FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA:

competencia geopolítica y regulación internacional

Autor: Esther López Fuentes

5º E-5

Derecho Mercantil Internacional

Tutor: Pablo Sanz Bayón

Madrid

Abril de 2025

" Hoy en día, la innovación vuelve a estar en el centro de la competencia global que reestructura el entorno de seguridad internacional: aquellos que obtienen una ventaja tecnológica y establecen los estándares hoy dominarán el futuro."[1]

[1] Esta aseveración de Josep Borrell de 2022 encapsula ya la premisa principal de esta investigación. Citado en León, G., "*Relevancia geopolítica de las tecnologías duales: consecuencias y oportunidades para reforzar la soberanía tecnológica de la Unión Europea*", *UPM Press*, 2023, p.25 (disponible en: https://oa.upm.es/76650/1/AF_GONZALO_LEON_Relevancia.pdf, última consulta 20/10/2024).

RESUMEN:

El presente trabajo aborda las problemáticas que surgen ante la intersección de desarrollo tecnológico, geopolítica y regulación internacional en el contexto de la estandarización de la criptografía post-cuántica (PQC, por sus siglas en inglés). El estudio se centra en analizar cómo esta tecnología emergente, diseñada para resistir ataques de computadores cuánticos en la protección de datos digitales, ha desencadenado una intensa competencia global por el desarrollo de estándares sólidos.

En primer lugar, se comienza estableciendo un marco teórico en que se presentan los fundamentos técnicos de la criptografía post-cuántica, explicando su relevancia para la ciberseguridad global y analizando la amenaza que los eventuales avances en computación cuántica plantea a los sistemas criptográficos tradicionalmente empleados.

A continuación, se examina el panorama geopolítico en que se encuadra la carrera internacional por el desarrollo de estándares de criptografía post-cuántica. En este punto se desglosan las principales motivaciones que justifican la competencia geopolítica y se identifican las principales estrategias e iniciativas de normalización realizadas hasta la fecha por actores clave.

Finalmente, se profundiza en las implicaciones regulatorias de la estandarización de la criptografía post-cuántica, para identificar los principales retos y oportunidades que la estandarización de esta tecnología plantea, enfatizando la necesidad de cooperación internacional en un contexto de competencia tecnológica. El trabajo concluye con un análisis de posibles estrategias regulatorias internacionales, proponiendo nuevas soluciones que reconozcan las complejas dinámicas tecnológicas, políticas y económicas que el desarrollo de unos estándares robustos plantea.

Palabras clave: criptografía post-cuántica, estandarización, geopolítica, derecho mercantil, ciberseguridad.

LISTADO DE SIGLAS Y ABREVIATURAS

AES: *Advanced Encryption Standard*.

AMETIC: Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones.

ANSSI: *Agence nationale de la sécurité des systèmes d'information*.

ASPI: *Australian Strategic Policy Institute*.

BSI: *Bundesamt für Sicherheit in der Informationstechnik*.

CACR: *Chinese Association for Cryptographic Research*.

CCN: Centro Criptológico Nacional.

CEN: Comité Europeo de Normalización.

CNSA 2.0.: *Commercial National Security Algorithm Suite 2.0.*

ECC: *Elliptic Curve Cryptography.*

ENISA: *European Union Agency for Cybersecurity*.

ETSI: *European Telecommunications Standards Institute*.

FRAND: *Friendly, Reasonable and Non-Discriminatory*.

GSMA: *Global System for Mobile Communications Association*.

INCIBE: Instituto Nacional de Ciberseguridad.

IEC: *International Electrotechnical Commission.*

ISO: *International Organization for Standardization.*

MPP: *Medicines Patent Pool.*

NIST: *National Institute of Standards and Technology.*

NSA: *National Security Agency.*

NSM-10: *National Security Memorandum* 10.

OCDE: Organización para la Cooperación y el Desarrollo Económicos.

ONU: Organización de Naciones Unidas.

OMC: Organización Mundial del Comercio.

OTAN: Organización del Tratado del Atlántico Norte.

PEN: Patentes Esenciales para Normas.

PQC: *Post-Quantum Cryptography*.

PYMES: Pequeñas y Medianas Empresas.

QKD: *Quantum Key Distribution.*

RSA: *Rivest-Shamir-Adleman.*

RGPD: Reglamento General de Protección de Datos.

SGSI: Sistemas de Gestión de Seguridad de la Información.

TIC: Tecnologías de la Información y la Comunicación.

UIT: Unión Internacional de Telecomunicaciones.

UIT-T: Sector de Normalización de las Telecomunicaciones de la UIT.

UNE: Asociación Española de Normalización.

1. INTRODUCCIÓN.

En el panorama actual, el volumen masivo de datos generados y transmitidos a través de tecnologías avanzadas se ha convertido en el eje central de las sociedades modernas. Estos datos no solo impulsan una gama cada vez más amplia de actividades económicas, sino que han pasado también a ser esenciales para el funcionamiento del sector público, abarcando su aplicación tanto al desarrollo de estrategias militares como a la gestión de información ciudadana[2]. Esto es una realidad que ya se reconoce a nivel global, lo que evidencian iniciativas como el Pacto Digital Mundial de la Organización de Naciones Unidas (ONU). Este pacto intergubernamental busca procurar un uso responsable y equitativo de las tecnologías digitales, subrayando el efecto transformador que las mismas tienen y tendrán a escala mundial[3].

En este escenario, la computación cuántica es una tecnología emergente que ha destacado en los últimos años, pues el potencial que la misma ofrece capta hoy una creciente atención a nivel internacional. Según señala el Centro Criptológico Nacional (CCN), esta promete revolucionar campos muy diversos, los cuales abarcan desde la optimización logística hasta avances en aeronáutica y biotecnología. Ahora bien, mientras que las oportunidades que la computación cuántica presenta son múltiples, se advierte también que su progreso plantea desafíos significativos, particularmente en lo que respecta a la seguridad de la información y la protección de datos[4].

La comunidad científica ha identificado que una de las capacidades que estos dispositivos prometen tener será la de descifrar los sistemas y protocolos criptográficos que hoy salvaguardan la información contenida en medios digitales, incluyendo de comunicaciones gubernamentales críticas, a operaciones financieras o transacciones e información comercial. Esta situación ha desencadenado una fuerte respuesta internacional, movilizando a expertos en

[2] Instituto Europeo de Normas de Telecomunicaciones, "Quantum Computing and the risk to security and privacy", 2018, (disponible en: https://www.etsi.org/images/files/ETSITechnologyLeaflets/QuantumSafeCryptography.pdf, última consulta 20/10/2024).

[3] Naciones Unidas, *Global Digital Compact*, 2024, (disponible en: https://www.un.org/global-digital-compact/en , última consulta 20/10/2024).

[4] Centro Criptológico Nacional, "Recomendaciones para una transición postcuántica segura", 2022, p.4 (disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file, última consulta 20/10/2024).

ciberseguridad, criptógrafos y científicos de todo el mundo. Estos profesionales han intensificado sus esfuerzos para desarrollar e implementar nuevos algoritmos criptográficos, lo que ha derivado a que sean dos los enfoques principales que se plantean como posibles soluciones ante la amenaza cuántica. El primer enfoque, propone la protección de los sistemas digitales mediante criptografía cuántica simétrica. El segundo enfoque, se centra en la creación de algoritmos asimétricos de nueva generación, diseñados para resistir ataques tanto de computadoras tradicionales como cuánticas, dando origen a un nuevo campo de investigación conocido como criptografía post-cuántica (PQC, por sus siglas en inglés).

Aunque las técnicas de cifrado basadas en tecnologías cuánticas tendrían una mayor resistencia a largo plazo, la Unión Internacional de Telecomunicaciones (UIT) señala que estas tecnologías enfrentan aún una serie de obstáculos significativos[5]. Esto ha llevado a que diversas entidades nacionales de normalización concentren sus esfuerzos en el desarrollo de la criptografía post-cuántica, entendiendo que esta tecnología resulta en la actualidad la opción más viable para garantizar la seguridad de la información informatizada. Entre ellas, se encuentra la Oficina Federal de Seguridad de la Información de Alemania (BSI, por sus siglas en alemán). Este organismo subraya las limitaciones de la criptografía cuántica frente a la post-cuántica, entre las que se incluye el hecho de que mientras el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de Estados Unidos ya ha publicado estándares oficiales de criptografía post-cuántica, la implementación de soluciones cuánticas parece demasiado compleja en cuanto a que requiere de una renovación masiva de la infraestructura digital actual[6].

La realidad actual del mercado, donde las tecnologías digitales facilitan un aumento significativo de las relaciones comerciales y comunicaciones transfronterizas, demanda que las soluciones criptográficas que los distintos operadores adopten se gestionen de una manera coordinada, que garantice la interoperabilidad de los sistemas digitales. Esto subraya la necesidad de fijar unos estándares post-cuánticos internacionalmente reconocidos y aplicables, lo que surge no sólo como una medida de seguridad, sino también como un medio para

[5] Sector de Estandarización de la Unión Internacional de Telecomunicaciones, "Consideraciones de seguridad para redes de distribución de claves cuánticas", 2020, p.4, (disponible en: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf, última consulta: 21/10/2024).

[6] Federal Office for Information Security, "Quantum-safe cryptography: fundamentals, current developments and recommendations", 2021, p.54, (disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6, última consulta 20/10/2024).

preservar la cohesión de la red global del internet[7]. No obstante, el desarrollo e implementación de nuevos estándares criptográficos se ve complicado por el complejo contexto geopolítico contemporáneo.

El panorama se distingue por una intensa rivalidad entre las principales potencias, que, incluida la criptografía post-cuántica, se debaten ahora el liderazgo de las tecnologías digitales avanzadas. Esto da lugar a una nueva dinámica, que refleja un reconocimiento creciente del valor estratégico que adquieren estas tecnologías[8].

El presente trabajo de fin de grado tiene como objeto definir un marco orientativo para ajustar la regulación internacional de manera que se procure una adopción uniforme de la tecnología post-cuántica en los sistemas digitales. Estas recomendaciones están diseñadas para abordar los desafíos y aprovechar las oportunidades que presenta la normalización de las tecnologías emergentes en el paradigma geopolítico y comercial contemporáneo. Para ello, se examinará el caso concreto de la normalización de la criptografía post-cuántica, por la especial relevancia que hoy presenta para el mercado internacional y la seguridad de la información a escala global, identificando las implicaciones políticas, económicas y jurídicas que subyacen en la carrera por su estandarización.

El estudio adopta una metodología mixta, combinando enfoques cualitativos y cuantitativos para ofrecer una perspectiva integral del tema. Esta incluirá una revisión de la literatura académica más reciente y relevante, así como un análisis detallado de documentos e informes oficiales de organismos clave en el campo, como el NIST, el *Australian Strategic Policy Institute* (ASPI) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI, por sus siglas en inglés). Además, para ayudar a ilustrar las complejidades del proceso e identificar las mejores prácticas globales, se evaluarán distintas iniciativas nacionales y regionales de estandarización.

Se espera que los resultados de este estudio aporten valor añadido al corpus de conocimiento en el campo del Derecho Mercantil al estudiar la intersección entre desarrollo tecnológico, geopolítica y regulación internacional. En última instancia, el presente trabajo aspira a

[7] *Vid*. Naciones Unidas, *Global Digital Compact*, *op. cit.*
[8] *Vid*. Fonfría, A. y Duch Brown, N. (2021). "La geopolítica de la transformación digital y sus efectos en el tejido industrial", Economía industrial, 2021, n.420, p. 26.

proporcionar recomendaciones que puedan informar la formulación de políticas públicas y estrategias que reconozcan la necesidad de mantener los marcos jurídicos internacionales relevantes ante la evolución de las tecnologías.

2. MARCO TEÓRICO: FUNDAMENTOS DE LA PQC.

2.1. LA CRIPTOGRAFÍA EN LOS SISTEMAS DIGITALES.

La criptografía, cuyo origen se remonta al ámbito militar, ha experimentado una destacada evolución en el contexto de digitalización actual. Esta disciplina, definida por el Instituto Nacional de Ciberseguridad (INCIBE) como el proceso por el cual se transforma un mensaje legible en un texto cifrado, e ilegible para aquellos que desconocen el método de codificación[9], se convierte en un elemento fundamental para los sistemas digitales contemporáneos. Hoy en día, la criptografía se integra en el hardware de ordenadores y dispositivos de comunicación, en sistemas operativos, aplicaciones de software y protocolos de comunicación en red, para facilitar tanto el cifrado de datos como la autenticación de usuarios.

Desde un punto de vista técnico, los sistemas criptográficos modernos se basan en dos componentes principales: algoritmos y claves. Los algoritmos son procedimientos matemáticos complejos que definen las operaciones por las cuales se articula el proceso para convertir el texto original en texto cifrado, e ininteligible. Por otro lado, las claves de cifrado, que son generadas por estos mismos algoritmos, actúan como llaves que permiten el acceso y la decodificación de la información encriptada.

Según su método de gestión de claves, la criptografía se divide en dos categorías principales: sistemas de clave secreta o simétrica, y sistemas de clave pública o asimétrica. El Gráfico 1 sintetiza el funcionamiento de ambos tipos de esquemas, cuya distinción fundamental reside en si para el proceso de cifrado y descifrado se emplean claves idénticas o diferentes.

[9] Instituto Nacional de Ciberseguridad, "Glosario de términos de ciberseguridad: una guía de aproximación para el empresario", 2021, p.33, (disponible en: https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el, última consulta 21/10/2024).

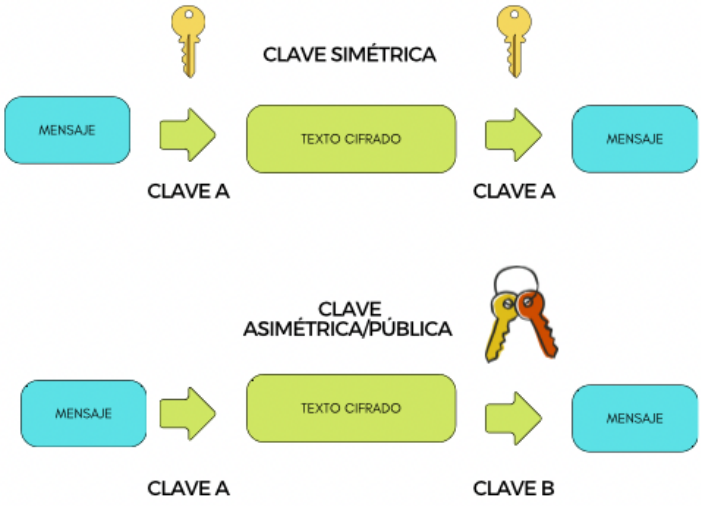


Gráfico 1. Diferencia entre criptografía simétrica y criptografía asimétrica[10].

Ambos sistemas ofrecen distintas ventajas e inconvenientes, que determinan sus aplicaciones específicas. La criptografía simétrica utiliza una clave única para cifrar y descifrar, lo que la hace altamente eficiente en el procesamiento de grandes volúmenes de datos. Sin embargo, su principal desventaja radica en que precisa que todos los participantes de la comunicación conozcan esta clave compartida. Por otro lado, la criptografía asimétrica emplea un par de claves para cada usuario, una pública, conocida por todas las partes, y una privada, sólo conocida por su propietario. Este sistema ofrece una gama más amplia de aplicaciones, incluyendo encriptación, autenticación y firmas digitales. Además, resuelve el problema de distribución de claves inherente a los esquemas simétricos. No obstante, requiere una capacidad computacional significativamente mayor y genera claves más extensas, lo que los hace sistemas menos eficientes para el cifrado de grandes cantidades de información.

Es preciso puntualizar que, visto que ambos sistemas presentan fortalezas y limitaciones distintivas, la comunidad criptográfica ha desarrollado esquemas híbridos, los cuales han venido siendo ampliamente adoptados para su implementación práctica. A través de estos se busca mitigar las debilidades respectivamente identificadas en sistemas asimétricos y simétricos, pues los mismos hacen uso de criptografía asimétrica para intercambiar de forma

[10] Fuente: Elaboración propia.

segura una clave simétrica, la cual se usa luego en conjunción con un algoritmo simétrico para cifrar la información[11].

2.2. LA COMPUTACIÓN CUÁNTICA Y SUS RIESGOS PARA LA CIBERSEGURIDAD.

Para analizar los rasgos distintivos que diferencian los computadores cuánticos de los convencionales, es preciso entender que la distinción principal entre ambos dispositivos radica en la unidad básica de información que los mismos emplean. Mientras que los computadores tradicionales utilizan bits, los cuales operan como un sistema binario de ceros y unos, los cuánticos emplean qubits. Los qubits son sistemas cuánticos de dos niveles, que ofrecen una capacidad de procesamiento significativamente superior a la de los ordenadores convencionales[12]. Esta característica permite a los computadores cuánticos la superposición y el entrelazamiento de algoritmos, lo que ha propiciado el desarrollo de algoritmos cuánticos que han demostrado ya el potencial teórico que estos dispositivos tienen para desafiar la seguridad de los esquemas criptográficos que se usan en la actualidad.

Dentro de las categorías de sistemas criptográficos previamente reseñados, de clave pública o privada, se han establecido estándares de algoritmos y protocolos criptográficos reconocidos internacionalmente. Entre los algoritmos más destacados se encuentran el *Advanced Encryption Standard* (AES) para cifrado simétrico, y el *Rivest-Shamir-Adleman* (RSA) para cifrado de clave pública y firmas digitales, o la *Elliptic Curve Cryptography* (ECC), también como esquema de clave pública.

El algoritmo de Grover destaca como una de las primeras amenazas cuánticas identificadas para la protección de datos cibernéticos. Este algoritmo ha demostrado su capacidad para comprometer sistemas de clave simétrica, pero hoy día su impacto criptográfico se considera limitado. La *Global System for Mobile Communications Association* (GSMA) sugiere que el impacto del algoritmo de Grover en los sistemas simétricos puede mitigarse eficazmente simplemente con un aumento en la longitud de las claves, por lo que no resulta necesario

[11] Escribano Pablos, J.I., "Criptografía segura frente a adversarios cuánticos: Análisis y variantes de propuestas para estandarización", *Universidad Rey Juan Carlos*, Madrid, 2022, pp.19-21.
[12] *Vid.* Anexo I con una ilustración gráfica de la diferencia en el potencial de procesamiento entre bits y qubits.

realizar cambios fundamentales en los estándares existentes[13]. Frente a esta casuística, es en los algoritmos de clave pública en los que verdaderamente se centran los desafíos que plantea la computación cuántica. El algoritmo de Shor, publicado por Peter Shor en 1994, es el algoritmo cuántico que demostró el potencial para quebrar los protocolos de ciberseguridad basados en los problemas matemáticos complejos que sustentan los sistemas de clave pública, como los logaritmos discretos y la factorización de números primos[14]. Un ejemplo es el algoritmo RSA, cuya seguridad se fundamenta en la dificultad de factorizar grandes números enteros. El Gráfico 2 proporciona una representación visual del impacto potencial de la computación cuántica en los algoritmos criptográficos tradicionales, según un análisis preliminar publicado por el NIST en 2016.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Gráfico 2. Análisis preliminar del impacto de la computación cuántica en los principales algoritmos criptográficos tradicionales[15].

Esto evidencia que un computador cuántico equipado con un número de qubits lo suficientemente grande podría resolver con facilidad la base de la seguridad en los algoritmos de cifrado de clave pública modernos. Sin embargo, cabe señalar que la computación cuántica aún no se ha convertido en una realidad práctica, y el camino hacia el desarrollo de computadores cuánticos enfrenta aún importantes obstáculos tecnológicos. La comunidad

[13] Global System for Mobile Communications Association, "Post Quantum Telco Network Impact Assessment: Whitepaper", 2023, (disponible en: https://www.gsma.com/newsroom/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper/, última consulta: 21/10/2024).
[14] Ver más en Campagna, M. *et al,* "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges", *ETSI White Paper,* n.8, 2015, (disponible en: https://www.etsi.org/media-library/white-papers, última consulta 21/10/2024).
[15] Fuente: Chen, L. *et al*, "Report on Post-Quantum Cryptography", *National Institute of Standards and Technology*, 2016, p.2, (disponible en: http://dx.doi.org/10.6028/NIST.IR.8105, última consulta 21/10/2024).

científica todavía no ha determinado una fecha exacta para en que se crearán dispositivos lo suficientemente avanzados para ser criptográficamente relevantes, aunque varias estimaciones sugieren que podrían materializarse entre 2027[16] y 2040[17]. Ahora bien, grandes empresas tecnológicas como Alice & Bob e IBM están trabajando de manera activa en reducir el número de qubits necesarios para comprometer algoritmos criptográficos actuales como el RSA-2048, lo que enfatiza la necesidad de anticiparse ya a esta realidad emergente. El Gráfico 3 ilustra esta observación, mostrando las proyecciones que la consultora McKinsey recoge en el informe "Quantum Technology Monitor 2024".

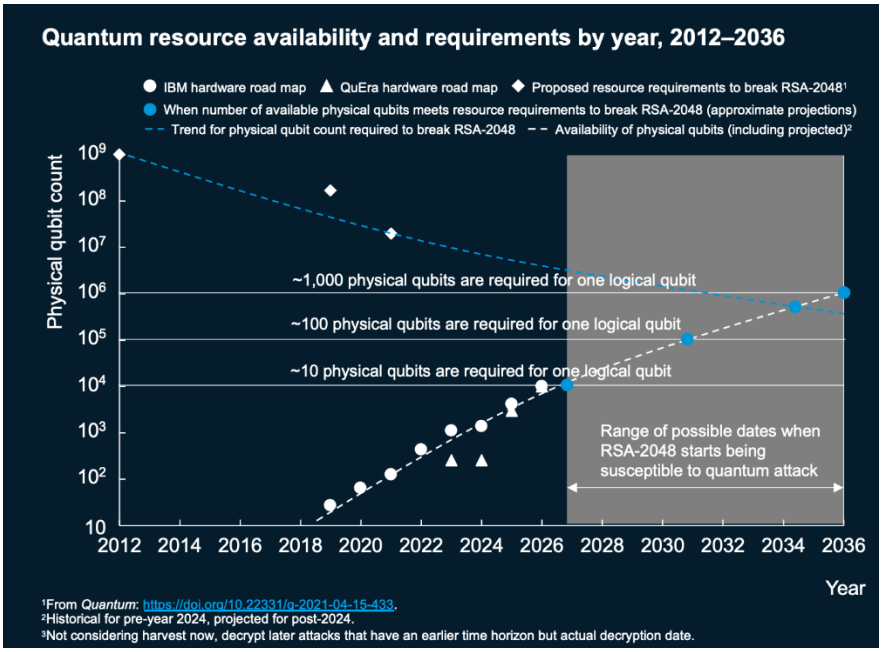


Gráfico 3. Predicciones de disponibilidad y requerimientos de recursos cuánticos para el desarrollo de computadores cuánticos (período 2012-2036)[18].

El advenimiento de la computación cuántica presenta un nuevo paradigma de desafíos para los sistemas criptográficos tradicionales. En los últimos años, el creciente interés en esta tecnología ha llevado a instituciones como el NIST a alertar sobre el peligro que el desarrollo de

[16] Bogobowicz, M. *et al*., "Quantum Technology Monitor 2024", *McKinsey Digital*, 2024, p.88, (disponible en: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage, última consulta: 21/10/2024).
[17] Reding, D.F. y Eaton, J., "Science & Technology Trends 2020-2040: Exploring the S&T Edge", *NATO Science & Technology Organization*, 2020, p.20, (disponible en: https://www.nato.int/cps/en/natohq/news_175574.htm, última consulta 21/10/2024).
[18] Fuente: Bogobowicz, M. *et al*., "Quantum Technology…", *op. cit.*, p.88.

computadores cuánticos[19] avanzados representa para la infraestructura de seguridad digital a nivel global. Hoy día, prácticamente la totalidad de la infraestructura digital contemporánea queda en riesgo ante la eventual creación de estos dispositivos. La interconexión entre los sistemas criptográficos simétricos y asimétricos crea una vulnerabilidad generalizada frente a los ataques cuánticos, pues el empleo de esquemas híbridos lleva a que, aunque se encripten datos mediante criptografía simétrica, su seguridad se vea comprometida cuando se complementan con sistemas asimétricos para la distribución de claves. En este respecto, el NIST subraya que la necesidad de iniciar la transición hacia esquemas criptográficos resistentes a ataques cuánticos se vuelve cada vez más imperativa, pues reconoce que existen incentivos sustanciales que motivan que la inversión en computación cuántica mantenga la tendencia creciente que ha seguido hasta ahora[20]. La Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (AMETIC), principal representante de la industria digital en España, respalda estas proyecciones en el informe "Quantum Spain report: A Business Approach". El mismo destaca el potencial transformador de la computación cuántica en sectores clave de la economía y en la generación de nuevas oportunidades de negocio, lo que contribuye a fundamentar que se espere un crecimiento sostenido en el interés por su desarrollo[21].

El auge de esta tecnología enfatiza ya la urgencia de empezar a prepararse ante la era cuántica. Sin embargo, se identifica que otros son los extremos de los que provienen los riesgos más significativos que plantean los computadores cuánticos en lo que respecta a la ciberseguridad global: la lentitud inherente a las transiciones criptográficas y el riesgo de ataques comúnmente referidos como *store now, decrypt later*.

Primeramente, cabe reseñar que los expertos advierten que, sin una planificación adecuada, el reemplazo de los sistemas de clave pública actuales podría llevar décadas. La experiencia de transiciones criptográficas anteriores sugiere que el proceso desde la publicación de nuevos estándares hasta su implementación completa suele extenderse entre 5 y 15 años. En el caso

[19] En adelante, se empleará el término "computador cuántico" para referir a computadores cuánticos criptográficamente relevantes por su capacidad de procesamiento.

[20] National Institute of Standards and Technology, "*Post-Quantum Cryptography: PQC*", 2024, (disponible en: *https://www.nist.gov/pqcrypto*, última consulta 21/10/2024).

[21] *Vid.* García, A. *et al.*, "Report: Spain Quantum Industry", *Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones*, 2023, (disponible en: https://biblio.ontsi.red.es/cgi-bin/koha/opac-detail.pl?biblionumber=7476, última consulta: 21/10/2024).

específico de la adopción de estándares de criptografía post-cuántica, se prevé un período más extenso[22]. Por otra parte, con el fenómeno *store now, decrypt later* se anticipa la amenaza que los ordenadores cuánticos representarán para la seguridad de los datos almacenados a largo plazo. Esta estrategia se refiere a la posibilidad de que un atacante pueda estar recopilando datos cifrados en la actualidad para descifrarlos con posterioridad, cuando disponga de la tecnología cuántica necesaria. En este respecto, aunque los sistemas de firma digital, con períodos de validez limitados, no se verán afectados por esta amenaza concreta, todo dato encriptado en el presente con algoritmos de clave pública queda expuesto a una eventual desencriptación futura[23].

2.3. LA CRIPTOGRAFÍA POST-CUÁNTICA.

La criptografía post-cuántica surge en respuesta a la compleja coyuntura que plantea el desarrollo de la computación cuántica para la seguridad de los sistemas digitales. Según la definición del NIST, la criptografía post-cuántica es un campo que busca desarrollar algoritmos de clave pública capaces de resistir ataques tanto de computadoras convencionales como cuánticas, sin necesidad de modificar sustancialmente las infraestructuras y protocolos de comunicación existentes. Es importante señalar que, a diferencia de la criptografía cuántica, la criptografía post-cuántica se basa en técnicas matemáticas tradicionales, por lo que no requiere tecnologías cuánticas para su implementación[24].

En este contexto, la investigación en esta disciplina se ha centrado principalmente en el desarrollo de nuevos algoritmos criptográficos de clave pública. Esto se justifica porque, aunque el algoritmo de Grover podría tener cierto impacto en los algoritmos de clave simétrica,

[22] Esto se atribuye principalmente al estado incipiente de los algoritmos post-cuánticos en comparación con la introducción de nuevos algoritmos de criptografía tradicional. Véase Barker, W., *et. al.*, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms", *National Institute of Standards and Technology,* 2021, pp.2-3, (disponible en: https://doi.org/10.6028/NIST.CSWP.04282021, última consulta 21/10/2024).

[23] Gadia, J. *et al.*, "ASPI's Critical Technology Tracker: The global race for future power", *Australian Strategic Policy Institute*, n.69, 2023, p.34, (disponible en: https://www.aspi.org.au/report/critical-technology-tracker, última consulta 21/10/2024).

[24] National Institute of Standards and Technology, "What Is Post-Quantum Cryptography", 13 de agosto de 2024, (disponible en:https://www.nist.gov/cybersecurity/what-post-quantum-cryptography, última consulta 21/10/2024).

la comunidad internacional no considera que esto represente un riesgo crítico hoy día[25]. Así, la investigación se ha enfocado en replicar las aplicaciones que actualmente se le da a la criptografía de clave pública: firmas digitales, encriptación general y distribución de claves. La problemática principal en este respecto radica en que el desarrollo de algoritmos post-cuánticos enfrenta dificultades técnicas significativas. El estado actual de la investigación sugiere que no resulta factible encontrar sustitutos directos para cada algoritmo actualmente en uso, como por ejemplo, reemplazos específicos para RSA y Diffie-Hellman. Cada una de las diversas propuestas matemáticas exploradas, que incluyen algoritmos basados en retículos, códigos correctores de errores, polinomios multivariables cuadráticos, funciones hash e isogenias, presentan limitaciones particulares, lo que contribuye a obstaculizar que se sustituyan los sistemas actuales de manera completa[26].

Esto permite entender que la eventual transición hacia nuevos sistemas criptográficos enfrenta aún retos importantes. Entidades como la Agencia Nacional de Seguridad de los Sistemas de Información de Francia (ANSSI) y el BSI abogan por la implementación de soluciones híbridas en etapas iniciales de la migración criptográfica. Estas recomendaciones se deben a que se considera que los nuevos estándares no han alcanzado todavía el nivel de madurez necesario para garantizar su seguridad de forma independiente[27]. La estrategia de hibridación propuesta implica la combinación de algoritmos post-cuánticos con algoritmos de clave asimétrica tradicionales. Este enfoque busca aprovechar la seguridad probada de los sistemas actuales contra ataques de computadoras clásicas mientras se incorporan gradualmente nuevos algoritmos resistentes a ataques cuánticos[28].

A pesar de estos desafíos, el NIST ha publicado ya los primeros estándares criptográficos post-cuánticos[29]. El proceso seguido para la selección de estos estándares, que detallan tanto el

[25]National Institute of Standards and Technology, "*Post-Quantum Cryptography: PQC*", 25 de octubre de 2024, (disponible en: *https://www.nist.gov/pqcrypto*, última consulta 25/10/2024).

[26] Barker, W., *et. al.*, "Getting Ready for Post-Quantum Cryptography…", *op. cit.*, p.3.

[27] Agence nationale de la sécurité des systèmes d'information, "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)", 2023, p.2, (disponible en: https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography, última consulta 21/10/2024).

[28] *Vid.* Anexo II con una representación esquemática del funcionamiento de un enfoque híbrido que combina criptografía cuántica y post-cuántica.

[29] Véase National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards", 13 de agosto de 2024, (disponible en: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, última consulta 21/10/2024).

funcionamiento de los algoritmos seleccionados como directrices para su implementación práctica será examinado con detenimiento posteriormente, en la sección rubricada “EEUU y el concurso del NIST”.

3. PANORAMA INTERNACIONAL DE LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA.

3.1. LA ESTANDARIZACIÓN INTERNACIONAL DE LAS NUEVAS TECNOLOGÍAS.

El desarrollo de normas técnicas es un proceso que cobra especial relevancia en el actual escenario de transformación digital, donde la protección de datos contenidos en plataformas web y la integridad de las comunicaciones transfronterizas se han convertido en prioridades críticas.

La estandarización contribuye a homogeneizar y fijar unos criterios comunes para evaluar la calidad de una amplia gama de métodos, productos y servicios. Los estándares pueden abarcar ámbitos muy diversos de la gestión empresarial y técnica, dentro de los que se incluyen los algoritmos criptográficos. En el caso específico de la criptografía, la estandarización sirve como un medio objetivo para acreditar que una entidad gestiona la información que maneja de manera segura.

La estandarización dentro de este campo se desarrolla en múltiples niveles, involucrando diversas instituciones especializadas que operan en distintos ámbitos territoriales. A nivel nacional, la mayoría de países cuenta con sus propios organismos especializados como la UNE en España[30]. A escala regional, se distingue el sistema que la Unión Europea ha establecido. En este ámbito el Comité Europeo de Normalización (CEN) elabora normas EN para ser aplicadas en territorio de la Unión. Finalmente, destaca el desarrollo de estándares internacionales, los cuales son publicados por organizaciones como la Organización Internacional de Normalización (ISO, por sus siglas en inglés) o la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), para ser aplicados a nivel mundial.

[30] La Asociación Española de Normalización (UNE), es el único organismo de normalización en España. Véase Ministerio de Industria y Turismo, "Legislación básica e infraestructura para la calidad y seguridad industrial", (disponible en: https://industria.gob.es/es-es/Servicios/calidad/Paginas/legislacion-basica.aspx?Faq=Normalizaci%C3%B3n, última consulta 21/10/2024).

En España, el artículo 8 de la Ley 21/1992 de Industria proporciona una definición formal de "norma técnica", describiéndolas como especificaciones técnicas de aplicación reiterada, cuyo cumplimiento no es obligatorio[31]. Estas normas se establecen con la participación de todas las partes interesadas y son aprobadas por organismos reconocidos en el ámbito de la normalización. El sistema de estandarización internacional se distingue así por dos características fundamentales: primero, por adoptar un enfoque inclusivo y basado en el consenso que permite la participación de gobiernos, empresas, ciudadanos y expertos, representando los intereses del sector público, privado y la sociedad civil; segundo, por adoptar un enfoque discrecional en cuanto al cumplimiento de estándares, los cuales carecen de carácter jurídicamente vinculante[32]. Así, las normas técnicas forman parte de un modelo basado en la autorregulación, puesto que son las autoridades reguladoras nacionales quienes determinan la aplicación de normas técnicas internacionales en sus respectivas reglamentaciones, pudiendo estar optar por establecer que el cumplimiento de las mismas tenga carácter obligatorio o voluntario a nivel nacional[33].

Ante estas peculiaridades, la Organización Mundial del Comercio (OMC) establece una distinción importante entre normas y reglamentos técnicos. Mientras que la adhesión a las normas es opcional, los reglamentos técnicos son de obligado cumplimiento. De esta diferenciación se derivan distintas implicaciones en el comercio internacional. Un producto importado que no cumpla con un reglamento técnico no podrá comercializarse, mientras que los productos que no se ajusten a las normas que adopta el país pueden acceder al mercado, sin perjuicio de que los consumidores puedan preferir aquellos que sí las cumplen[34].

[31] Ley 21/1992, de 16 de julio, de Industria (BOE 23 de julio de 1992).

[32] Liaudat, S., "Estándares técnicos, desarrollo y geopolítica: historia, actualidad y desafíos", *Centro de Investigaciones de Política Internacional*, 2023, pp.14-15, (disponible en: https://www.cipi.cu/wp-content/uploads/2023/02/Trabajo.-Estandares-tecnicos-geopolitica-y-desarrollo.pdf, última consulta 21/10/2024).

[33] Organización Internacional de Normalización y Comisión Electrotécnica Internacional, "Uso y referencia a normas ISO e IEC en la reglamentación técnica", *Asociación Española de Normalización y Certificación*, 2007, p.7, (disponible en: https://www.une.org/normalizacion_documentos/referencia_normas_iso_iec_reg_tecnica.pdf, última consulta 21/10/2024).

[34] *Vid.* Organización Mundial del Comercio, "Acuerdo sobre Obstáculos Técnicos al Comercio", 1994, (disponible en: https://www.wto.org/spanish/docs_s/legal_s/17-tbt_s.htm, última consulta 21/10/2024).

3.2. CONTEXTO GEOPOLÍTICO.

3.2.1. La gobernanza de las tecnologías emergentes.

La gobernanza de las normas técnicas ha experimentado una evolución significativa en las últimas décadas, reflejando cambios en las dinámicas geopolíticas y tecnológicas globales. Inicialmente, esta gobernanza se había canalizado principalmente a través de organismos internacionales de estandarización como la ISO, la UIT y la IEC, lo que relegaba a los Estados a un papel secundario. Sin embargo, el creciente reconocimiento de las implicaciones geoestratégicas del desarrollo de estándares tecnológicos ha introducido una nueva tendencia en este ámbito

Desde la cumbre de Madrid, en 2022, la OTAN ha pasado a posicionar las "tecnologías emergentes y disruptivas" como una prioridad estratégica dentro de su línea de trabajo[35]. Esto indica ya que la concepción de la seguridad internacional está experimentando un cambio fundamental, lo que se refuerza ante una realidad en que gobiernos de todo el mundo reconocen de manera creciente la intersección entre tecnología y seguridad nacional[36]. Las principales potencias han comprendido que el posicionamiento geopolítico se ve hoy fuertemente influenciado por el poder tecnológico, lo cual es un proceso que va más allá de la mera inversión en investigación y desarrollo tecnológico. El informe "Critical Technology Tracker", publicado por el ASPI identifica que el liderazgo de las nuevas tecnologías abarca un conjunto muy amplio de factores, que abarcan desde la implementación de políticas pública eficaces hasta el ejercicio de una diplomacia tecnológica efectiva[37].

