptotyoryhman-linjaukset-kansallisiin-pqc-salaustuotearviointeihin-112026-alkaen

[REF 024] **P.W. Shor.** *Polynomial-time algorithms for prime factorization and discrete algorithms on a quantum computer. SIAM Journal on Computing, 26, 5, 1484-1509, 1997.* https://doi.org/10.1137/S0097539795293172.

[REF 025] **L.K. Grover.** *Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett., 79, 2, 325–328, 1997.* https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.79.325

[REF 026] **CCN-STIC 221 Guía de Mecanismos Criptográficos autorizados por el CCN** https://www.ccn-cert.cni.es/es/guias-de-acceso-publico-ccn-stic/6954-ccn-stic-221-guia-de-mecanismos-criptograficos-autorizados-por-el-ccn-1/file.html

[REF 027] **CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad** https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

7. Referencias

[REF 028] **CCN-TEC 009 BP37 Recomendaciones para una transición postcuántica segura (Julio 2026).** https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file

[REF 029] **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.** https://www.boe.es/eli/es/rd/2022/05/03/311/con

ANEXO I.
Tabla de vulnerabilidad cuántica



ANEXO I. Tabla de vulnerabilidad cuántica

Algoritmo	Longitud de clave	Longitud hash	Puntuación vulnerabilidad cuántica	Vulnerable a ataques tradicionales
ALGORITMOS ASIMÉTRICOS				
RSA	Indiferente	N/A	2	No
ElGamal	Indiferente	N/A	2	No
Paillier	Indiferente	N/A	2	No
ECDH	Indiferente	N/A	2	No
ECDSA	Indiferente	N/A	2	No
EdDSA	Indiferente	N/A	2	No
ECIES	Indiferente	N/A	2	No
ML-KEM	Indiferente	N/A	0	No
ML-DSA	Indiferente	N/A	0	No
SLH-DSA	Indiferente	N/A	0	No
XMSS	Indiferente	N/A	0	No
LMS	Indiferente	N/A	0	No
HSS	Indiferente	N/A	0	No
FrodoKEM	Indiferente	N/A	0	No
Falcon (FN-DSA)	Indiferente	N/A	0	No
Classic McEliece	Indiferente	N/A	0	No
BIKE	Indiferente	N/A	0	No
HQC	Indiferente	N/A	0	No
SIKE	Indiferente	N/A	2	Sí
Rainbow	Indiferente	N/A	2	Sí
SIDH	Indiferente	N/A	2	Sí

ANEXO I. Tabla de vulnerabilidad cuántica

Algoritmo	Longitud de clave	Longitud hash	Puntuación vulnerabilidad cuántica	Vulnerable a ataques tradicionales
ALGORITMOS SIMÉTRICOS				
AES	128	N/A	1	No
AES	256	N/A	0	No
DES	56	N/A	2	Sí
3DES	168	N/A	2	No
Camellia	128	N/A	1	No
Camellia	192	N/A	0	No
Camellia	256	N/A	0	No
Blowfish	Variable	N/A	1	No
Twofish	128	N/A	1	No
Twofish	192	N/A	0	No
Twofish	256	N/A	0	No
IDEA	128	N/A	1	No
RC5	Variable	N/A	1	No
ChaCha20	256	N/A	0	No
RC4	Variable	N/A	2	Sí
Trivium	80	N/A	2	Sí
Salsa20	128	N/A	1	No
Salsa20	256	N/A	0	No
Ascon	128	N/A	1	No
A5/1	64	N/A	2	Sí
A5/2	64	N/A	2	Sí

ANEXO I. Tabla de vulnerabilidad cuántica

Algoritmo	Longitud de clave	Longitud hash	Puntuación vulnerabilidad cuántica	Vulnerable a ataques tradicionales
FUNCIONES HASH				
MD5	N/A	128	2	Sí
SHA-1	N/A	160	2	Sí
SHA-2	N/A	224	1	No
SHA-2	N/A	256-512	0	No
SHA-3	N/A	224	1	No
SHA-3	N/A	256-512	0	No
Whirlpool	N/A	512	0	No
BLAKE2	N/A	224	1	No
BLAKE2	N/A	256-512	0	No
BLAKE3	N/A	224	1	No
BLAKE3	N/A	256-512	0	No
PBKDF2	N/A	N/A	0	No
HKDF	N/A	N/A	0	No
Argon2id	N/A	N/A	0	No
Scrypt	N/A	Variable	0	No
bcrypt	N/A	192	0	No

Tabla 8. Vulnerabilidad cuántica algoritmos



Hoja de ruta de la transición a criptografía postcuántica en España

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

Catálogo de productos y servicios de seguridad TIC: **PDF** | **ONLINE**

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC