CCN-TEC 009

BP/37

Recomendaciones para una transición postcuántica segura

GUÍA DE BUENAS PRÁCTICAS

JULIO 2026

CCN centro criptológico nacional

CCN-PYTEC centro criptológico nacional

Edita:

CCN-CERT
centro criptológico nacional

Fecha de Edición: julio de 2026

El Grupo de investigación en Criptología y Seguridad de la Información (CiGSI) del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI) del Consejo Superior de Investigaciones Científicas (CSIC), ha participado en el desarrollo del presente documento y sus anexos.

Índice

1. Introducción

A lo largo de los últimos años, estamos asistiendo a un importante auge en el desarrollo de la computación cuántica. Este desarrollo está despertando un amplio interés debido a las enormes ventajas que supondrá la aparición de un ordenador cuántico con gran capacidad de cálculo para abordar problemas que hoy en día son de difícil solución, como los relacionados con la logística, la aeronáutica, la biotecnología, la farmacología, etc.

Otro de los aspectos en los que la computación cuántica tendrá una enorme repercusión en nuestras vidas, son los relacionados con la seguridad, protección y custodia de la información. En este caso se trata de que tal poder de cálculo podrá resolver la mayor parte de los problemas matemáticos en los que se basa la seguridad de la criptografía actual, dejándola indefensa, esto es, permitiendo que el acceso no autorizado a la información pase a ser una realidad. En otras palabras, la criptografía tal y como la conocemos hoy en día, **dejará de cumplir con sus objetivos de confidencialidad, integridad, autenticación y no repudio**.

La estimación de la aparición del ordenador cuántico criptográficamente relevante ha ido variando con el tiempo. Inicialmente se esperaba su aparición para 2050, pero con los desarrollos en computación cuántica, se prevé que esté disponible para mediados de la próxima década (2035).

1. Introducción

La computación cuántica supone una amenaza para la ciberseguridad de las comunicaciones y las transacciones y los sistemas que las protegen. Para evitar que sean vulneradas, es necesario comenzar a prepararse.

Necesidad de prepararse

Esta aparición supone una amenaza para la ciberseguridad de las comunicaciones y las transacciones y los sistemas que las protegen. Para evitar que se vean vulneradas, es necesario comenzar a prepararse.

La protección de la información es una tarea compleja que compete a todos los Estados y a todos los estamentos de la sociedad (Administración pública, empresas, instituciones, usuarios, etc.). Es necesario comenzar a tomar medidas ya, para que, independientemente de cuándo se materialice la amenaza de la computación cuántica, la sociedad en su conjunto esté preparada para asegurar la protección de la información.

Base técnica de la amenaza

Es bien sabido que la seguridad de los criptosistemas asimétricos (o de clave pública) más utilizados en la actualidad, dependen de dos problemas matemáticos computacionalmente difíciles de resolver con los ordenadores actuales:

- **El problema de la factorización de números enteros** (**PFE**, véase el **Anexo A.1**), que consiste en determinar los factores primos que dividen a un número entero compuesto dado.
- **El problema del logaritmo discreto** (**PLD**, véase el **Anexo A.2**), que requiere determinar la potencia (en el caso de un grupo multiplicativo) a la que se debe elevar el generador dado del grupo considerado, o el múltiplo (en el caso de un grupo aditivo) del generador en el correspondiente grupo, para obtener un elemento de dicho grupo, dado de antemano.

El primero de estos dos problemas es la base de la seguridad del **criptosistema RSA** **[12]**, **[36]**; mientras que el segundo lo es, en su versión multiplicativa, del criptosistema de ElGamal **[8]**, **[12]**, y en su versión aditiva, de los criptosistemas basados en curvas elípticas o CCE **[12]**, **[19]**, **[22]**.

Como ya se ha mencionado, tanto el **PFE** como el **PLD** se han considerado tradicionalmente dos problemas computacionalmente seguros, debido a que la capacidad computacional de los ordenadores actuales requiere de un tiempo de ejecución subexponencial para poder vulnerar (romper) cualquiera de ellos.

Sin embargo, el matemático estadounidense ***Peter Shor,*** en 1997 (sus primeros resultados datan de 1994), publicó dos algoritmos cuánticos capaces de vulnerar ambos problemas de forma eficiente, esto es, en un tiempo de ejecución

1. Introducción

polinómico, si se dispusiera de un ordenador cuántico con la suficiente capacidad de cómputo **[37]**. Tales algoritmos, con los conocimientos actuales, no pueden ser implementados en ordenadores convencionales y requieren para su ejecución de ordenadores cuánticos.

Así pues, se puede afirmar que los algoritmos de *Shor* han demostrado que la **criptografía asimétrica** de hoy en día es vulnerable a la computación cuántica, por lo que se hace imprescindible la búsqueda y el establecimiento de nuevos sistemas asimétricos que sean invulnerables a este tipo de computación. De hecho, si un ordenador convencional necesita $O(2^{\sqrt[3]{\log n}})$ operaciones bit para romper uno de estos dos problemas, un ordenador cuántico, usando el algoritmo de *Shor* correspondiente, reduciría ese número de operaciones *bit* a $O(\log^3 n)$ con un almacenamiento de memoria de $O(\log n)$ *bits*.

Debe recordarse que los mismos problemas que sustentan la seguridad de los sistemas de cifrado asimétrico son los que se emplean para garantizar la fiabilidad de los procesos de elaboración y verificación de las **firmas electrónicas**. Así pues, en términos generales, la seguridad de aquellos es la misma que la de estos.

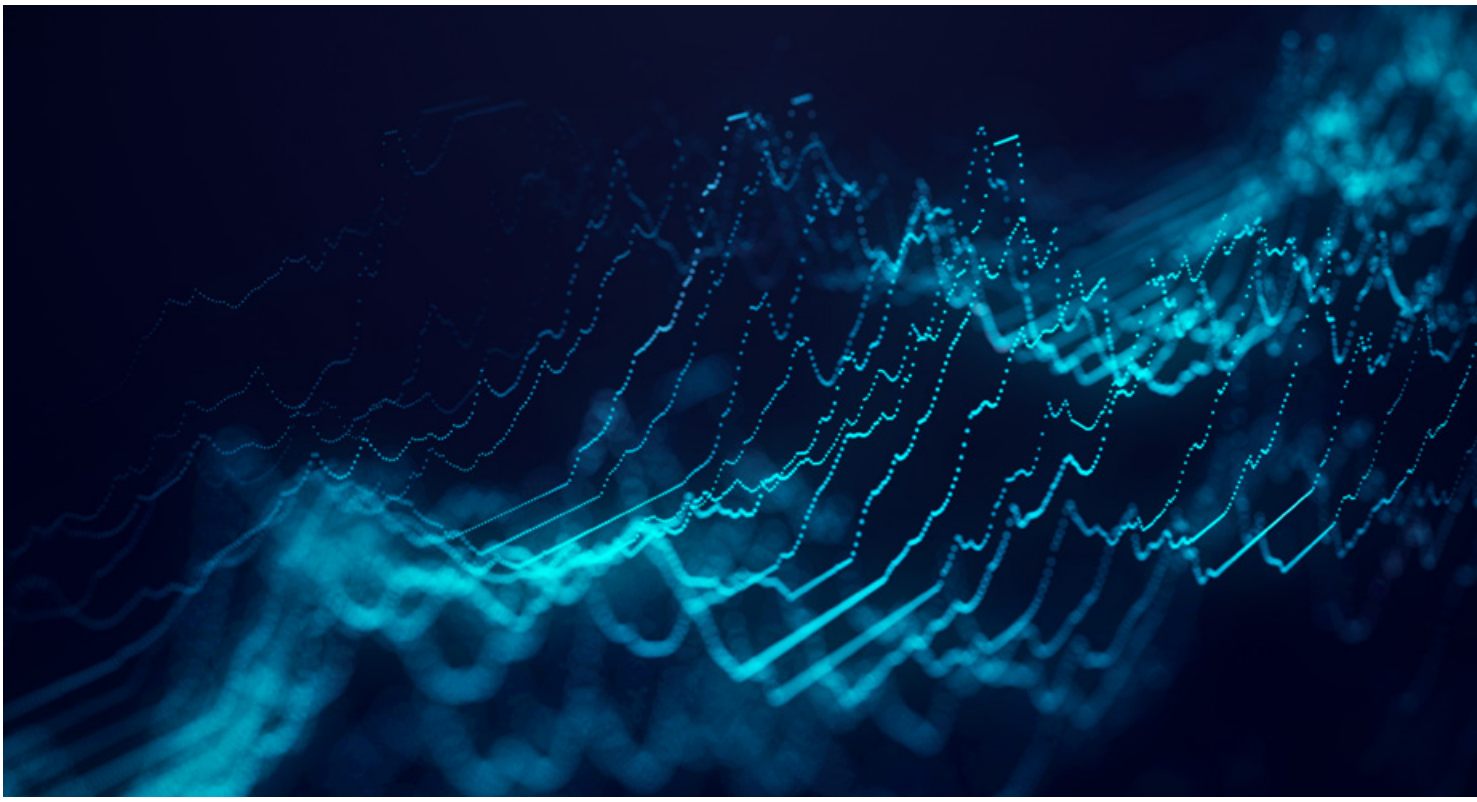
No obstante, en el caso de las firmas, sobre todo cuando se emplean para procesos de autenticación, solo necesitan garantizar su seguridad hasta que son verificadas, lo que suele requerir un periodo de tiempo mucho más corto que el que precisa mantener la confidencialidad de la información. Caso aparte sería si la validez de la firma fuera de varios años (como es el caso de *firmware* o de la firma de contratos).