Esto ha llevado a que las principales potencias busquen influir de manera creciente en los foros internacionales de normalización, lo que se evidencia ante la realidad de que naciones que antes se mantenían al margen de los procesos de estandarización internacional han empezado a tomar

[35] Ricart, R.J., "Innovación en defensa y tecnologías profundas en la OTAN: cuestión de disposición y eficacia*",* *Real Instituto Elcano,* 2023, (disponible en https://www.realinstitutoelcano.org/comentarios/innovacion-en-defensa-y-tecnologias-profundas-en-la-otan-cuestion-de-disposicion-y-eficacia/, última consulta 21/10/2024).

[36] Surge un interés particular en la regulación y desarrollo de las tecnologías duales, término que hace referencia a tecnologías cuyos usos abarcan tanto en el ámbito civil, como en el ámbito de defensa. *Vid.* León, G., "*Relevancia geopolítica de las tecnologías duales…*", *op. cit.,* p.33.

[37] Gadia, J. *et al.*, "ASPI's Critical Technology Tracker…", *op. cit.,* p.9.

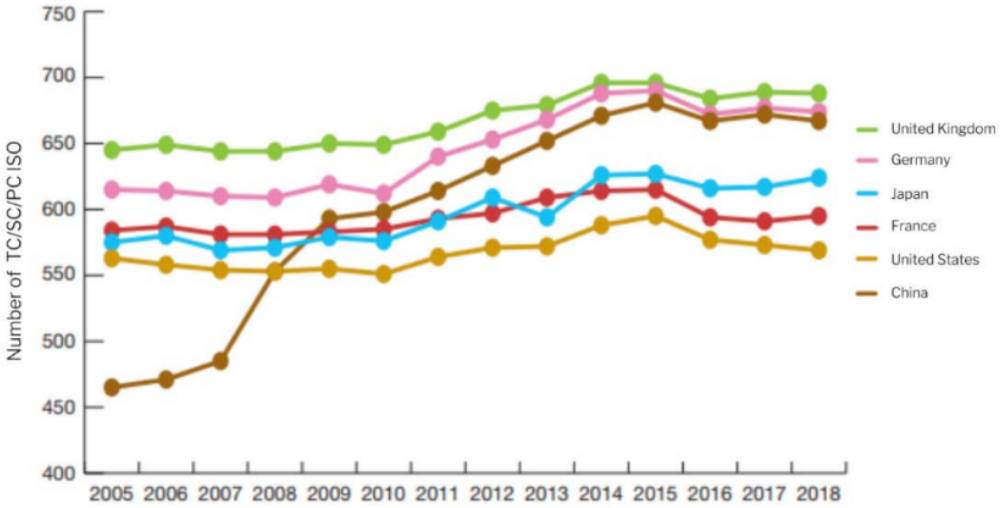
parte activa en los mismos. En este sentido, el caso de China merece un análisis detallado, ya que el país ha experimentado una transformación destacada, pasando de ser una economía predominantemente agrícola a convertirse en un líder mundial en innovación y desarrollo tecnológico. Esta evolución se atribuye en gran medida a las reformas regulatorias implementadas por el gobierno chino, que han facilitado un entorno propicio para el fomento de la innovación.

En materia de estándares y normas técnicas China ha seguido una estrategia que se ha denominado como política de "doble vía", por la cual el país complementa la adopción de normas técnicas internacionales para elevar el nivel de su producción, con el desarrollo de estándares propios para favorecer su competitividad, intentando imponer los mismos internacionalmente usando el tamaño de la economía china como plataforma[38]. Por otra parte, es preciso subrayar que el país ha articulado medidas concretas que reflejan la importancia que el gobierno Chino da al liderazgo de las normas técnicas. Entre ellas destaca el "Esquema de desarrollo de estandarización nacional" emitido por el Comité Central del Partido Comunista de China y el Consejo de Estado en Octubre de 2022, en el cual se establecen las bases para una reforma integral en la estrategia de estandarización del país. El documento señala de manera particular que las autoridades nacionales deberán priorizar de manera particular los sectores de alto valor añadido en el desarrollo de estándares técnicos, dentro de los que se engloban las tecnologías emergentes[39].

Esta postura puede verse reflejada en el patrón que la participación de China ha seguido en los foros internacionales de estandarización en las últimas décadas. El Gráfico 4 ilustra cómo la participación de China en la ISO ha aumentado de manera significativa en el periodo de 2005 a 2018.

[38] Seaman, J., "China and the New Geopolitics of Technical Standardization", *Notes de l'Ifri*, French Institute of International Relations, 2020, pp.20-27, (disponible en: https://www.ifri.org/en/papers/china-and-new-geopolitics-technical-standardization, última consulta 21/10/2024).

[39] *Vid.* Agencia de noticias Xinhua, "El Comité Central del Partido Comunista de China y el Consejo de Estado publicaron el Esquema de desarrollo de la normalización nacional", *Red del Gobierno de China,* 10 de octubre de 2021, (disponible en: https://www.gov.cn/zhengce/2021-10/10/content_5641727.htm, última consulta: 21/10/2024).



Source: reproduced from AFNOR, Baromètre International Edition 2019: Positionnement français dans la normalisation internationale

Gráfico 4. Evolución en el número de miembros participantes en los comités y subcomités técnicos de la ISO (2005-2018)[40].

Es preciso señalar que esta tendencia creciente se ha mantenido en los últimos años. En 2022, China obtuvo cinco de los nueve puestos de liderazgo técnico dentro de la ISO y la IEC y en el año 2021 destacó en la UIT-T en términos de contribuciones a comisiones de estudio, dentro de la cual presentó el 54,4% del total de las contribuciones a comisiones[41]. Estas dinámicas han contribuido a redefinir el panorama geopolítico de manera notable, llevando a una competencia internacional cuyo centro de poder ha pasado a debatirse en torno a Estados Unidos y China como principales actores estatales. Esta tensión queda claramente reflejada en la postura oficial de Estados Unidos, que en su Estrategia Internacional sobre Política Digital y Ciberespacio reseña de manera explícita que la República Popular China constituye la amenaza cibernética más significativa que las redes gubernamentales y del sector privado estadounidense enfrentan hoy día[42].

La problemática central surge en cuanto a que este panorama de creciente rivalidad pone a prueba los fundamentos del sistema de estandarización internacional, creando un escenario en

[40] Fuente: Seaman, J., "China and the New Geopolitics…", *op. cit.,* p.21.
[41] Rühling, T., "Implicaciones y riesgos del poder tecnológico de China", *Diálogo Político*, n.1, 2023, pp. 90- 91, (disponible en: https://dialogopolitico.org/edicion-especial-2024-claves-para-entender-a-china/implicaciones-y-riesgos-del-poder-tecnologico-de-china/, última consulta 21/10/2024).
[42] *Vid.* U.S. Department of State, "United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future", 2024, (disponible en: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/, última consulta 21/10/2024).

que se dificulta el mantenimiento del modelo seguido hasta el momento, sustentado sobre los principios de consenso y voluntariedad.

3.2.2. Principales actores en la competencia por el liderazgo post-cuántico.

La evolución en las dinámicas de gobernanza de las normas técnicas ha propiciado que los Estados asuman un papel cada vez más prominente en la estandarización de las tecnologías emergentes. Esta conclusión, derivada del análisis geopolítico desarrollado en la sección precedente, permite comprender la prioridad que los gobiernos otorgan a la normalización de la criptografía post-cuántica en particular.

Es crucial reconocer que en el ámbito de la estandarización de esta tecnología concreta, el escenario es especialmente complejo, siendo tres los grupos de actores que juegan un papel principal. Este marco multipolar se caracteriza por la interacción de los intereses, capacidades y estrategias distintivas de estados, organizaciones internacionales y empresas tecnológicas, lo cual plantea importantes dificultades a la hora de abordar una migración criptográfica coordinada.

La Comisión Europea, por ejemplo, ha reconocido la importancia crucial de la normalización para respaldar las prioridades de la Unión Europea en la *Estrategia Europea de Normalización* presentada en 2022[43]. Por otra parte, además de atender a las ventajas competitivas que la criptografía post-cuántica promete traer a nivel económico, potencias como Estados Unidos y China tienen especialmente en cuenta las implicaciones de seguridad nacional coadyuvadas a esta tecnología.

El rol que los actores estatales adoptan en el ámbito de la criptografía post-cuántica se define hoy por una dominancia de China en lo relativo a investigación y desarrollo, y el liderazgo de Estados Unidos en su estandarización. Un estudio comparativo del estado de desarrollo de las distintas tecnologías cuánticas a nivel internacional publicado por el ASPI en 2023, ilustra

[43] *Vid.* Comisión Europea (COM 2022), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de la UE en materia de normalización; Establecer normas mundiales para apoyar un mercado único de la Unión resiliente, ecológico y digital, (disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031, última consulta 21/10/2024).

cómo China ha venido posicionándose como la potencia a la vanguardia dentro de la carrera internacional por la investigación de la criptografía post-cuántica, siendo esta la categoría en la que se refleja un mayor margen de diferencia sobre Estados Unidos en comparación con otras tecnologías cuánticas.

Table 4: Top 5 country rankings: Quantum technologies.

Technology	Top 5 countries					Technology monopoly risk
Quantum computing	33.90%	15.03%	6.11%	5.52%	4.13%	8/10 2.26 **medium**
Post-quantum cryptography	30.98%	13.30%	6.41%	4.73%	3.69%	4/10 2.30 **low**
Quantum communications (incl. quantum key distribution)	31.47%	16.68%	7.58%	6.45%	3.81%	5/10 1.89 **low**
Quantum sensors	23.70%	23.27%	7.76%	4.29%	4.20%	2/10 1.02 **low**

Gráfico 5. Ranking de los países destacados en el desarrollo de tecnologías cuánticas[44].

Este análisis del ASPI es respaldado por datos recogidos por la consultora McKinsey, que posiciona a China como el líder mundial en inversión en tecnología cuántica. Según McKinsey, China había acumulado una financiación de más de 15 mil billones de dólares en este campo a fecha de 2023, una cifra que superaría en más de cuatro veces la inversión de Estados Unidos, situada en 3.800 millones de dólares[45].

No obstante, Estados Unidos, a través del NIST, está liderando los esfuerzos internacionales para encontrar una batería de estándares post-cuánticos lo suficientemente robustos. El Gráfico 6 muestra las principales iniciativas y posturas que distintos gobiernos han adoptado en lo referente a la criptografía post-cuántica, lo cual sirve para ilustrar el papel dominante que Estados Unidos adopta en la normalización de esta tecnología. Si bien los distintos gobiernos han desarrollado recomendaciones y planes de acción para preparar la migración criptográfica, la mayoría de países plantea implementar los algoritmos publicados como estándares por el NIST.

[44] Fuente: Gadia, J. *et al.*, "ASPI's Critical Technology Tracker…", *op. cit.*, p.29.
[45] Bogobowicz, M. *et al.*, "Quantum Technology…", *op. cit.*, p.88.

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2021)	Start planning; early implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Start planning; impl. from 2025
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022)	Start planning; Transition from 2025
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
New Zealand	NIST	NZISM (2022)	Start planning
Singapore South Korea	Monitoring NIST KpqC	MCI (2022) MSIT (2022)	No timeline available Start competition First round (Nov.'22-Nov.'23)
United Kingdom	NIST	NCSC (2020)	Start planning;
United States	NIST	NSA (2022)	Implementation 2023-2033

Gráfico 6. Principales iniciativas gubernamentales en criptografía post-cuántica[46].

Por otra parte, a pesar del papel preeminente que los Estados desempeñan en los procesos internacionales de estandarización de la criptografía post-cuántica, es importante reconocer la creciente influencia de las empresas en este campo. Grandes corporaciones tecnológicas y compañías especializadas en ciberseguridad se han convertido en actores cada vez más relevantes en el desarrollo e implementación de estándares criptográficos. Un ejemplo destacado es el papel de la multinacional estadounidense IBM, que ha co-desarrollado tres de los cuatro algoritmos que el NIST seleccionó en 2022 para su estandarización[47]. En este respecto, es preciso señalar que, más allá de su aporte técnico en la investigación y desarrollo de estándares, las empresas tecnológicas están ejerciendo una influencia considerable en la adopción práctica de los mismos en el mercado global. La "hoja de ruta de IBM Quantum Safe", presentada por la multinacional en 2023 ilustra esta tendencia. En el Gráfico 7 puede verse una ilustración esquemática de este plan de acción, de cuyo contenido puede identificarse

[46] Fuente: Global System for Mobile Communications Association, "Post Quantum Telco Network Impact Assessment: Whitepaper", 2023, pp.11-12, (disponible en: https://www.gsma.com/newsroom/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper/, última consulta: 21/10/2024).