1. Introducción

"Los mismos problemas que sustentan la seguridad de los sistemas de cifrado asimétrico (vulnerable a la computación cuántica) son los que se emplean para garantizar la fiabilidad de los procesos de elaboración y verificación de las firmas electrónicas"

Por su parte, los **criptosistemas simétricos** (o de clave secreta), hasta la fecha, no parece que sean tan vulnerables a la computación cuántica. El mejor algoritmo cuántico que ataca esta criptografía es el algoritmo de búsqueda exhaustiva de *Grover* **[13]**, **[14]**, que reduciría el tiempo de cálculo necesario para romperla a la raíz cuadrada del tiempo actual. Esto es, si se desarrollara un ordenador cuántico con la capacidad de cómputo suficiente, la seguridad de los sistemas simétricos actuales sería equivalente a la de los mismos sistemas, pero con claves cuya longitud fuera la mitad. Es decir, si un ordenador actual necesita de $O(n)$ operaciones bits para romper uno de estos sistemas simétricos, con el algoritmo de *Grover* este tiempo se reduciría a $O(\sqrt{n})$ operaciones *bits* y requeriría un almacenamiento en memoria de $O(\log n)$ *bits*.

Hasta ahora no se conoce que exista un ordenador cuántico con la suficiente capacidad de cómputo como para vulnerar los protocolos criptográficos que se emplean en la actualidad.



Migración a criptografía resistente y calendario de transición

Así pues, y debido a los avances ya mencionados y alineados con la hoja de ruta y el calendario elaborados por los Estados miembros de la Unión Europea *"A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography"* **[32]**, el **Centro Criptológico Nacional** (**CCN**) ha actualizado este documento con la finalidad de concienciar sobre la necesidad de migrar la criptografía de nuestros sistemas, hacia sistemas con criptografía resistente a la computación cuántica (denominados *quantum resistant* – **QR**, o *quantum safe* - **QS**).

La migración deberá completarse antes de finales de 2030 o 2035, en función del riesgo[1] de los sistemas:

- Antes del 31.12.2030, los sistemas con riesgo alto deberán estar completamente migrados.
- Antes del 31.12.2035 todos los sistemas con riesgo medio deberán estar migrados y con riesgo bajo en la medida de lo posible.

Los grandes riesgos a los que nos enfrentamos durante la transición criptográfica son los siguientes:

- **Almacena ahora y descifra luego** *(Store/Harvest now and decrypt later):* La información que necesitamos salvaguardar, puede verse expuesta cuando se disponga de un ordenador cuántico criptográficamente relevante, 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.

1. **La determinación del riesgo se define en la Hoja de ruta para la transición postcuántica en España [42]**

2. Criptografía postcuántica

Debido al desarrollo en la computación cuántica y a su aplicación para vulnerar los sistemas criptográficos precuánticos (usados en la actualidad); desde hace unos años, la comunidad criptográfica ha comenzado a investigar con el fin de proponer nuevos sistemas que sean resistentes a tal computación. Esta nueva criptografía, basada en problemas matemáticos diferentes a los empleados en la actualidad (entre los que se encuentran el **PFE** y el **PLD**), se ha dado en llamar «**criptografía postcuántica**» (**PQC** o *Post-Quantum Cryptography*) o **resistente a la computación cuántica** (**QR**).

El **NIST** (*National Institute of Standards and Technology*), como entidad responsable de los procesos de estandarización en EEUU y debido a la amenaza de la computación cuántica, en noviembre de 2016 hizo una Convocatoria Internacional para seleccionar nuevos algoritmos criptográficos resistentes a esta computación con el fin de ser considerados nuevos estándares **[27]**. La entidad solo incluyó en esta convocatoria a los cifrados asimétricos, los mecanismos de encapsulación de claves o **KEM** (*Key Encapsulation Mechanism*) y las firmas digitales.

La seguridad de los algoritmos presentados a la convocatoria del **NIST** se ha basado en problemas matemáticos que tienen cabida en las siguientes cinco áreas:

- Códigos correctores de errores (criptografía basada en códigos).
- Retículos (criptografía basada en retículos).
- Funciones resumen (criptografía basada en resúmenes o *hashes*).
- Polinomios multivariantes cuadráticos (criptografía multivariante cuadrática).
- Isogenias definidas sobre curvas elípticas (criptografía basada en isogenias).

Después de la publicación de los candidatos que han ido superando las diferentes rondas, en 2024, el **NIST** publicó una primera lista de algoritmos considerados estándares, a la que se ha añadido uno nuevo en 2025 **[43]**.

Los estándares ya publicados, así como los que están pendientes de publicar se listan en las **Tabla 1** y **Tabla 2**. En ambas tablas se indican las áreas a las que pertenecen los candidatos y, entre paréntesis, los correspondientes problemas matemáticos asociados: **MLWE** (*Module Learning With Errors*, véase el **Anexo A.3**), **SIS** (*Short Integer Solution*, véase el **Anexo A.4**), y **HQC** (*Hamming Quasi-Cyclic*, véase el **Anexo A.5**).

KEM ESTÁNDAR	PROPUESTA DE KEM	ÁREA Y PROBLEMA MATEMÁTICO	ESTÁNDAR
ML-KEM	CRYSTALS-Kyber	Retículo estructurado (MLWE)	FIPS 203
HQC-KEM	HQC	Código corrector de errores (HQC)	FIPS 207 (previsto 2027)

Tabla 1. Estándares (y propuestas originales de las que proceden) de KEM publicadas (o pendiente de serlo) por el NIST, junto con las primitivas matemáticas asociadas.

ESTÁNDAR DE FIRMA	PROPUESTA DE FIRMA DIGITAL	ÁREA Y PROBLEMA MATEMÁTICO	ESTÁNDAR
ML-DSA	CRYSTALS-Dilithium	Retículo estructurado (MLWE)	FIPS 204
SLH-DSA	SPHINCS$^+$	Funciones *hash*	FIPS 205
FN-DSA	FALCON	Retículo estructurado (SIS)	FIPS 206 (previsto 2026)

Tabla 2. Estándares (y propuestas originales de las que proceden) de firmas digitales publicadas por el NIST, junto con las primitivas matemáticas asociadas.

Los estándares ya publicados se conocen como **ML-KEM** (*Module-Lattice-Based Key-Encapsulation Mechanism*) **[26]**, **ML-DSA** (*Module-Lattice-Based Digital Signature*) **[29]** y **SLH-DSA** (*Stateless Hash-Based Digital Signature*) **[30]**, mientras que los que han sido aprobados como tales, pero están pendientes de publicación, son **FALCON** (*FAst-Fourier Lattice-based COmpact signatures over* **NTRU**, denominado **FN-DSA**) **[35]** y **HQC** (*Hamming Quasi-Cyclic*, denominado **HQC-KEM**)**[1]**.

Como se puede apreciar en las **Tabla 1** y **Tabla 2**, a excepción del mecanismo de encapsulación **HQC** y de la firma digital **SLH-DSA**, las restantes propuestas que han sido declaradas estándares fundamentan su seguridad en el área de retículos.

Por otra parte, el **CCN** considera que, además de los algoritmos propuestos por el **NIST** para el acuerdo de claves, el **FrodoKEM** **[24]** es otro algoritmo que se debe tener en cuenta. En la **Sección 4.2** se darán más detalles sobre esta recomendación.

Finalmente, es importante señalar que el **NIST** ha dado a conocer una nueva convocatoria para algoritmos de firma digital resistentes a la computación cuántica. El hecho parece justificarse para que la aplicación más extendida de la criptografía asimétrica pueda utilizar otras áreas que no se limiten a los retículos estructurados y a las funciones *hash*.

"El CCN considera que, además de los algoritmos propuestos por el NIST para el acuerdo de claves, el FrodoKEM es otro algoritmo que se debe tener en cuenta"

De hecho, esta convocatoria adicional para nuevas firmas digitales se encuentra en el momento de publicar este informe en la Ronda 3 [44] y en la misma han vuelto a presentarse propuestas basadas en las mismas áreas de problemas matemáticos mencionados previamente, a las que se ha añadido un área nueva, conocida como **MPCitH** (*MultiParty Computation-in-the-Head*).

Una vez que concluya esta nueva convocatoria para firmas del **NIST**, y en futuras versiones de la **CCN-TEC-009**, se considerarán y recomendarán aquellas que sean declaradas estándares.

3. Gobernanza de la transición postcuántica

Durante muchos años, cuando se hablaba de la transición postcuántica, la conversación se centraba en la criptografía post-cuántica (**PQC**): qué esquema resiste mejor la amenaza cuántica, los finalistas del **NIST**, la estandarización de algoritmos, librerías que la implementan, etc.

Sin embargo, a nivel organizativo, las instituciones necesitan definir quién lidera la transición, cómo medir el progreso, y cómo mantener el cumplimiento normativo.

La transición hacia la criptografía resistente a la computación cuántica requiere un **modelo de gobernanza** que garantice la coordinación entre las distintas áreas de la institución (técnicas, de negocio, legales, de protección de datos y de riesgo) con la finalidad de estar alineados con los distintos marcos regulatorios y estándares internacionales que le sean de aplicación a la institución.