[47] *Vid.* Anexo III con una relación de los algoritmos seleccionados. IBM, "Algoritmos desarrollados por IBM son los primeros estándares de criptografía post-cuántica del mundo", 13 de agosto de 2024, (disponible en: https://latam.newsroom.ibm.com/2024-08-13-Algoritmos-desarrollados-por-IBM-son-los-primeros-estandares-de-criptografia-post-cuantica-del-mundo, última consulta: 21/10/2024).

un marco de referencia idóneo para que distintos operadores puedan adaptar los sistemas criptográficos que gestionan de manera más sencilla, ya que presenta de manera sencilla y clara las principales iniciativas y objetivos fijados en lo relativo a la transición criptográfica.

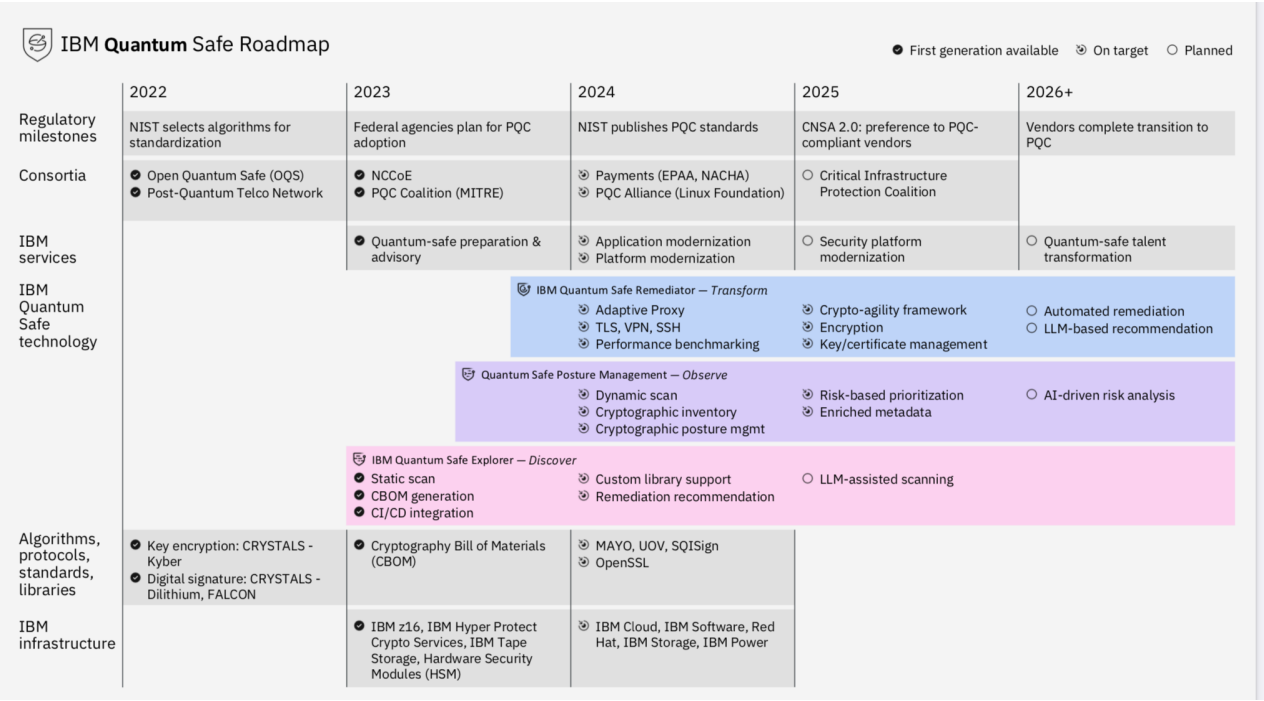


Gráfico 7. Hoja de ruta de desarrollo cuántico de IBM[48].

Finalmente, cabe también reseñar la importancia que cobran las organizaciones internacionales de normalización puesto que, proporcionando plataformas para la cooperación internacional, actúan como facilitadoras y mediadoras en el proceso de desarrollo de estándares globales de criptografía post-cuántica. Entre estos organismos destaca el trabajo de la ISO, la IEC y la UIT, el cual será examinado de manera más detallada a continuación, en la sección rubricada "El papel de las organizaciones internacionales de estandarización".

[48] IBM, "Make the world quantum safe", (disponible en: https://www.ibm.com/quantum/quantum-safe#roadmap, última consulta: 21/10/2024).

3.3. EL PAPEL DE LAS ORGANIZACIONES INTERNACIONALES DE ESTANDARIZACIÓN.

3.3.1. Normas ISO-IEC.

La ISO y la IEC son organismos internacionales de normalización que reúnen a organismos nacionales de todo el mundo para desarrollar y publicar normas técnicas internacionales. En el seno de estas organizaciones, sus países miembros participan en la creación de estándares internacionales, articulando su participación a través de comités técnicos específicos.

La ISO, con sus 172 miembros[49], cuya distribución geográfica puede verse ilustrada en el Gráfico 8, se caracteriza por adoptar una estructura de representación única. Cada país es representado por un solo organismo, generalmente el más destacado en normalización a nivel nacional. Este modelo ha sido fundamental para que, a diferencia de otras instituciones internacionales surgidas en la posguerra, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), donde la influencia estadounidense era más notoria, la ISO se haya distinguido por mantener un equilibrio ejemplar en su gobernanza. En concreto, se señala que el sistema de toma de decisiones que el organismo adopta ha proporcionado a Europa una posición estratégica frente al potencial dominio de Estados Unidos, sirviendo la representación de múltiples países europeos para actuar como contrapeso. Esto se complementa con la observación de que, desde su fundación, la ISO se haya caracterizado por adoptar un enfoque inclusivo, en cuanto a que ha integrado a países con sistemas políticos y económicos diversos, incluidos estados comunistas durante la Guerra Fría[50].

[49]Los miembros de la ISO se clasifican en tres categorías, cada una con diferentes niveles de participación e influencia en el proceso de desarrollo de estándares. Los miembros de pleno derecho son aquellos que cuentan con organismos nacionales de normalización consolidados, participan activamente en las reuniones de la ISO y tienen pleno derecho de voto en las mismas. Por otro lado, los miembros correspondientes generalmente representan a países en vías de desarrollo que no cuentan con un sistema de normalización nacional plenamente consolidado. Estos participan en las reuniones de la ISO pero no tienen derecho de voto. Finalmente, los miembros suscritos son aquellos que desean mantenerse al corriente del trabajo de la ISO pero no participan en ella ni adoptan sus normas a nivel nacional. *Vid.* Organización Internacional de Normalización, "Miembros", (disponible en: https://www.iso.org/es/sobre/miembros, última consulta 21/10/2024).

[50] Liaudat, S., "Estándares técnicos…", *op. cit.*, pp.13-14.

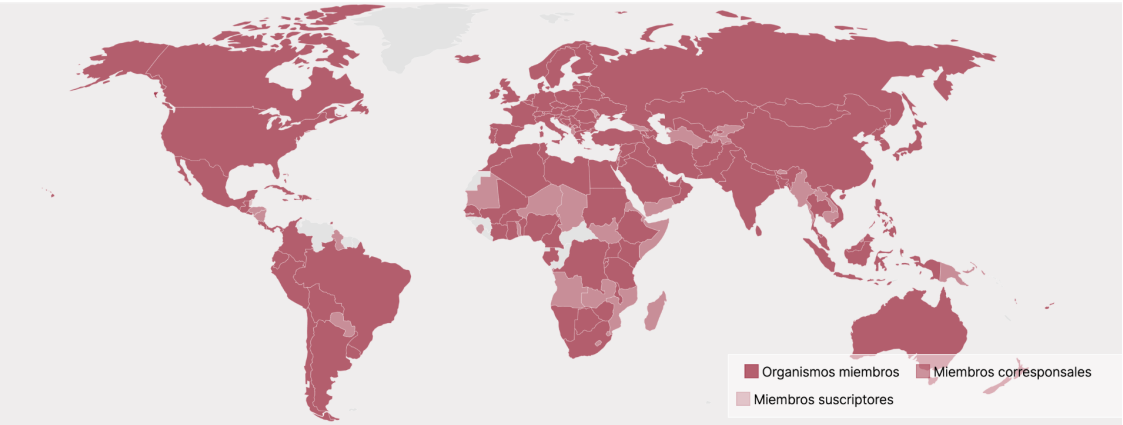


Gráfico 8. Distribución geográfica de países miembros de la ISO[51].

Por su parte, la IEC cuenta actualmente con 89 comités nacionales, incluyendo miembros de pleno derecho y asociados[52]. Tanto la IEC como la ISO convocan a un grupo diverso de expertos para el desarrollo de estándares, incluyendo representantes de la industria, gobierno, consumidores, asociaciones comerciales y académicos. Las normas que las mismas publican se mantienen actualizadas mediante revisiones quinquenales, asegurando su adecuación a los avances tecnológicos y las necesidades cambiantes del mercado global. Ambas organizaciones adoptan un modelo similar y han forjado una colaboración estratégica que ha resultado en el desarrollo de una serie de estándares cruciales en el campo de la seguridad de la información.

En lo relativo a la criptografía post-cuántica ambas organizaciones han reconocido la importancia de acordar unos estándares sólidos en un futuro próximo. Aunque aún no han publicado estándares propios que contribuyan a la normalización de esta tecnología, han iniciado esfuerzos significativos para contribuir a la investigación global. Estos se materializan a través de esfuerzos del comité conjunto ISO/IEC JTC 1/SC 27, cuya labor incluye la evaluación de algoritmos candidatos al concurso del NIST, la definición de requisitos de seguridad y la consideración de aspectos de implementación práctica.

Por otro lado, la serie ISO/IEC 27000, que regula la implementación y gestión de Sistemas de Gestión de Seguridad de la Información (SGSI) cobra relevancia en su aplicación al desarrollo de nuevas soluciones criptográficas. Recientemente, dos normas de esta serie han sido

[51] Fuente: Organización Internacional de Normalización, "Miembros", *op. cit.*
[52] Comisión Electrotécnica Internacional, "National Committees", (disponible en: https://www.iec.ch/national-committees, última consulta: 21/10/2024).

revisadas, de las cuales puede anticiparse una posible compatibilidad con nuevos estándares específicos de criptografía post-cuántica. La revisión de 2022 de la norma ISO/IEC 27001 introdujo nuevos controles para abordar los riesgos distintivos de tecnologías emergentes[53], mientras que, reflejando un compromiso por mantener los estándares al día con la evolución tecnológica, la actualización de la ISO/IEC 27032, centrada en ciberseguridad, destacó los peligros que plantean las nuevas tendencias en Inteligencia Artificial y el Internet de las Cosas[54].

3.3.2. Naciones Unidas y la UIT-T.

La UIT es el organismo especializado de las Naciones Unidas en el sector de las telecomunicaciones. Fundada en 1865, se distingue por ser la organización intergubernamental más antigua del mundo, habiendo evolucionado desde sus orígenes en la era del telégrafo hasta convertirse en una de las principales instituciones para la normalización tecnológica en la era digital.

En la actualidad, la UIT cuenta con 193 Estados miembros y reúne a más de 700 entidades del sector privado e instituciones académicas. Esta composición heterogénea contribuye a que, a pesar de su carácter intergubernamental, la UIT haya adoptado un enfoque metodológico similar al de organizaciones como la ISO y la IEC, basado en el consenso y la inclusividad[55].

Dentro de la UIT[56], el Sector de Normalización de las Telecomunicaciones (UIT-T) es el órgano responsable de desarrollar los estándares internacionales, conocidos como "Recomendaciones UIT-T", que definen los principales elementos en las redes y servicios de Tecnologías de la Información y la Comunicación (TIC). El trabajo de normalización de la

[53] UNE, "Publicadas las nuevas normas UNE-ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para impulsar la ciberseguridad y digitalización", 17 de mayo de 2023, (disponible en: https://www.une.org/la-asociacion/sala-de-informacion-une/notas-de-prensa/nuevas-normas-une-isoiec-27001-y-27002-ciberseguridad-digitalizacion, última consulta 20/10/2024).

[54] Hernández, S. "Fortalece estrategias y Políticas de Ciberseguridad: ISO 27032:2023", *Global Suite Solutions*, 2024, (disponible en: https://www.globalsuitesolutions.com/es/estrategias-politicas-de-ciberseguridad-iso-iec-27032-2023/, última consulta 20/10/2024).

[55] Unión Internacional de Telecomunicaciones, "Elaboración de normas", (disponible en: https://www.itu.int/es/ITU-T/about/Pages/development.aspx, última consulta 20/10/2024).

[56] La UIT se compone de tres grandes divisiones: Sector de Normalización (UIT-T), Sector de Radiocomunicaciones (UITR) y Sector de Desarrollo (UIT-D).