Con el fin de llevar a cabo la transición postcuántica de manera adecuada, las instituciones deberán asignar personal y presupuesto para tal fin.

3. Gobernanza de la transición postcuántica

La gobernanza de la transición se regirá por los siguientes principios:

- Definición de roles y responsabilidades a todos los niveles organizativos.
- Documentación continua de decisiones, dependencias criptográficas, avances realizados y riesgos.
- Priorización de activos y sistemas críticos en función de su exposición y riesgo (alto, medio y bajo).
- Capacidad de evolucionar conforme maduren los estándares postcuánticos y cambien las amenazas (cripto-agilidad).
- Alineación con estándares emergentes (p. ej., **NIST PQC**) y regulaciones sectoriales (**ENS**, **NIS2**, **DORA**, **RGPD**, etc.).

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

- **Comité de Dirección Postcuántico**
  - Órgano responsable de la supervisión global.
  - Define la estrategia de migración y prioridades, aprueba inversiones y gestiona riesgos a nivel corporativo.
- **Oficina de Programa PQC**
  - Actúa como punto central de recopilación de la información, y gestiona las inversiones y adquisiciones necesarias para la migración
  - Encargada de la coordinación de la estrategia de migración, seguimiento de hitos y reporte de incidencias y logros.
- **Equipo técnico especializado**
  - Grupo de expertos en criptografía, arquitectura y seguridad.
  - Encargado de valorar y definir qué algoritmos y estándares son más adecuados para la institución, y apoyar en la implementación de los mismos.
- **Responsables de dominio/aplicación**
  - Personal de la unidad de sistemas o responsables de negocio.
  - Responsables de la ejecución local de la migración.

4. Recomendaciones del CCN

El **Centro Criptológico Nacional** sigue atentamente las publicaciones del **NIST** conducentes al establecimiento de nuevos estándares resistentes a la computación cuántica. En este sentido, en colaboración con otros organismos internacionales, especialmente europeos, lleva a cabo sus propias investigaciones sobre los algoritmos postcuánticos propuestos.

Ya nadie pone en duda la amenaza que supone el desarrollo de los ordenadores cuánticos para la criptografía actual. Por ello, el **CCN** urge a la comunidad criptográfica española, así como al sector público, la industria, las empresas y la Academia a iniciar su preparación, a la mayor brevedad, para evitar o, al menos, paliar, tal amenaza.

A continuación se recogen las principales recomendaciones del **CCN** para planificar e implementar los procesos de migración y mitigar los riesgos asociados a la computación cuántica.

4.1. Plan de migración

Es necesario desarrollar un **plan de migración** que debe incluir los siguientes puntos:

- Asignar personal y presupuesto (ver **Sección 3.**).
- Determinar la información que se debe proteger y hasta cuándo.
- Realizar un inventario exhaustivo de los elementos de la infraestructura que empleen criptografía (productos *hardware* o *software*, tarjetas, y cifradores, etc.) para proteger la información y los activos.
- Analizar con rigor si tales elementos son o no resistentes a la computación cuántica.
- Establecer un plan de migración a las soluciones *quantum resistant* (**QR**) (véase la **Sección 4.6**).
- Decidir qué nuevos productos se necesitan y cuánto tiempo requieren para su adquisición y despliegue.
- Determinar cuánto tiempo se tiene disponible (véase el Teorema de M. Mosca en el **ANEXO B**).

4.2. Mecanismos de encapsulación de claves

El **CCN**, recomienda los **KEM** seleccionados por el **NIST** como el estandarizado, **ML-KEM** [29], y el futuro estándar **HQC-KEM** [1]. Además, al igual que otros organismos de seguridad europeos, tiene en cuenta el algoritmo **FrodoKEM** [24], basado en el problema **LWE** (*Learning With Errors*, véase el **anexo A.3**) definido sobre retículos, que se incluye en la **Tabla 3**, junto con los ya considerados estándares.

CRIPTOSISTEMA ASIMÉTRICO Y KEM	PRIMITIVA MATEMÁTICA
ML-KEM	Retículo estructurado (MLWE)
HQC-KEM	Código corrector de errores (HQC)
FrodoKEM	Retículo no estructurado (LWE)

Tabla 3. Algoritmos KEM recomendados por el CCN y primitivas matemáticas asociadas.

Debe recordarse que **FrodoKEM** [24] fue incluido por el **NIST** en la tercera ronda como un algoritmo alternativo y no como finalista, habiendo sido descartado a partir de la tercera ronda [28]. Las razones alegadas se deben, fundamentalmente, a que su rendimiento es menor que el de otros algoritmos basados en retículos.

Está aceptado que este menor rendimiento se debe a que **FrodoKEM** no emplea ninguna estructura matemática adicional y solo se basa en el problema **LWE**, al contrario de lo que hacen otros algoritmos basados en retículos, como la definición de una estructura subyacente de anillo (**RLWE**) o de módulo (**MLWE**). Esta falta de estructura hace que sea la opción de seguridad más conservadora, de ahí que el **CCN** lo mantenga como algoritmo para **KEM**.

4. Recomendaciones del CCN

El hecho de que tanto el **CCN** como otros organismos europeos apuesten por **FrodoKEM** ha supuesto que tanto **ISO** (*International Organization for Standardization*) como **IEC** (*International Electrotechnical Commission*) hayan redactado una nueva versión de la ISO/IEC 18033-2:2006/AMD 2:2026 **[16]** con el fin de incorporar este algoritmo como futuro estándar dentro de su lista de algoritmos criptográficos.

Las estructuras adicionales mencionadas (anillo o módulo) ofrecen la ventaja de que los algoritmos que se basan en ellas son más eficientes a la hora de realizar sus cómputos y requieren claves más pequeñas. Sin embargo, la existencia de tal estructura subyacente podría ser la causante de que se desarrollaran ataques contra los algoritmos que las utilizan. De hecho, esta opinión, compartida por algunos organismos de seguridad europeos, parece estar refrendada, de alguna manera, por el propio **NIST** quien considera a **FrodoKEM** como una especie de algoritmo de respaldo conservador para el caso en el que se desarrollen ataques contra los algoritmos basados en retículos estructurados.

Como es lógico, el **CCN** también considera como autorizados los **KEM** seleccionados por el **NIST**, esto es, **ML-KEM** y **HQC-KEM**, presentados en la **Tabla 1**.

En la guía **CCN-STIC 221** "Mecanismos Criptográficos Autorizados por el **CCN**" **[5]** se incluyen todos los mecanismos criptográficos mencionados.

4.3. Firmas digitales

El **CCN** también recomienda las firmas que el **NIST** ha seleccionado como estándares (véase **Tabla 4**).

FIRMA DIGITAL	PRIMITIVA MATEMÁTICA
ML-DSA	Retículo estructurado (MLWE)
FN-DSA (pendiente de estandarización)	Retículo estructurado (SIS)
SLH-DSA	Funciones *hash*

Tabla 4. Estándares de firma recomendados por el CCN y primitivas matemáticas asociadas.

4.4. Firmas digitales para actualizaciones de *firmware* y *software*

El **CCN** considera que la firma digital del *firmware* y *software* es uno de los puntos más críticos en la transición.

Antes de que el concurso del **NIST** para firma postcuántica se resolviera, el **CCN** recomendó el empleo del algoritmo **XMSS** para la firma de *firmware* o *software* definido en la Publicación Especial SP800-208 del **NIST** **[25]**. No obstante, este algoritmo, presenta algunas desventajas, ya que solo puede realizar un número

limitado de firmas. Por ello, se considera que es especialmente adecuado para la firma de actualizaciones de *firmware* o *software*.

Asimismo, una vez publicados los estándares del **NIST** para los algoritmos de firma postcuánticos, desde el **CCN** también se autoriza el empleo de estos algoritmos para la firma de las actualizaciones de *firmware* o *software*. La necesidad de hibridación o no de estos algoritmos, dependerá de la primitiva matemática en la que se base su seguridad (ver **punto 4.6.2**).

El **CCN** recomienda el **uso de forma inmediata de las firmas digitales autorizadas para la actualización de *firmware* y *software***, tal y como se muestra en la **Tabla 5**.

FIRMA PARA *FIRMWARE* Y *SOFTWARE*	PRIMITIVA MATEMÁTICA
XMSS	Funciones *hash* con estado
SLH-DSA	Funciones *hash* sin estado
Hibridación de firma PQC con firma precuántica	Firma hibridada (ver **punto 4.6.2**)

Tabla 5. Esquema de firma para *firmware* recomendado por el CCN y primitiva matemática asociada.

4.5. Longitudes de clave para algoritmos simétricos y funciones *hash*

Como ya se ha mencionado en la **Sección 1.** los algoritmos de cifrado simétrico se consideran menos vulnerables a la computación cuántica que los asimétricos, dado que la amenaza demostrada hasta ahora es que, caso de existir un ordenador cuántico con la suficiente capacidad de cómputo, la seguridad que ofrecen sería equivalente a la del mismo algoritmo cuya clave tuviera la mitad de la longitud original.

Recientes estudios **[41]**, han demostrado que la implementación del **algoritmo de *Grover*** contra los algoritmos simétricos y algoritmos de funciones *hash*, no es tan prometedora, debido a que la ventaja teórica de este algoritmo se ve limitada en la práctica por su naturaleza secuencial (no paralelizable) y por el elevado coste de los ordenadores cuánticos tolerantes a fallos.

Por este motivo, aunque sería recomendable aumentar la seguridad de los algoritmos simétricos y funciones *hash* siempre que sea posible, el **CCN** considera que no es lo más prioritario, autorizando, además del AES 256, el empleo de AES 128 y AES 192, así como funciones *hash* a partir de 256 *bits*.

En la **Tabla 6** se listan los algoritmos simétricos y las funciones *hash* recomendadas por el **CCN**.

ALGORITMO	LONGITUD DE CLAVE / RESUMEN
AES	128 | 192 | 256
SHA2	256 | 384 | 512
SHA3	256 | 384 | 512

Tabla 6. Algoritmos simétricos recomendados por el CCN y las longitudes de clave o resúmenes correspondientes.

4.6. Soluciones híbridas

Dado que los **algoritmos criptográficos postcuánticos** recientemente estandarizados (o en proceso) son relativamente nuevos, es claro que necesitarán de un largo periodo de análisis para garantizar su seguridad. Además, en los últimos años se han venido publicando ataques contra los mismos, que explotan, fundamentalmente, errores en sus implementaciones y ataques por canal lateral o inducción de fallos. Por estas razones se recomienda emplear, al menos en estas primeras etapas, soluciones híbridas cuanto antes, es decir, **combinar de modo simultáneo algoritmos postcuánticos con algoritmos precuánticos**.

Dicho de otro modo, una «solución híbrida» consiste en construir una solución que combine primitivas precuánticas (actuales) y primitivas postcuánticas, con el fin de obtener tanto las garantías criptográficas tradicionales como las que ofrecen las soluciones resistentes a la computación cuántica **[20]**.

Otra ventaja adicional de estas soluciones es que facilitan el desarrollo de soluciones cripto-ágiles (ver **Sección 4.7**). Si uno de los algoritmos de la solución resultara ser vulnerable, sería fácilmente reemplazable por otro de su misma familia.

Por otra parte, es claro que la hibridación no es una solución permanente. De hecho, se trata de un paso intermedio en la migración de la criptografía actual a la postcuántica, dado que a medida que vaya pasando el tiempo, la **PQC** se irá convirtiendo en una solución cada vez más confiable.

4.6.1. Establecimiento de claves

A modo de ejemplo, se puede mencionar que en los mecanismos de encapsulación de claves, las salidas de ambos algoritmos se envían a una función de derivación de claves o **KDF** (*Key Derivation Function*) para producir la clave para el cifrado simétrico (véase la **Figura 1**).

Figura 1. Solución híbrida para el intercambio de claves como medida de transición.

Además, el empleo de soluciones híbridas requiere, en ocasiones, ajustar los protocolos criptográficos utilizados actualmente. De hecho, ya existen recomendaciones en este sentido para los protocolos **TLS 1.3** (*Transport Layer Security*) **[39]** e **IKEv2** (*Internet Key Exchange*) **[11]**, **[40]**.

4.6.2. Firmas digitales

El **CCN** recomienda la hibridación de las firmas digitales en el caso de que se empleen esquemas **PQC** de firma digital basadas en retículos (**ML-DSA** y **FN-DSA**).

En el caso de emplear firmas digitales **PQC** basadas en *hashes*, no se considera necesario realizar hibridación (**XMSS** y **SLH-DSA**).

4.7. Cripto-agilidad

El concepto de «cripto-agilidad» o agilidad criptográfica es la capacidad que debe tener un sistema de seguridad para cambiar de forma rápida a nuevos mecanismos criptográficos ante la aparición de vulnerabilidades o amenazas contra los algoritmos empleados de forma habitual por dicho sistema.

La idea es poder ser resilientes, en el caso de que aparezca una vulnerabilidad, realizando las modificaciones y sustituciones de algoritmos necesarios sin interrumpir las operaciones normales de la infraestructura tecnológica. Este proceso puede incluir cambiar algoritmos criptográficos, claves de seguridad, certificados y otras tecnologías criptográficas.

Así pues, la cripto-agilidad no solo fomenta el desarrollo y la evolución del sistema, sino que también actúa como medida de seguridad o mecanismo de respuesta a incidentes.

Es posible que se publiquen nuevos ataques contra los sistemas criptográficos empleados actualmente, así como que se disponga de un ordenador cuántico con la suficiente capacidad de cómputo como para romper los criptosistemas actuales. Es por ello que la cripto-agilidad cobra mayor importancia y hay que poner especial atención en el diseño de las soluciones de seguridad, de modo que sean lo suficientemente flexibles para que permitan reaccionar con rapidez y paliar las amenazas de los nuevos desarrollos y que posibiliten garantizar el nivel de seguridad necesario.

En definitiva, la cripto-agilidad debería convertirse en un **criterio de diseño** para nuevos productos, al margen del estado de desarrollo de los ordenadores cuánticos.

4.8. Calendario recomendado

El Grupo de Cooperación en Redes y Sistemas de Información (*Network and Information Systems Cooperation Group*, **NIS CG**) ha publicado una hoja de ruta coordinada para la transición a la criptografía postcuántica en Europa **[32]**. Este documento establece un conjunto de recomendaciones que los Estados miembros deben implementar, así como un cronograma recomendado para la transición a la **PQC** en la Unión Europea.

Con la finalidad de alinearse con esta hoja de ruta, el CCN ha actualizado las fases y fechas de la transición postcuántica publicada en su primera versión de este documento (diciembre de 2022).

FASE 1

Empleo inmediato de las firmas digitales para actualizaciones de *firmware* y *software*.

FASE 2

Uso de soluciones híbridas (precuántica, postcuántica sin estandarizar, claves precompartidas) para proporcionar mayor defensa a la criptografía precuántica.

FASE 3

Empleo de soluciones híbridas (precuántica, postcuántica estandarizada) con las garantías de seguridad proporcionadas por la criptografía postcuántica.

FASE 4

Empleo de soluciones híbridas con algoritmos precuánticos seguros y postcuánticos estandarizados y recomendados por el **CCN**.

Migración completa de casos de uso de riesgo alto.

FASE 5

Adoptar e implementar los algoritmos que hayan sido recomendados por el **CCN**.

Migración completa de casos de uso de riesgo medio.

Migración completa en la medida de lo posible de casos de uso de riesgo bajo.

De forma más precisa, las acciones de cada una de las fases son:

Fase 1 "Incorporación de mecanismos de firma postcuántica para actualización de FW y SW" (desde diciembre 2022):

Tal y como se ha comentado en la **Sección 4.4**, el **CCN** recomendó el uso inmediato (diciembre de 2022) del esquema **XMSS** para la actualización de *firmware*. En esta nueva versión se añaden los nuevos mecanismos de firma digitales autorizados por el **CCN** (véase la **Tabla 5**).

Fase 2 "Preparación y adopción de soluciones híbridas preestandarización" (desde diciembre 2022 – agosto 2024):

En la **Sección 4.6** se ha señalado la importancia de utilizar soluciones híbridas para combinar las primitivas precuánticas con las primitivas postcuánticas (aún sin estandarizar), y con claves precompartidas con el fin de obtener las garantías probadas de seguridad que ofrecen las primeras a las que se añadirían las que ofrecen las segundas. Estas garantías estarían alineadas con las ventajas de la cripto-agilidad comentadas en la **Sección 4.7**.

Fase 3 "Inicio de la transición hacia estándares postcuánticos" (desde septiembre 2024 – diciembre 2026):

- En la **Sección 4.6** se ha señalado la importancia de utilizar soluciones híbridas para combinar las primitivas precuánticas con las primitivas postcuánticas (ya estandarizadas), con el fin de obtener las garantías probadas de seguridad que ofrecen las primeras a las que se añadirían las que ofrecen las segundas. Estas garantías estarían alineadas con las ventajas de la cripto-agilidad comentadas en la **Sección 4.7**. Se recomienda la pronta implementación de estos estándares **PQC**, ya sean **KEM** (véase la **Tabla 3**), firmas digitales (véase la **Tabla 4**), firmas digitales para actualizaciones de *firmware* (véase la **Tabla 5**) o simétricos (véase la **Tabla 6**), y la puesta en marcha de los mecanismos necesarios para la implementación de los nuevos estándares cuando sean publicados.
- Las instituciones han iniciado la planificación de la transición de la **PQC** y los proyectos piloto para casos de uso de riesgo alto y medio.

Fase 4 "Consolidación de la transición y protección de los casos de alto riesgo" (desde enero 2027 hasta diciembre 2030):

- Se recomienda el proceso de hibridación de modo que a los algoritmos seguros de la criptografía precuántica se unan los algoritmos postcuánticos estandarizados y recomendados por el **CCN**.
- Las instituciones han completado la transición de la **PQC** para casos de uso de alto riesgo.
- Las instituciones han completado la planificación de la transición **PQC** y los proyectos piloto para casos de uso de riesgo medio.

Fase 5 "Adopción generalizada y culminación de la transición postcuántica" (desde enero 2031 hasta diciembre 2035):

- En esta fase se deberían adoptar e implementar de forma generalizada los algoritmos que hayan sido recomendados por el **CCN**.
- Se ha completado la transición de la **PQC** para casos de uso de riesgo medio.
- Se ha completado la transición de la **PQC** para casos de uso de riesgo bajo, en la medida de lo posible.