UIT-T se organiza en series, cada una identificada por una letra que representa un área específica de las telecomunicaciones y las tecnologías de la información. En el ámbito de la criptografía post-cuántica, la Serie X resulta particularmente relevante, ya que aborda temas de redes de datos, comunicación entre sistemas abiertos y seguridad. Aunque el UIT-T aún no ha publicado un estándar específico de criptografía post-cuántica, la Comisión de Estudio 17 (CE17) está trabajando en el desarrollo de soluciones de seguridad frente a las tecnologías cuánticas emergentes[57].

Sin embargo, es importante notar que los esfuerzos de la UIT-T, a través de este grupo de trabajo, se han centrado más en el análisis de soluciones de criptografía cuántica que en el estudio de nuevos algoritmos post-cuánticos. Esta orientación se evidencia en trabajos como el informe "Consideraciones de seguridad para redes de distribución de claves cuánticas", que examina las vulnerabilidades potenciales de los sistemas criptográficos actuales frente a la computación cuántica, pero se centra principalmente en el desarrollo de redes de distribución de claves cuánticas (QKD, por sus siglas en inglés)[58].

Mientras que esta situación refleja que la investigación dentro del seno de Naciones Unidas no ha priorizado el estudio concreto de las tecnología post-cuántica, cabe destacar que la organización ha establecido pautas generales relevantes para la gobernanza de tecnologías digitales, destacando el modelo acordado en el Pacto Digital Mundial. Este esfuerzo intergubernamental, adoptado en la Cumbre del Futuro de septiembre de 2024, enfatiza la importancia del enfoque multilateral en el desarrollo tecnológico digital y propone un marco basado en la inclusión digital y el respeto a los derechos humanos.[59]

Este enfoque cobra especial relevancia en lo referente a la criptografía post-cuántica, donde las tensiones geopolíticas dificultan los procesos de estandarización y una subsiguiente implementación efectiva. Las directrices proporcionadas por las Naciones Unidas pueden

[57] *Vid.* Unión Internacional de Telecomunicaciones, "Security for/by emerging technologies including quantum-based security", (disponible en: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Q15.aspx, última consulta 20/10/2024).
[58] *Vid.* Sector de Normalización de la Unión Internacional de Telecomunicaciones, "Consideraciones de seguridad para redes de distribución de claves cuánticas", 2020, (disponible en: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf, última consulta: 21/10/2024).
[59] *Vid.* Naciones Unidas, *Global Digital Compact*, *op. cit.*

ofrecer una orientación valiosa para afrontar estos retos, fomentando una aproximación más colaborativa y equitativa al desarrollo e implementación de tecnologías emergentes.

3.4. LOS ACTORES ESTATALES Y SU PAPEL EN LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA.

Esta sección se centra en analizar las iniciativas específicas que Estados Unidos, China y la Unión Europea han puesto en marcha en el campo de la criptografía post-cuántica. A través de un análisis comparativo, se busca identificar las mejores prácticas globales que permitan abordar las oportunidades y retos que surgen en el contexto geopolítico y tecnológico actual.

3.4.1. EEUU y el NIST.

En Estados Unidos, el NIST, una agencia dependiente del Departamento de Comercio, es la encargada de desarrollar estándares para proteger la información sensible del gobierno. El trabajo del NIST es particularmente relevante a nivel mundial, destacando el hecho de que los estándares criptográficos que la agencia ha desarrollado son ampliamente reconocidos y utilizados internacionalmente para garantizar la seguridad de sistemas y productos.[60]

En 2016, el NIST lanzó el Programa de Estandarización de Criptografía Post-Cuántica, un concurso público centrado en dos categorías: cifrado e intercambio de claves, y firmas digitales; con el fin de identificar diversos algoritmos criptográficos que probaran ser resistentes a ataques cuánticos. Los principales objetivos del NIST en este proceso han sido garantizar la seguridad a largo plazo de los sistemas criptográficos, fomentar la colaboración internacional y promover el consenso en la selección de estándares. Para ello, el NIST ha lanzado convocatorias públicas para recibir propuestas de algoritmos, realizado análisis exhaustivos de cada candidato y seleccionado diversos algoritmos finalistas.

Hasta ahora, el proceso se ha desarrollado en tres rondas. En la primera ronda, que se extendió hasta 2017, se recibieron 82 propuestas de algoritmos candidatos, abarcando diversos enfoques

[60] El AES o el SHA son algunos de los estándares más destacados publicados por el NIST.

matemáticos que incluían retículos, códigos correctores de errores, y esquemas multivariables. En la segunda ronda, entre 2018 y 2019, se evaluaron 64 de las 82 propuestas iniciales, de las cuales 26 resultaron seleccionadas para la tercera y última fase. La fase final, desarrollada entre 2019 y 2022, concluyó con el anuncio el 5 de julio de 2023 de la selección de cuatro algoritmos para su estandarización.

Tres de estos algoritmos ya han sido publicados como estándares oficiales: ML-KEM (antes CRYSTALS-Kyber) y ML-DSA (antes CRYSTALS-Dilithium)[61], seleccionados como mecanismos principales para encapsulación de claves y firmas digitales respectivamente, y SLH-DSA (antes SPHINCS+) como algoritmo alternativo a ML-DSA. Un cuarto algoritmo, Falcon (que será denominado FN-DSA), está pendiente de publicación[62].

Ahora bien, el proceso de estandarización del NIST continúa abierto, pues se contempla la posibilidad de incluir nuevas propuestas en el futuro. Otros cuatro algoritmos (BIKE, HQC y Classic McEliece) siguen en consideración para ser analizados en una cuarta ronda. Asimismo, paralelamente al proceso de estandarización de 2016, el NIST lanzó en 2023 un proceso adicional centrado en la categoría de firmas digitales, buscando una mayor variedad de algoritmos para hacer frente a la amenaza que la computación cuántica presenta en este ámbito concreto.

En cuanto a la transición criptográfica, el gobierno federal de Estados Unidos ha enfatizado la importancia de la transición criptográfica y ha implementado medidas proactivas para facilitar este proceso. En septiembre de 2022, la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) publicó el *Commercial National Security Algorithm Suite 2.0* (CNSA 2.0.)[63], un documento que detalla los algoritmos criptográficos a utilizar en los Sistemas de Seguridad Nacional de Estados Unidos[64]. El CNSA 2.0., junto con su documento complementario *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ* establece un cronograma definido para la transición criptográfica. El objetivo es que todos los sistemas de

[61] Estos algoritmos fueron co-desarrollados por IBM, tal como se reseña en la sección 3.1.2. "principales actores en la competencia por el liderazgo post-cuántico".
[62] *Vid.* apéndice III con una representación sintetizada de los resultados del concurso del NIST.
[63] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", 2022, (disponible en: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF, última consulta 20/10/2024).
[64] *Vid.* Apéndice IV con la Suite de Algoritmos de Seguridad Nacional Comercial 2.0 propuesta por la NSA.

seguridad nacional completen la migración a algoritmos resistentes a la computación cuántica para el año 2035[65]. Además, reconociendo los desafíos inherentes a una transición de esta magnitud, la NSA recomienda la adopción inicial de soluciones híbridas en la industria, que permitan minimizar disrupciones en los sistemas existentes mientras se introducen soluciones resistentes contra futuras amenazas cuánticas[66].

Por otra parte, en mayo de 2022 el gobierno de Biden emitió el *Memorando de Seguridad Nacional 10* (NSM-10)[67], instando a las agencias gubernamentales a prepararse para la transición. Esto se complementó en diciembre de 2022 con la "Ley de Preparación para la Ciberseguridad Cuántica", que establece obligaciones más concretas para las agencias gubernamentales. Esta ley requiere que la Oficina de Gestión y Presupuesto desarrolle directrices para la migración a soluciones de criptografía post-cuántica en las agencias gubernamentales, y que éstas remitan al gobierno central un inventario de aquellos sistemas criptográficos que manejen y se identifiquen como vulnerables a la computación cuántica[68].

Finalmente, en marzo de 2023 el gobierno estadounidense publicó la "Estrategia de Ciberseguridad Nacional", que destaca como objetivo estratégico la "preparación para nuestro futuro post-cuántico"[69]. Este documento insta a priorizar la inversión en la sustitución de la infraestructura digital para adaptarla a nuevos algoritmos post-cuánticos, subrayando la importancia que el gobierno estadounidense otorga a la transición criptográfica.

3.3.2. China y su política de doble vía.

[65] *Vid.* National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ", 2024, p.10, (disponible en: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF, última consulta 20/10/2024).
[66] *Vid., Ibid,* pp.17-19.
[67] *Vid.* La Casa Blanca, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 2022, (disponible en: https://www.whitehouse.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/, última consulta 20/10/2024).
[68] Congreso de los Estados Unidos, Quantum Computing Cybersecurity Preparedness Act, 2022, (disponible en: https://www.congress.gov/bill/117th-congress/house-bill/7535, última consulta 20/10/2024).
[69] *Vid.* objetivo 4.3. de la Estrategia de Ciberseguridad Nacional; La Casa Blanca, National Cybersecurity Strategy, 2023, (disponible en: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, última consulta: 21/10/2024).

En el campo de la criptografía post-cuántica, China ha adoptado una estrategia enfocada en el desarrollo de estándares nacionales propios, como parte de su esfuerzo por contrarrestar el liderazgo estadounidense en la normalización de esta tecnología.

En 2018, la Asociación China para la Investigación Criptológica (CACR, por sus siglas en inglés) lanzó su propio concurso de estandarización de la criptografía post-cuántica. El concurso se centró en identificar algoritmos para las categorías de intercambio de claves, firma digital y cifrado de clave pública, recibiendo 36 propuestas. Como resultado, el CACR anunció sus ganadores en enero de 2020, publicando ese mismo año sus recomendaciones sobre algoritmos post-cuánticos.

A diferencia del concurso del NIST en Estados Unidos, la competición china se desarrolló en una sola ronda y la participación en la misma quedó restringida a equipos que incluyeran al menos un miembro chino. Esto permite entender que la difusión internacional de las recomendaciones de la CACR haya sido muy limitada, lo que se justifica vista la naturaleza restrictiva del concurso en cuanto a la participación y el hecho de que la documentación está disponible únicamente en mandarín[70].

3.3.3. La Unión Europea

Mientras que la Unión Europea no ha iniciado una iniciativa propia para desarrollar estándares de criptografía post-cuántica, está desempeñando un papel crucial en la coordinación de esfuerzos regionales y nacionales.

En el ámbito de la ciberseguridad con miras a la era cuántica, la investigación de la Unión Europea se ha centrado principalmente en el desarrollo de soluciones de criptografía cuántica, a través de proyectos como el *EuroQCI*[71] o el *OpenQKD*[72]. Sin embargo, la Comisión ha

[70] Global System for Mobile Communications Association, "Post Quantum Telco…", *op. cit.*, p.14.

[71] Con el proyecto EuroQCI la Comisión Europea busca crear una infraestructura de comunicación cuántica segura que abarque todo el territorio de la Unión Europea. Comisión Europea, "European Quantum Communication Infrastructure (EuroQCI) Initiative", 2023, (disponible en: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci, última consulta: 21/10/2024).

[72] El proyecto OpenQKD se llevó a cabo en el marco del Programa Horizonte 2020 de la Unión Europea. Concluido el 1 de marzo de 2023, esta iniciativa reunió a un diverso grupo de partes interesadas, incluyendo

reconocido también la importancia de la criptografía post-cuántica en el panorama tecnológico y geopolítico actual. La Recomendación de la Comisión Europea del 11 de abril de 2024, "sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía post-cuántica", subraya la necesidad de adoptar un enfoque coordinado para la transición de Europa hacia una infraestructura digital resistente a amenazas cuánticas[73].

Siguiendo la lógica aquí expuesta, dos entidades europeas han realizado contribuciones particularmente significativas en la investigación de criptografía post-cuántica: el ETSI, a través de su grupo de trabajo *TC Cyber Working Group for Quantum-Safe Cryptography*, y la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés).

El ETSI se ha enfocado en desarrollar esfuerzos de estandarización orientados al mercado, monitoreando y evaluando la implementación de los nuevos algoritmos y protocolos propuestos en el concurso del NIST[74]. Así, sus informes técnicos han contribuido significativamente a los esfuerzos internacionales de estandarización. Un ejemplo notable es el "*ETSI TR 103 823"*, publicado en 2021. En este documento se proporciona una descripción técnica de los algoritmos presentados en la tercera ronda del concurso del NIST, contribuyendo así a su evaluación[75].

Asimismo, ENISA ha desempeñado un papel destacado en el análisis del proceso de estandarización de la criptografía post-cuántica a nivel internacional. En 2022, la agencia publicó un informe titulado *"Post-Quantum Cryptography: Integration Study"*, que ofrece una

expertos en telecomunicaciones, investigadores científicos y usuarios finales, entre otros, con el objetivo de impulsar el desarrollo de una infraestructura de comunicación cuántica segura en el ámbito de la Unión Europea. Comisión Europea, "OPENQKD - Open European Quantum Key Distribution Testbed", *CORDIS EU Research Results*, 2023, (disponible en:10.3030/857156, última consulta: 21/10/2024).