En la **Figura 2** se muestra el calendario recomendado para implementar las fases anteriormente señaladas.

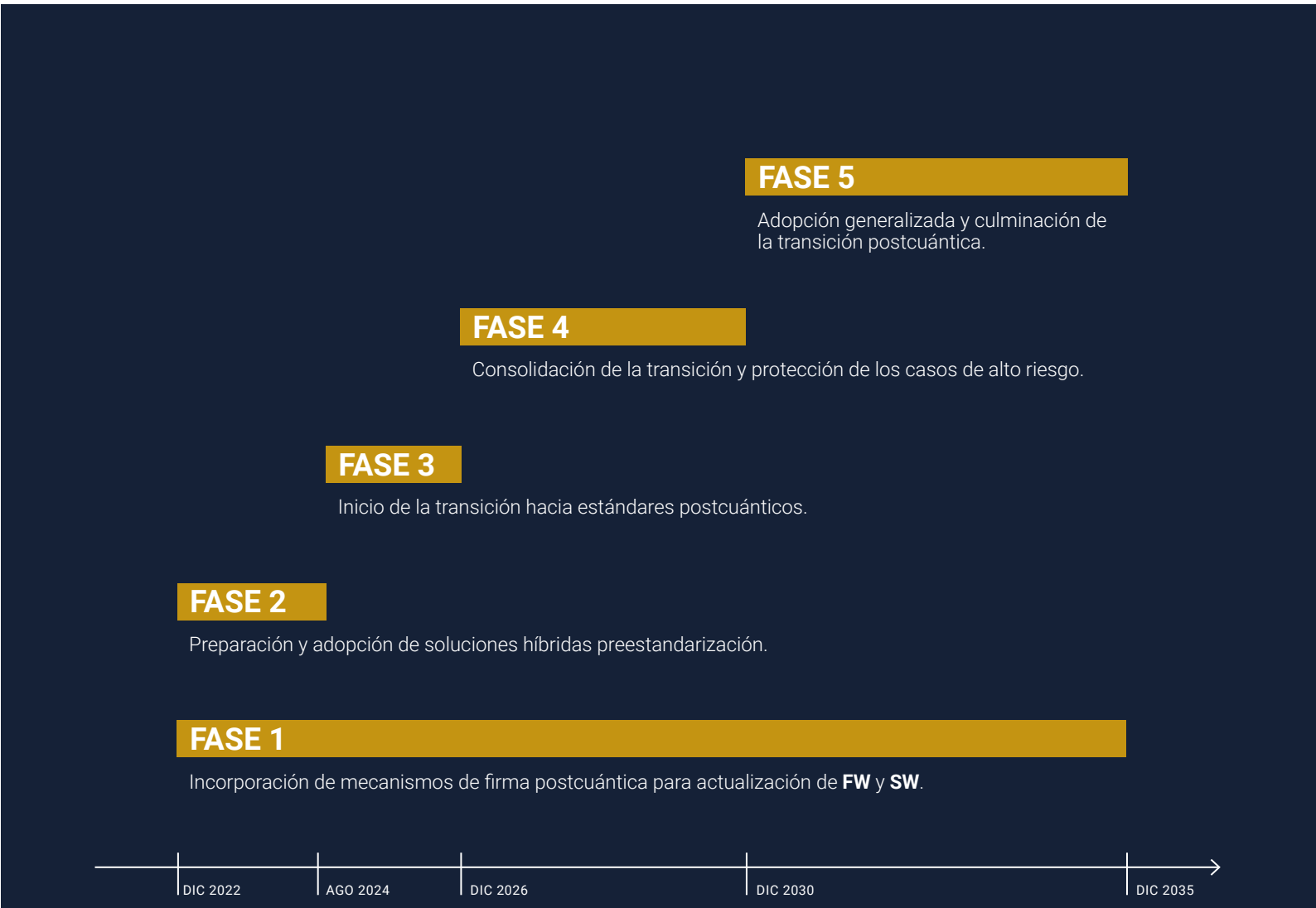


Figura 2. Calendario recomendado de las fases de actuación para la transición de la criptografía precuántica a la postcuántica.

5. Recomendaciones de otros organismos

Otros organismos internacionales, conscientes de la amenaza que supone la potencia de cálculo de la computación cuántica y de la vulnerabilidad que la misma supondrá para la protección de la información clasificada o privada, han publicado sus propias recomendaciones para abordar este problema. Entre otras, destacamos las siguientes publicaciones, que van en la línea de las recomendaciones contenidas en este informe.

1) **Agencia Nacional de Seguridad de Sistemas de Información francesa** (*Agence Nationale de la Sécurité des Systèmes d'Information,* **ANSSI**). Considera **[2]** muy positivos los esfuerzos de investigación y desarrollos prácticos y anima a los diseñadores de productos de seguridad a experimentar y prototipar soluciones híbridas precuánticas y postcuánticas, especialmente para productos que buscan una protección de la confidencialidad que perdure más allá de 2030 o que probablemente se sigan utilizando después de 2030. La **ANSSI** anima a todas las industrias a incluir la amenaza cuántica en sus análisis de riesgos y a considerar la inclusión de la mitigación cuántica en los productos criptográficos pertinentes.

2) **Oficina Federal de Seguridad de la Información alemana** (*Bundesamt für Sicherheit in der Informationstechnik*, **BSI**). Recomienda **[3]** como paso fundamental, realizar un inventario detallado de sus sistemas tecnológicos actuales, aconsejan no emplear los nuevos algoritmos **PQC** de forma aislada durante la transición, sino

adoptar enfoques híbridos que combinen los métodos tradicionales con soluciones postcuánticas, promueve la cripto-agilidad para permitir el reemplazo sencillo de algoritmos en el futuro, y sugieren la adopción de firmas digitales basadas en hash para las actualizaciones seguras de *firmware*.

3) **Agencia Nacional de Seguridad de las Comunicaciones de los Países Bajos** (*Netherlands National Communications Security Agency*, **NLNCSA**). Con el fin de proteger los datos sensibles o confidenciales, recomienda en **[33]** el uso de la criptografía postcuántica en combinación con un algoritmo asimétrico existente (construcción híbrida). La **NLNCSA** considera que esta es la mejor manera de protegerse contra ataques de ordenadores cuánticos y confía plenamente en la seguridad y la aplicación de este tipo de criptografía. En los casos en que la implementación de la **PQC** aún no sea posible, recomiendan añadir criptografía simétrica a las aplicaciones existentes como solución provisional.

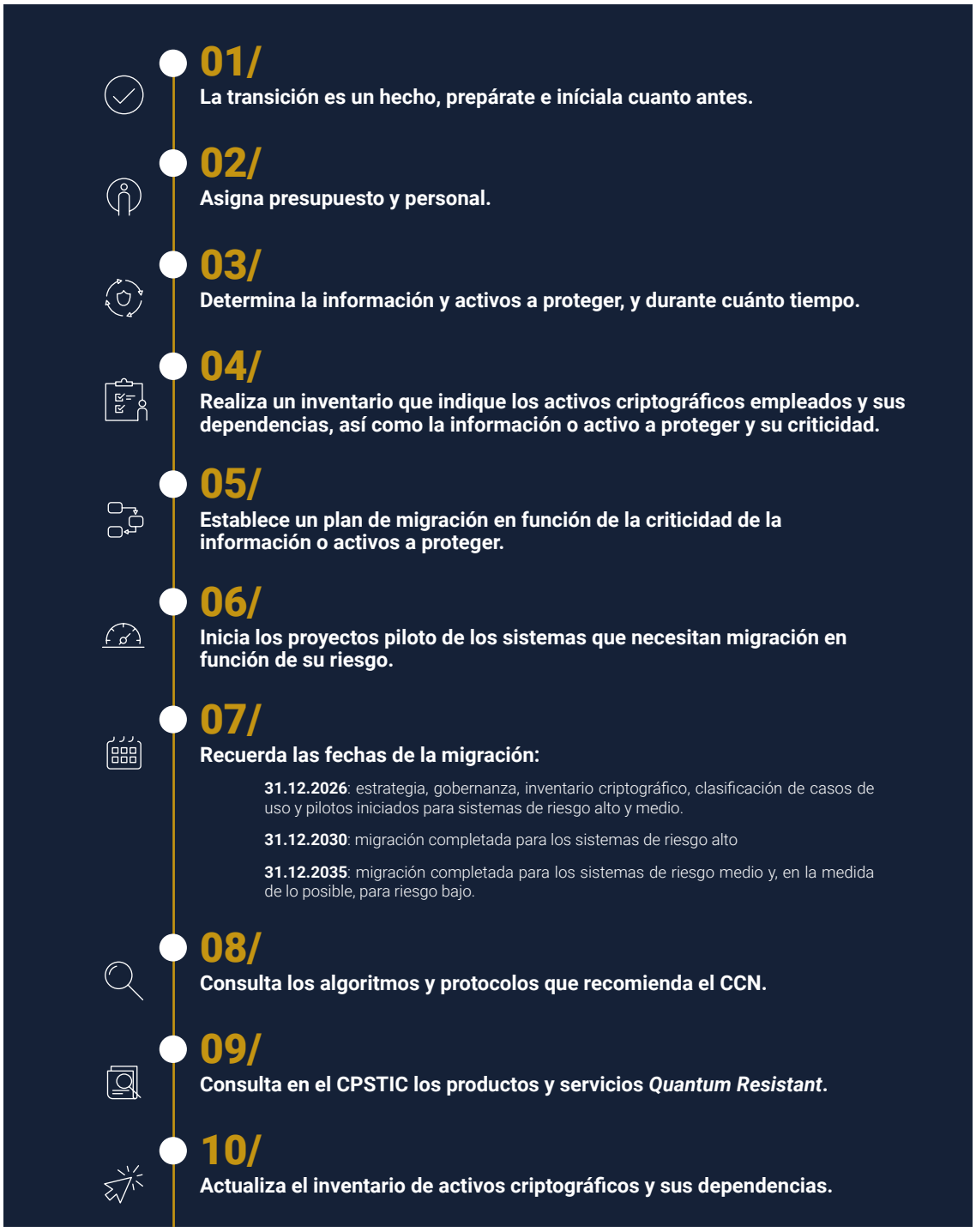
4) **Comisión Europea.** Ha publicado una Recomendación **[6]** sobre una hoja de ruta para "llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica". Así, señala que "los Estados miembros de la Unión Europea deben considerar la posibilidad de migrar sus actuales infraestructuras y servicios digitales para las administraciones públicas y otras infraestructuras críticas hacia la criptografía postcuántica lo antes posible, induciendo un cambio fundamental en los algoritmos, protocolos y sistemas criptográficos. Esta Recomendación anima a los Estados miembros a elaborar una estrategia global para la adopción de la criptografía postcuántica a fin de garantizar una transición coordinada y sincronizada entre los distintos Estados miembros y sus sectores públicos".

5) **NIST.** Su informe **[31]** describe su enfoque para la transición de algoritmos criptográficos vulnerables a la computación cuántica a algoritmos de firma digital y esquemas de establecimiento de claves postcuánticos. De hecho, identifica los estándares criptográficos vulnerables a la computación cuántica existentes y los estándares resistentes a la computación cuántica a los que deberán migrar los productos y servicios de tecnologías de la información. El objetivo del informe es fomentar la colaboración con la industria, las organizaciones de normalización y otras agencias para facilitar y acelerar la adopción de la criptografía postcuántica.

6) **Agencia de la Unión Europea para la Ciberseguridad** (*European Union Agency for Cybersecurity*, **ENISA**). En su estudio **[9]** ofrece una visión general del estado actual del proceso de estandarización de la criptografía postcuántica y en **[10]** busca comprender los desafíos de la postestandarización.

7) **NISCG** **[32]**. Su informe es la primera publicación de la hoja de ruta para la implementación coordinada incluida en la Recomendación de la Comisión **[6]**. El informe señala que las entidades de la administración pública y otras infraestructuras críticas, en particular las que se encuentran dentro del ámbito de aplicación de la Directiva **NIS2** **[34]**, deberán consultar este documento y sus posteriores publicaciones para garantizar una transición sincronizada en toda la **UE**. Esta publicación contiene un calendario recomendado para la migración de los Estados miembros hacia la **PQC** y una lista de medidas que deben incluirse en las hojas de ruta nacionales de cada Estado miembro, teniendo en cuenta y remitiéndose a la bibliografía existente cuando corresponda para evitar la duplicación de esfuerzos.

6. Decálogo para la transición



7. Referencias

[1] **C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and J. Bos.** *HQC (Hamming Quasi-Cyclic).* NIST, Round 2, 2020. http://pqc-hqc.org/index.html.

[2] **ANSSI *(Agence Nationale de la Sécurité des Systèmes d'Information).*** *ANSSI views on the post-quantum cryptography transition*, 2023, https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.

[3] **BSI *(Bundesamt für Sicherheit in der Informationstechnik).*** *Migration to Post Quantum Cryptography, Recommendations for action by the BSI*, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2.

[4] **J. Buchmann, E. Dahmen, and A. Hülsing.** *XMSS – A practical forward secure signature scheme based on minimal security assumptions.* Proc. Post-Quantum Cryptography (PQCrypto 2011), Lecture Notes Comput. Sci. 7071, pp. 117–129, 2011.https://doi.org/10.1007/978-3-642-25405-5_8.

[5] **CCN (Centro Criptológico Nacional).** *Guía de Seguridad de las TIC CCN-STIC 221. Guía de Mecanismos Criptográficos Autorizados por el CCN*, 2025. 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.

[6] **Comisión Europea. Diario Oficial de la Unión Europea.** *Recomendación (UE) 2024/1101 de la Comisión de 11 de abril de 2024 sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica.* https://www.boe.es/doue/2024/1101/L00001-00004.pdf.

[7] **R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué.** *El criptosistema RSA.* RA-MA, Madrid, España, 2005. https://www.ra-ma.es/libro/el-criptosistema-rsa_192525/.

7. Referencias

[8] **T. ElGamal.** *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Trans. Inform. Theory 31, 469–472, 1985. https://doi.org/10.1109/TIT.1985.1057074.

[9] **ENISA *(European Union Agency for Cybersecurity)***. *ENISA Report - Post-Quantum Cryptography Current state and quantum mitigation-V2*, 2021, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf.

[10] **ENISA *(European Union Agency for Cybersecurity)***, *Post-Quantum Cryptography. Integration study*, 2022, https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study.

[11] **S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov**. *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*. Internet Engineering Task Force, RFC 8784, 2020. https://tools.ietf.org/html/rfc8784.

[12] **A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini, y J. Muñoz Masqué**. *Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales.* RA-MA, Madrid, España, 2012. https://www.ra-ma.es/libro/criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para-estudiantes-y-profesionales_192382.

[13] **L.K. Grover.** *A fast quantum mechanical algorithm for database search.* Proc. 28th annual ACM symposium on Theory of Computing (STOC'96), pp. 212–219, 1996. https://dl.acm.org/doi/10.1145/237814.237866.

[14] **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.

[15] **A. Hülsing, D. Butin, S.L. Gazdag, J. Rijneveld, and A. Mohaisen.** *XMSS: extended Merkle signature scheme*. Internet Engineering Task Force, RFC 8391, 2018. https://tools.ietf.org/html/rfc8391.

[16] **ISO/IEC**, *ISO/IEC 18033-2:2006/* **AMD 2:2026**. *Information technology – Security techniques – Encryption algorithms. Part 2: Asymmetric ciphers*, 2006, https://www.iso.org/es/contents/data/standard/03/79/37971.html.

[17] **M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia.** *Breaking symmetric cryptosystems using quantum period finding*. Proc. Advances in Cryptology – CRYPTO 2016, Lecture Notes Comput. Sci. 9815, pp. 207–237, 2016. https://doi.org/10.1007/978-3-662-53008-5_8.

7. Referencias

[18] **M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia**, *Quantum differential and linear cryptanalysis*. IACR Trans. Symmetric Cryptol. 1, 71–94, 2016. https://doi.org/10.13154/tosc.v2016.i1.71-94.

[19] **N. Koblitz.** *Elliptic curve cryptosystems*. Math. Comp. 48, 177, 203–209, 1987. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[20] **B.A. LaMacchia.** *Getting Ready for the Post-Quantum Transition*. Microsoft Utimaco Webinar, 2020. https://ecstech.com/wp-content/uploads/ 2020/08/2020_ISO_BLaMacchia_Final.pdf.

[21] **D. McGrew, M. Curcio, and S. Fluhrer.** *Leighton-Micali hash-based signatures*. Internet Engineering Task Force, RFC 8554, 2019. https://tools.ietf. org/html/rfc8554.

[22] **V.S. Miller.** *Use of elliptic curves in cryptography.* Proc. Advances in Cryptology – CRYPTO 1986, Lecture Notes Comput. Sci. 218, 417–426, 1986. https://doi.org/10.1007/3-540-39799-X_31.

[23] **M. Mosca.** *Cybersecurity in a Quantum World: will we be ready?* University of Waterloo, 2015. https://csrc.nist.gov/csrc/media/events/ workshop-on-cybersecurity-in-a-post-quantum-world/documents/ presentations/session8-mosca-michele.pdf.

[24] **M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila.** *FrodoKEM*. Online publication, 2020. https://frodokem.org/.

[25] **NIST (*National Institute of Standards and Technology*).** *Recommendation for Stateful Hash-Based Signature Schemes*. NIST, Special Publication, SP800-208, 2020. https://doi.org/10.6028/NIST.SP.800-208.

[26] **NIST (*National Institute of Standards and Technology*).** *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, NIST FIPS 203, 2024. https://doi.org/10.6028/NIST.FIPS.203.

[27] **NIST (*National Institute of Standards and Technology*)**. *Post-quantum cryptography*. On-line publication, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[28] **NIST (*National Institute of Standards and Technology*).** *PQC standardization process: Third round candidate announcement.* Online publication, 2020. https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement.

7. Referencias

[29] **NIST (*National Institute of Standards and Technology*).** *Module-Lattice-Based Digital Signature Standard,* NIST FIPS 204, 2024. https://doi.org/10.6028/NIST.FIPS.204.

[30] **NIST (*National Institute of Standards and Technology*).** *Stateless Hash-Based Digital Signature Standard*, NIST FIPS 205, 2024. https://doi.org/10.6028/NIST.FIPS.205.