[73] 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. (DOUE 12 de abril de 2024).

[74] *Vid.* Instituto Europeo de Normas de Telecomunicaciones, "TECHNICAL COMMITTEE (TC) CYBER (CYBERSECURITY)", (disponible en: https://www.etsi.org/committee/1393-cyber, última consulta: 21/10/2024).

[75] Instituto Europeo de Normas de Telecomunicaciones, "CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation", 2021, (disponible en: https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.01_60/tr_103823v010101p.pdf, última consulta: 21/10/2024).

visión general de las categorías de algoritmos de criptografía post-cuántica propuestas hasta la fecha, los procesos de selección de estándares y las consideraciones de implementación[76].

Ahora bien, a diferencia de algunas agencias nacionales de ciberseguridad como el ANSSI en Francia, que han desarrollado cronogramas específicos para la transición criptográfica, la Unión Europea no ha fijado una programación coordinada y específica a nivel regional. Esto refleja y anticipa las complejidades de establecer un enfoque común ya solo en el ámbito comunitario de la Unión.

Las recomendaciones técnicas de agencias nacionales como la ANSSI y la BSI muestran similitudes en su enfoque. Ambas agencias abogan por la hibridación para facilitar la migración criptográfica y consideran la posibilidad de adoptar algoritmos adicionales a los estándares publicados por el NIST, como FrodoKEM, postulando el mismo solución alternativa a los algoritmos seleccionados[77]. Sin embargo, cabe notar que la ANSSI adopta un enfoque de precaución adicional con respecto a la postura del NIST y la BSI. La agencia pone un especial énfasis en la necesidad de redimensionar el tamaño de las claves utilizadas en algoritmos simétricos, como AES, anticipando también la potencial vulnerabilidad de estos sistemas a algoritmos cuánticos[78].

4. PRINCIPALES DESAFÍOS RELACIONADOS CON LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA.

4.1. DESAFÍOS GEOPOLÍTICOS Y LA INTEROPERABILIDAD DE SISTEMAS.

[76] *Vid.* Bernstein, D.J., Hülsing, A. y Lange, T., "Post-Quantum Cryptography: Integration study", *European Union Agency for Cybersecurity*, 2022, (disponible en: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study, última consulta: 21/10/2024).

[77] *Vid.* Agence nationale de la sécurité des systèmes d'information, "ANSSI views on the Post-Quantum…", *op. cit.*, p.3; y Federal Office for Information Security, "Cryptographic Mechanisms: Recommendations and Key Lengths", 2024, p.35, (disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile, última consulta 21/10/2024).

[78] Agence nationale de la sécurité des systèmes d'information, "ANSSI views on the Post-Quantum…", *op. cit.*, p.2.

Los estándares tecnológicos siempre han tenido una dimensión de influencia política internacional, dada su estrecha vinculación con cuestiones de seguridad nacional, como la protección de infraestructuras críticas de gobierno, entre otras[79]. En lo referente a la criptografía post-cuántica, esta dimensión geopolítica se intensifica, presentando retos significativos para el desarrollo de estándares efectivos y globalmente aceptados, lo que complica los esfuerzos de normalización tanto a nivel nacional como internacional.

Como se ha visto, las implicaciones de la criptografía post-cuántica en el ámbito de la seguridad nacional introduce desafíos adicionales. Esta tecnología se posiciona actualmente como la solución más prometedora para mitigar la amenaza cuántica, lo que genera una tensión internacional particularmente intensa debido al potencial uso que algunos países podrían hacer de ella. El Gráfico 9, que muestra una representación gráfica de las potencias preeminentes en términos de patentes en computación cuántica, sirve para ilustrar en parte la justificación de estas tensiones. Si bien Estados Unidos se posiciona como país líder en este ámbito, China destaca también como una de las potencias más activas. Esta situación ha llevado a instituciones como el ASPI a advertir sobre la posible aplicación militar que el gobierno chino podría dar a estas tecnologías, potencialmente aplicándolas para ocultar sus comunicaciones, consecuentemente reduciendo la capacidad de otros países para desarrollar planes de contingencia ante hostilidades[80].

[79] Feijóo, C., "El consenso internacional sobre los estándares", *el Alcázar de las Ideas*, 2022, (disponible en: https://www.elalcazardelasideas.es/el-consenso-internacional-sobre-los-estandares/#_ednref21 última consulta 21/10/2024).
[80] *Vid.* Gadia, J. *et al.*, "ASPI's Critical Technology Tracker…", *op. cit.*, p. 18.

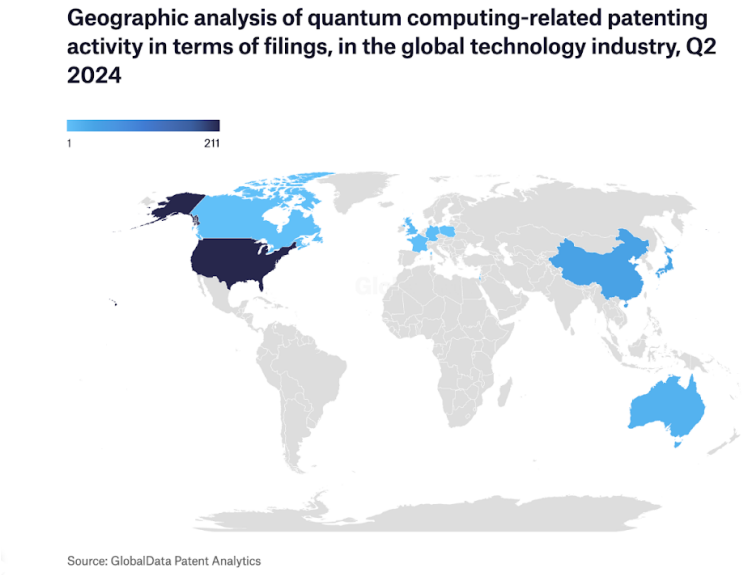


Gráfico 9. Análisis geográfico de los países más activos en la presentación de patentes de computación cuántica en el segundo cuatrimestre de 2024.[81]

En este respecto, la intersección entre ventajas competitivas a nivel comercial y consideraciones de seguridad nacional ha generado una intensa competencia internacional por el liderazgo en la normalización de algoritmos criptográficos post-cuánticos. Este escenario obstaculiza la interoperabilidad y la armonización de estándares, dentro de lo que pueden identificarse dos obstáculos principales que dificultan el proceso de estandarización.

En primer lugar, los esfuerzos de diversos actores estatales tienden a entrar en conflicto con los procesos internacionales de estandarización. Como se ha analizado en la sección "Los actores estatales y su papel en la estandarización de la criptografía post-cuántica", la creciente politización de los estándares y los intereses nacionales divergentes, especialmente entre potencias como Estados Unidos y China, han llevado a que estos países busquen promover sus propios procesos o intenten influir en la definición de estándares globales según sus prioridades estratégicas.

En segundo lugar, el papel de los derechos de propiedad intelectual añade una capa adicional de complejidad a la competencia que rodea los procesos internacionales de estandarización. La

[81] Fuente: Global Data's Patent Analytics, "Q2 2024 update: quantum computing related patent activity in the technology industry", *Verdict*, 2024, (disponible en: https://www.verdict.co.uk/patent-activity-quantumcomputing-technology-industry/?cf-view&cf-closed, última consulta 21/10/2024).

mera existencia de un estándar no garantiza automáticamente su disponibilidad pública o su adopción universal. Las empresas que han desarrollado tecnologías relevantes deben estar dispuestas a compartir su conocimiento y, en muchos casos, su propiedad intelectual[82]. Así, la implementación de muchos estándares está sujeta a licencias, lo que anticipa nuevos obstáculos en la estandarización de las nuevas tecnologías, pues el campo de la innovación tecnológica tiende a estar protegido mediante derechos de explotación exclusiva, por las implicaciones estratégicas que lo rodean. Los pioneros en el desarrollo de tecnologías emergentes tienden a asegurar sus innovaciones mediante un robusto sistema de patentes, lo que no solo protege sus avances tecnológicos, sino que también les otorga una posición privilegiada para explotar los beneficios económicos del mercado. Shapiro ilustra las implicaciones que derivan de esta táctica con el concepto de "*patent hold-up"*, explicando cómo la misma resulta en una desventaja competitiva a largo plazo para el resto de potencias, que se verán obligadas a asumir los costos de adaptación a los estándares dominantes[83].

4.2. DESAFÍOS TÉCNICOS Y LA *CRIPTOAGILIDAD* EN LOS SISTEMAS DE INFORMACIÓN.

La estandarización de la criptografía post-cuántica no solo enfrenta desafíos geopolíticos, sino también retos técnicos significativos que abarcan desde el desarrollo de algoritmos robustos hasta su implementación adecuada.

Se han identificado varias áreas matemáticas prometedoras para el desarrollo de nuevos algoritmos, como la criptografía basada en retículos, en códigos correctores de errores o en polinomios multivariables cuadráticos. Sin embargo, cada una de estas categorías enfrenta desafíos significativos cuando se compara con los paradigmas criptográficos tradicionales, como la necesidad de manejar claves y firmas de gran longitud[84]. Además, idealmente, se buscaría encontrar reemplazos directos para cada clase de algoritmos de clave pública

[82] Los organismos de estandarización negocian con las compañías privadas para que éstas pongan sus patentes a disposición de terceros en condiciones que no dificulten la implementación del estándar, pero no obligan a que su uso sea gratuito. Feijóo, C., "El consenso internacional…", *op. cit.*

[83] Shapiro, C. "Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting,", *Innovation Policy and the Economy*, vol. 1, 2001, pp.124-126, (disponible en: https://doi.org/10.1086/ipe.1.25056143, última consulta: 21/10/2024).

[84] Instituto Europeo de Normas de Telecomunicaciones, "CYBER; Quantum-Safe…", *op. cit.*

actualmente en uso. No obstante, la realidad es más compleja, ya que cada categoría de algoritmos post-cuánticos presenta al menos un requisito de implementación segura que impide la transición directa desde los sistemas criptográficos actuales. Esta situación ha llevado a que la investigación en criptografía post-cuántica se haya orientado hacia el desarrollo de una gama diversa de algoritmos capaces de adaptarse a las necesidades específicas de diferentes operadores y sistemas, en lugar de buscar una solución única y universal. Este enfoque, si bien resulta pertinente, complica el proceso de estandarización, prolongando la necesidad de investigación continua en este campo. De ello deriva que mantener los estándares actualizados y relevantes a medida que la tecnología avanza se presente como un desafío adicional a la convergencia regulatoria, pues implica la necesidad de mantener una revisión constante tanto de estándares como de marcos legislativos.

Por otra parte, la implementación práctica de los estándares de criptografía post-cuántica presenta complejidades particulares. Es probable que los protocolos en uso necesiten modificaciones para manejar firmas o tamaños de clave más grandes, lo que podría implicar, por ejemplo, la implementación de técnicas de segmentación de mensajes. Como ya se ha reseñado, el NIST anticipa que este proceso de transición será más complejo que la introducción de nuevos estándares de criptografía tradicional[85].

Esto se alinea con las observaciones del ASPI, que subraya que la rigidez de los protocolos digitales existentes dificulta la adaptación de la infraestructura actual a los nuevos estándares post-cuánticos[86], lo que se atribuye en gran parte a la falta de "cripto-agilidad" en los sistemas de seguridad actuales. Este concepto, definido por el CCN, se refiere a la capacidad de los sistemas para adaptarse a nuevos estándares criptográficos sin necesitar cambios sustanciales en la infraestructura existente[87]. Esta observación queda respaldada por el informe "Hype Cycle" de Gartner de 2023, que revela que la mayoría de las organizaciones carecen de un conocimiento profundo sobre los sistemas criptográficos que utilizan, lo que dificulta su sustitución[88]. Así, la combinación de estos factores, falta de cripto-agilidad y limitado

[85] Barker, W. *et. al*, "Getting Ready for Post-Quantum Cryptography…", *op. cit.,* pp.2-3.
[86] Gadia, J. *et al.*, "ASPI's Critical Technology Tracker…", *op. cit.,* p.18.
[87] Centro Criptológico Nacional, "Recomendaciones para una…", *op. cit.,* p.13.
[88] Es preciso reseñar que el panorama digital que manejan las organizaciones se ha vuelto cada vez más complejo. Ahora las compañías tienden a manejar aplicaciones digitales desarrolladas internamente en conjunción con softwares o servicios gestionados y provistos por terceros. *Vid.* Horvath, M. *et al*., "Postquantum Cryptography: The Time to Prepare Is Now!*", Gartner,* 1 de julio de 2024, (disponible en: https://www.gartner.com/en/documents/5550295, última consulta 21/10/2024).

conocimiento organizacional, crea un escenario particularmente desafiante para la implementación generalizada de la criptografía post-cuántica.

4.3. DESAFÍOS ÉTICOS Y REGULATORIOS.

La creciente inestabilidad geopolítica y la ausencia de marcos regulatorios claros genera un entorno complejo en el que las empresas tecnológicas compiten por posicionarse favorablemente en un mercado en que la criptografía post-cuántica promete tener un efecto revolucionario. Esta tecnología cobra especial relevancia en un contexto donde, como señala la UNE, el uso generalizado de tecnologías de la información no solo ofrece ventajas a nivel comercial, sino que también resulta esencial para garantizar la protección de información empresarial y la privacidad de los usuarios[89]. Sin embargo, la implementación eficaz de estándares post-cuánticos enfrenta también desafíos considerables en términos de inclusividad y representación, desafíos que se manifiestan de manera diversa.

En primer lugar, la transición hacia la criptografía post-cuántica requerirá inversiones sustanciales por parte de las empresas para actualizar sus sistemas de seguridad. Esto podría afectar de manera desproporcionada la competitividad de aquellas organizaciones con recursos limitados, especialmente a Pequeñas y Medianas Empresas (PYMES) y a empresas que operan en economías emergentes. Como advierte la OMC, los costos asociados y la naturaleza altamente técnica de tecnologías avanzadas pueden conducir a una adopción desigual entre países, creando nuevas barreras técnicas al comercio internacional y exacerbando las desigualdades existentes en el comercio internacional[90]. Así, la adopción desigual de tecnologías post-cuánticas podría ampliar la brecha tecnológica entre países desarrollados y en desarrollo, lo que podría asimismo resultar en nuevas formas de dependencia tecnológica.

Por otra parte, la competencia global por el talento en criptografía post-cuántica es una cuestión adicional a considerar. Países y empresas compiten intensamente por atraer y retener a los mejores investigadores. Esto genera nuevos patrones de migración de talento, lo que se

[89] Asociación Española de Normalización, "Conocimiento para afrontar los desafíos de las organizaciones", *La revista de la normalización española*, n.7, 2018, (disponible en: https://revista.une.org/7/conocimiento-para-afrontar-los-desafios-de-las-organizacione.html, última consulta 20/10/2024).
[90] Organización Mundial del Comercio, "Acuerdo sobre Obstáculos…", *op. cit.*

identifica como un factor añadido con el potencial de exacerbar las desigualdades existentes en la distribución global del conocimiento tecnológico. El Gráfico 10 ilustra las principales dinámicas que ha seguido el flujo de talento global en criptografía post-cuántica, conforme al análisis publicado por el ASPI en el informe "Critical Technology Tracker". Este destaca cómo la investigación en tecnologías post-cuánticas influye de manera significativa en el flujo de talento global, mostrando que el conocimiento especializado en esta tecnología se concentra principalmente en la Unión Europea y en China, siendo estas las regiones con mayor capacidad para atraer y retener talento en este ámbito concreto. Esta concentración plantea preocupaciones sobre el acceso global a tecnologías post-cuánticas, subrayando la necesidad de estrategias internacionales coordinadas para procurar una distribución más equitativa de los beneficios de las mismas.

Figure 11: Flow of global talent in post-quantum cryptography (top 25% of research papers).

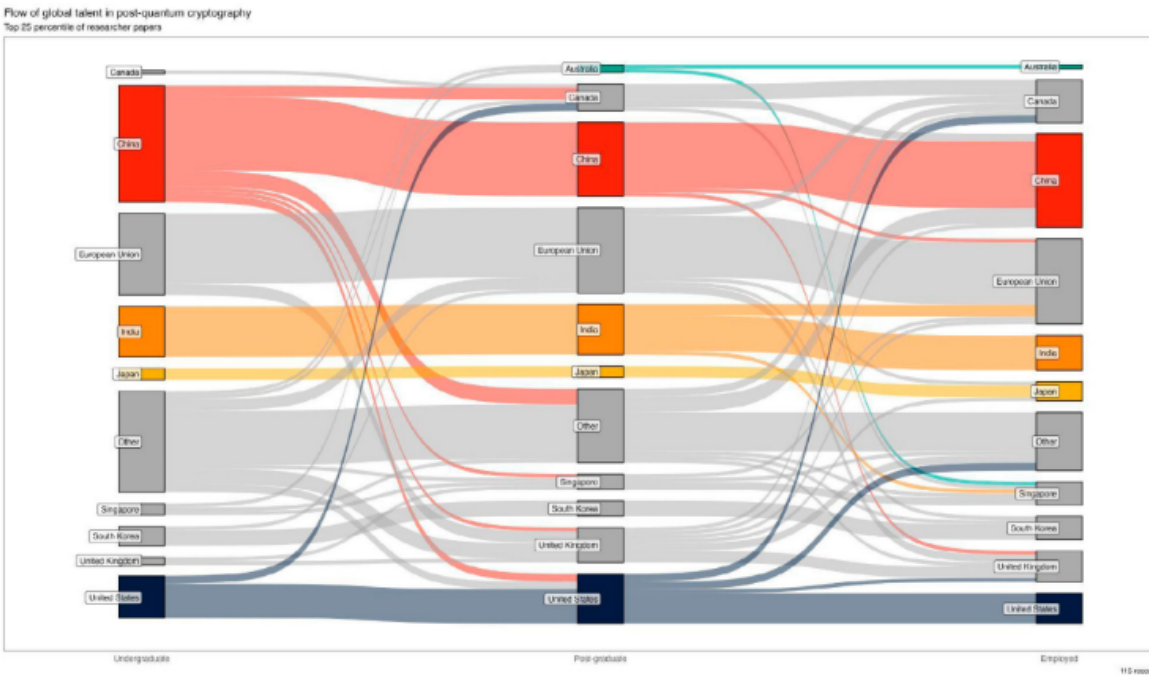


Gráfico 10. Flujo global de talento especializado en criptografía post-cuántica[91].

[91] Fuente: Gadia, J. *et al.*, "ASPI's Critical Technology Tracker…", *op. cit.,* p.35.

5. ANÁLISIS CRÍTICO: OPORTUNIDADES Y PERSPECTIVAS EN LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA.

5.1. OPORTUNIDADES PARA LA ESTANDARIZACIÓN DE LA CRIPTOGRAFÍA POST-CUÁNTICA.

5.1.1. La coordinación y cooperación internacional.

Los retos identificados en la normalización efectiva de la criptografía post-cuántica evidencian la necesidad de adoptar un enfoque global coordinado que equilibre intereses de seguridad nacional, competitividad empresarial y equidad internacional. Esta necesidad se intensifica en el contexto actual del mercado, caracterizado por un incremento significativo de relaciones comerciales y comunicaciones transfronterizas, todas ellas impulsadas por tecnologías digitales.

Instancias de todo el mundo reconocen los beneficios de adoptar un enfoque colaborativo en el desarrollo de tecnologías emergentes. Amandeep Singh Gill, enviado del Secretario General de la ONU en materia de tecnología, refuerza esta visión, destacando que el desarrollo y gobernanza de las tecnologías digitales requiere un enfoque inclusivo que integre a todas las partes interesadas[92].

Este enfoque permitiría a los operadores utilizar sistemas comunes, evitando obstáculos en las comunicaciones y transacciones internacionales debido a problemas de compatibilidad en las soluciones criptográficas. Además, dada la complejidad técnica de la criptografía post-cuántica, que requiere de una investigación constante y exhaustiva, es crucial que la investigación sea lo más inclusiva y colaborativa posible. Los expertos señalan que es imposible que una única entidad posea todos los conocimientos necesarios para el desarrollo

[92] *Vid.* Kasperen, A. y Wallach, W., "La gobernanza tecnológica y el papel del multilateralismo, con Amandeep Singh Gill: Iniciativa sobre Inteligencia Artificial e Igualdad", *Carnegie Council para la Ética en los Asuntos Internacionales,* 7 de febrero de 2023, (disponible en: https://es.carnegiecouncil.org/media/series/aiei/technology-governance-multilateralism, última consulta 22/10/2024).

efectivo de estas tecnologías emergentes, lo que hace esencial que los distintos actores implicados compartan sus recursos y conocimientos complementarios[93]. Por tanto, la colaboración internacional facilita no solo la adopción generalizada de la criptografía post-cuántica, con los beneficios de interoperabilidad que esto trae consigo, sino que favorece también que se mantenga una investigación continua de nuevos algoritmos criptográficos, lo que se ha identificado como fundamental para mantenerlos relevantes y actualizados.

Por otra parte, este enfoque trasciende la mera conveniencia técnica, teniendo implicaciones éticas y geopolíticas significativas. Al fomentar la colaboración y el intercambio de conocimientos, se permite una distribución más equitativa de recursos, mitigando la potencial brecha tecnológica entre naciones y organizaciones con diferentes capacidades. Este análisis se alinea con la postura que Naciones Unidas adopta en su Pacto Digital Global, en el que se enfatiza que el potencial de las tecnologías digitales, como la criptografía post-cuántica, sólo puede materializarse plenamente mediante una sólida cooperación internacional[94].

Además, la disponibilidad de soluciones criptografía post-cuántica estandarizadas permitiría a las empresas aprovechar sistemas ya listos para su uso, reduciendo de manera significativa los costos y complejidades asociados con la transición criptográfica. Esto resulta particularmente relevante para las PYMES, ya que les ayudaría a superar los obstáculos financieros que podrían enfrentar durante esta transición tecnológica.

Finalmente, es preciso resaltar que la estandarización internacional de la criptografía post-cuántica contribuiría a fortalecer la confianza y la seguridad en el ecosistema digital global. La implementación de estándares reconocidos a nivel internacional proporciona una mayor garantía sobre la fiabilidad de las soluciones criptográficas adoptadas. Esta confianza es particularmente crucial en su aplicación a sectores críticos como el financiero o el sanitario, donde la protección de datos sensibles no solo es una cuestión de estabilidad operativa.

[93] León, G., "Soberanía e interdependencias tecnológicas en el contexto geopolítico: hacia una gobernanza tecnológica inteligente", *Anales de la Real Academia de Doctores de España*, vol. 8, n.2, 2023, pp. 407, (disponible en: https://www.rade.es/imageslib/ACADEMICOS/DISCURSOS/V8N2%20-%2013%20-%20TPC%20-%20LE%C3%93N_gobernanza%20tecnol%C3%B3gica.pdf, última consulta 20/10/2024).
[94] Véase Naciones Unidas, "Global Digital Compact", *op. cit.*

5.1.2. El papel de la ISO.

En un escenario multipolar como el actual, donde diversas potencias y actores no estatales desempeñan un papel crucial en la estandarización de tecnologías digitales, emergen tanto desafíos como oportunidades de colaboración. El análisis presentado en este estudio concluye con que la cooperación internacional resulta la vía más efectiva para desarrollar e implementar estándares de criptografía post-cuántica. No obstante, la ausencia de una coordinación sólida y un liderazgo definido en la formulación de estos estándares ha resultado en ineficiencias y una duplicación de esfuerzos, entorpeciendo la armonización de los procesos de estandarización y la colaboración internacional. Esta situación genera un entorno complejo para las corporaciones, que se ven obligadas a navegar entre diversas propuestas y adaptarse a sus especificidades, lo cual resulta particularmente contraproducente.

Frente a este panorama, se hace evidente la necesidad de designar un organismo internacional que lidere los esfuerzos de cooperación, para que este asuma un papel central en el desarrollo de directrices para una transición criptográfica más uniforme y efectiva. Tras una evaluación detallada de las principales iniciativas para la estandarización de la criptografía post-cuántica en curso y de la labor de diversos organismos de normalización, la ISO emerge como el candidato idóneo para liderar este proceso, conclusión que se basa en varios factores clave.

Primero, la ISO cuenta con una extensa trayectoria en el desarrollo de estándares para tecnologías emergentes, lo que le confiere el prestigio y la credibilidad necesarios para liderar el proceso de estandarización en este ámbito. Desde su creación, la ISO ha elaborado más de 25.000 normas que abarcan múltiples aspectos de la gestión empresarial y los procesos de producción. Este historial de creación de normas ampliamente adoptadas la sitúa en una posición favorable para coordinar la armonización de estándares de criptografía post-cuántica a nivel global.

En segundo lugar, la reputación de independencia de la ISO le permite mantener una postura neutral e imparcial en el proceso de estandarización. Este rasgo es esencial para asegurar que los estándares desarrollados sean aceptados de manera generalizada y representen los intereses de todos los involucrados, evitando sesgos hacia países o empresas específicas. Si