[31] **NIST (*National Institute of Standards and Technology*).** *NIST Internal Report, Transition to Post-Quantum Cryptography Standards*, NIST IR 8547 ipd, https://doi.org/10.6028/NIST.IR.8547.ipd.

[32] **NIS CG (*Network and Information Systems Cooperation Group*),** *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Part 1, Version: 1.1*, EU PQC Workstream, 11/06/2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[33] **NLNCSA (*Netherlands National Communications Security Agency*).** *Prepare for the threat of quantum computers*, 2022, https://english.aivd.nl/site/binaries/site-content/collections/documents/2022/01/18/prepare-for-the-threat-of-quantumcomputers/Prepare+for+the+threat+of+quantumcomputers.pdf.

[34] **Parlamento Europeo.** *Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) No. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)*, 2022. https://www.boe.es/doue/2022/333/L00080-00152.pdf.

[35] **T. Prest, P.A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang.** *FALCON*. Online publication, 2020. https://falcon-sign.info/.

[36] **R. Rivest, A. Shamir, and L.M. Adleman.** *A method for obtaining digital signatures and public-key cryptosystems. Commun*. ACM, 21, 2, 120–126, 1978. https://doi.org/10.1145/359340.359342.

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

[38] **D.R. Simon.** *On the power of quantum computation.* SIAM Journal on Computing, 26, 5, 1474–1483, 1997. https://doi.org/10.1137/ S0097539796298637.

7. Referencias

[39] **D. Stebila, S. Fluhrer, and S. Gueron.** *Hybrid key Exchange in TLS 1.3* (draft-ietf-tls-hybrid-design-16). Internet Engineering Task Force, 2025. https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/.

[40] **C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, and V. Smyslov.** *Multiple Key Exchanges in IKEv2 (draft-ietf-ipsecme-ikev2-multiple-ke-08).* Internet Engineering Task Force, RFC 9370, 2023. https://datatracker.ietf.org/doc/pdf/ draft-ietf-ipsecme-ikev2-multiple-ke-08.

[41] **Sarah D. and Peter C.** , *On the practical cost of Grover for AES key recovery* https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.

[42] *Hoja de ruta para la transición postcuántica en España (pendiente de publicación).*

[43] *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, 2025,* https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

[44] *Post-Quantum Cryptography: Additional Digital Signature Schemes, Ronda 3,* https://csrc.nist.gov/projects/pqc-dig-sig/round-3-additional-signatures.

ANEXO A. Problemas matemáticos

En este anexo se presentan las definiciones de los problemas matemáticos en los que se fundamenta la seguridad de determinados criptosistemas mencionados en este documento, así como otros aspectos matemáticos que se consideran oportunos para la comodidad del lector.

A1. Problema de la factorización de números enteros (PFE)

El problema matemático en el que se fundamenta la seguridad de uno de los criptosistemas de clave pública más utilizados en la actualidad (**RSA**) es el problema de la factorización de números enteros **[7]**, **[12]**.

ANEXO A. Problemas matemáticos

Es conocido el **Teorema Fundamental de la Aritmética**, en el que se afirma que todo número compuesto $n \geq 2$ admite una factorización única como producto de potencias de primos:

$$n = \prod_{i=1}^{k} p_i^{e_i} = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

Siendo los p_i primos distintos y cada e_i un entero positivo. A partir de este teorema se plantea el siguiente problema.

Definición 1

El «**problema de la factorización**» de un número entero compuesto n consiste en determinar su factorización como producto de sus factores primos.

Los métodos de factorización se clasifican en dos grupos dependiendo, fundamentalmente, de su tiempo de ejecución: los de «propósito general» y los de «propósito especial». Los tiempos de computación de los de propósito general sólo dependen del tamaño del número compuesto a factorizar; mientras que los segundos proporcionan mejores resultados, es decir, su tiempo de computación mejora si el número a factorizar tiene propiedades especiales.

En el grupo de los métodos de propósito general están el método de la criba cuadrática y el de la criba general del cuerpo numérico; mientras que en el grupo de los de propósito especial destacan el método de las divisiones sucesivas, los métodos ***ρ(ro)*** y ***p-1*** de *Pollard*, el método de las curvas elípticas y el método de la criba especial del cuerpo de números.

Como norma, en el problema de la factorización de un número compuesto se deben utilizar, en primer lugar, los métodos de propósito especial dado que suelen ser más eficientes. Por esta razón, inicialmente se deben buscar los factores primos pequeños del número compuesto dado utilizando, siempre que sea posible, algunas de las propiedades del número. Si estos métodos no proporcionan la solución deseada, se pueden utilizar los métodos de propósito general.

A2. Problema del logaritmo discreto (PLD)

El «**problema del logaritmo discreto**» es un caso particular del problema general del cálculo de logaritmos. Es conocido que el logaritmo de a en la base b es el número $x \in \mathbb{R}$, escrito, $\log_b a = x$, precisamente si x es la potencia a la que hay que elevar la base para obtener el número dado: $b^x = a$

No obstante, cuando el conjunto de los números reales se sustituye por el grupo multiplicativo $\mathbb{Z}^*_p$, entonces se habla del logaritmo discreto [7], [12].De forma más precisa,

Definición 2

Dado un número primo p, un generador g del grupo cíclico multiplicativo $\mathbb{Z}^*_p$ y un elemento $a \in \mathbb{Z}^*_p$, el «**problema del logaritmo discreto**» consiste en determinar de forma eficiente el entero x con $0 \leq x \leq p - 2$ de modo que $g^x \equiv a \pmod p$, es decir, $x = \log_g a \pmod p$.

Si el grupo cíclico es aditivo, todo elemento del grupo G será un múltiplo del generador g, $g + g + \ldots + g = k \cdot g$. Por tanto, en este caso se tiene la siguiente:

Definición 3

Dado un grupo aditivo cíclico G, un elemento $a \in G$ y un generador g, el «**problema del logaritmo elíptico**» (a veces llamado logaritmo discreto aditivo) consiste en determinar de forma eficiente el entero x con $0 \leq x \leq p - 2$ de modo que $x \cdot g = a$.

El problema del logaritmo discreto es el problema en el que se basa la seguridad de determinados protocolos criptográficos, como es el protocolo de intercambio de clave de *Diffie-Hellman* (**DH**) y el esquema de cifrado de *ElGamal*. Por su parte, el problema del logaritmo elíptico es la base de la seguridad del protocolo análogo de intercambio de clave de *Diffie-Hellman* sobre curvas elípticas (**ECDH**) y los esquemas de cifrado basados en curvas elípticas (**ECC**).

A3. Problema del aprendizaje con errores (LWE)

Algunos de los problemas más interesantes de la criptografía postcuántica se han definido considerando el concepto de retículo (*lattice*, en inglés), como ya se ha mencionado para los estándares **ML-KEM**, **ML-DSA** y **FALCON** en la **Secciones 4.2** y **4.3**.

Dada una base de vectores, $\boldsymbol{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$, del espacio vectorial $\mathbb{R}^n$, un retículo, $\boldsymbol{L}$, es un subespacio vectorial formado por las combinaciones lineales enteras (no reales) de los vectores $\boldsymbol{b}_i$, esto es, $\boldsymbol{L} = \{\sum_{i=1}^{n} a_i \cdot b_i : a_i \in \mathbb{Z}\}$. El conjunto de vectores $\boldsymbol{B}$ se conoce como base del retículo.

El «**problema del aprendizaje con errores**» o **LWE** (*Learning With Errors*) se parametriza por un entero $\boldsymbol{n}$, un número primo $\boldsymbol{q} \geq \mathbf{2}$ y una distribución de probabilidad $\boldsymbol{\chi}$ sobre $\mathbb{Z}_q$. Aunque el problema **LWE** no se define directamente sobre un retículo, se puede reducir al problema de encontrar vectores cortos en un retículo específico, lo que lo vincula con la seguridad de los sistemas basados en retículos.

De hecho, el «**problema del vector más corto**» o **SVP** (*Shortest Vector Problem*) en un retículo consiste en encontrar un vector no nulo del retículo que sea el más corto, es decir, el de menor norma posible (en general, la norma considerada es la euclídea). Dicho de otro modo, se tiene la siguiente definición:

Definición 4

Dado un retículo, $\boldsymbol{L}$, el «***problema del vector más corto***» consiste en calcular un vector no nulo del retículo, $v \in \boldsymbol{L}$, tal que $\|v\| = \min_{x \in L / \{0\}} \|x\|$.

Típicamente $\boldsymbol{\chi}$ es una distribución normal de media v y desviación estándar $\boldsymbol{\delta}$:

$$\chi = G(x) = \frac{1}{\delta\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{x-v}{\delta}\right)^2}.$$

Una distribución $A_{s,\chi}$ de un problema **LWE** sobre $\mathbb{Z}_q^n$ **X** $\mathbb{Z}_q$ se muestrea eligiendo al azar un valor secreto $s \in \mathbb{Z}_q^n$ uniforme y aleatoriamente $a \xleftarrow{}_{\chi} \mathbb{Z}_q^n$, $e \xleftarrow{}_{\chi} \mathbb{Z}_q$ y considerando como salida el par (a , b), siendo $b = \langle s , a \rangle + e \ (mod\ q)$.

Existen dos versiones del problema **LWE**: búsqueda y decisión.

En la **versión de búsqueda del problema LWE** se dan m muestras independientes (a_i , b_i)$\in \mathbb{Z}_q^n$ **X** $\mathbb{Z}_q$ de $A_{s,\chi}$ con $b_i = \langle s , a_i \rangle + e_i \ (mod\ q) \in \mathbb{Z}_q$, siendo e_i un error pequeño tomado de la misma distribución χ, entonces, se trata de encontrar el vector secreto s $\in \mathbb{Z}_q^n$, siendo $m > n$.

La idea es determinar el valor s a partir de m muestras dadas:

$$
\begin{aligned}
a_1 \xleftarrow{}_{\chi} \mathbb{Z}_q^n, b_1 &= \langle s, a_1 \rangle + e_1 \ (mod\ q), \\
a_2 \xleftarrow{}_{\chi} \mathbb{Z}_q^n, b_2 &= \langle s, a_2 \rangle + e_2 \ (mod\ q), \\
&\vdots \\
a_m \xleftarrow{}_{\chi} \mathbb{Z}_q^n, b_m &= \langle s, a_m \rangle + e_m \ (mod\ q).
\end{aligned}
$$

Si se emplea la **notación matricial**, el problema **LWE** consiste en calcular el vector secreto $s = (s_1, s_2 , \dots , s_n)^T \in \mathbb{Z}_q^n$ en la expresión matricial $b = A \cdot s + e$, siendo la matriz de los vectores $a_i \in \mathbb{Z}_q^n$, esto es, $A = (a_1, a_2 , \dots , a_n)^T \in \mathbb{Z}_q^{mxn}$, $e = (e_1, e_2 , \dots , e_n)^T \in \mathbb{Z}_q^{mxn}$ es el vector de error y $b = (b_1, b_2 , \dots , b_n)^T \in \mathbb{Z}_q^m$ es un vector con $b_i = \langle s , a_i \rangle + e_i \ (mod\ q)$.

En la **versión de decisión del problema LWE**, el objetivo es distinguir entre dos pares de vectores (a_i , b_i) y ($\overline{a}_i$, $\overline{b}_i$) donde a_i , $\overline{a}_i \xleftarrow{}_{\chi} \mathbb{Z}_q^n$, $b_i = \langle s , a_i \rangle + e_i \ (mod\ q) \in \mathbb{Z}_q$ y $\overline{b}_i \in \mathbb{Z}_q$. Es decir, se trata de decidir, para un par de vectores dados, si el segundo vector es el producto escalar del primer vector por algún vector secreto, s sumado con algún error, o si es el segundo vector es uniformemente aleatorio.

En el caso de que se considere una estructura subyacente de anillo en el retículo, se habla del problema **LWE** sobre anillos o **RLWE** (*Ring Learning With Errors*) y si tal estructura es la de módulo, se habla del problema **LWE** sobre módulos o **MLWE** (*Module Learning With Errors*).

En particular, el problema sobre el que se sustenta la seguridad del estándar **ML-KEM** es el **MLWE**. Este problema lleva a cabo las operaciones haciendo uso de la estructura de módulo, lo que permite una mayor eficiencia y flexibilidad en los parámetros. De forma más formal, el «**problema MLWE**» considera los siguientes parámetros: un módulo sobre el anillo $R_q = \mathbb{Z}_q^n [x]/(x^n + 1)$, es decir, $(R_q)^k$, donde q es

un número primo, n es una potencia de 2, k es la dimensión del módulo (número de filas) y l (número de columnas). En general, las distribuciones de error consideradas son discretas y centradas en el 0.

Una **instancia del problema MLWE** es la siguiente: se da una matriz $A \in (R_q)^{k \times l}$ elegida al azar, un vector secreto $s \in (R_q)^l$ con coeficientes pequeños, un vector de error $e \in (R_q)^l$, también con coeficientes pequeños, se calcula $b = A \cdot s + e$. El problema **MLWE** consiste en distinguir entre pares (A,b) generados como se acaba de indicar y pares (A,b), donde b se elige uniformemente al azar en $(R_q)^k$.

A4. Problema de la solución entera más corta (SIS)

Dado un retículo, en el «**problema de la solución entera más corta**» o **SIS** (*Short Integer Solution*) se consideran m vectores uniformemente aleatorios $a_i \in \mathbb{Z}_q^n$ que definen una matriz $A \in \mathbb{Z}_q^{n \times m}$ se trata de encontrar un vector no nulo $z \in \mathbb{Z}^m$ de norma $||z|| \leq \varepsilon$, tal que:

$$A \cdot z = \sum_{i=1}^{m} a_i \cdot z_i = 0 \in \mathbb{Z}_q^n.$$

A5. Problema de decodificación de síndromes en códigos cuasicíclicos (HQC)

Es sabido que cuando se transmite un mensaje codificado, $\boldsymbol{m}$, éste puede sufrir modificaciones o errores debido, por ejemplo, al ruido en el canal de transmisión, de modo que, en lugar de transmitirse $\boldsymbol{m}$, se transmite una información errónea, $\boldsymbol{r}$. Para detectar estos errores, se utiliza lo que se conoce como matriz de control de paridad, $\boldsymbol{H}$, que está diseñada específicamente para el código que se esté utilizando. El síndrome, $\boldsymbol{s}$, asociado al código utilizado es un vector que indica si hay errores y, en algunos casos, indica dónde están. El síndrome se calcula por la expresión $\boldsymbol{s} = \boldsymbol{H} \cdot \boldsymbol{r}^{\boldsymbol{T}} \ (\boldsymbol{mod}\ \ \boldsymbol{2})$. La decodificación de síndromes es el proceso por el cual, dado un mensaje recibido, r, se calcula un síndrome que indica la posición o patrón del error, y luego se corrige el mensaje recibido para obtener el mensaje original, $\boldsymbol{m}$.

Un código cuasicíclico es un tipo de código lineal en el que los bloques de bits se repiten de forma cíclica, de modo que se logran determinadas propiedades, como que las representaciones son más compactas, las operaciones algebraicas a realizar son más eficientes y se logra un mejor rendimiento criptográfico. En particular, los códigos de *Hamming* cuasicíclicos combinan la estructura de los códigos de *Hamming* con la propiedad de ser cuasicíclicos. Por su parte, un código de **Hamming** es un código lineal binario que permite detectar y corregir errores agregando bits de paridad redundantes a los datos originales, de forma que se pueda identificar la posición del bit erróneo si ocurre un error de un solo bit.

El «problema de decodificación de síndromes en códigos de *Hamming* cuasicíclicos» (*Hamming Quasi-Cyclic*) consiste en: dado un síndrome, se trata de encontrar el vector de error que lo generó, sin que se conozca la estructura interna del código.

Este problema es NP-completo en el caso general, lo que significa que no se conoce ningún algoritmo eficiente para resolverlo en todos los casos.

ANEXO B.
Teorema de Michele Mosca

El teorema de M. Mosca puede enunciarse en los siguientes términos [23]:

Teorema Sea x el tiempo (en años) que uno necesita que sus datos confidenciales sean seguros, y el tiempo (en años) que uno necesita para volver a equipar la infraestructura existente con una solución resistente a la computación cuántica y z el tiempo (en años) que se tardará en construir un ordenador cuántico a gran escala (o cualquier otro avance relevante). Entonces, si $x + y > z$, uno tiene un grave problema.

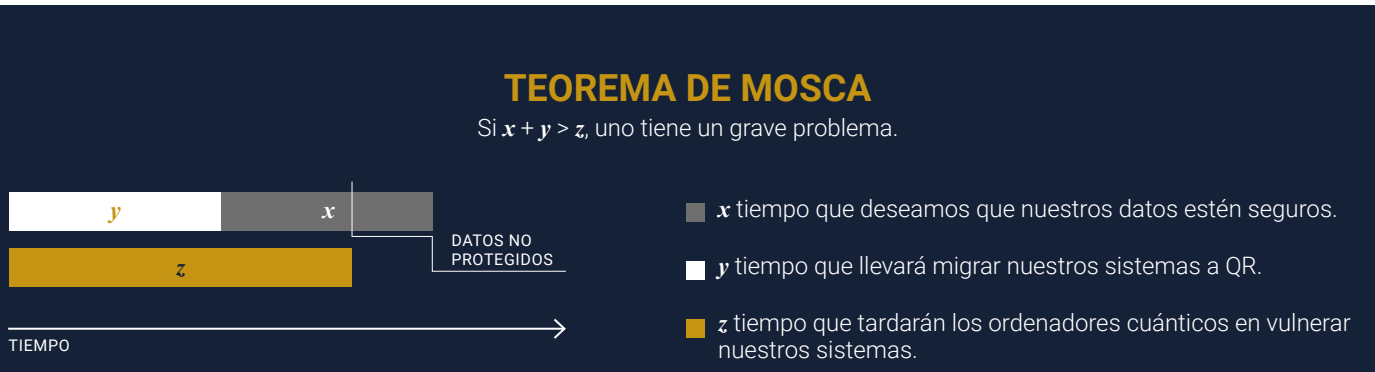


Figura 3. Esquema gráfico del teorema de M. Mosca.


JULIO 2026
CCN-TEC 009
BP/37

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**

Recomendaciones para una transición postcuántica segura

GUÍA DE BUENAS PRÁCTICAS

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC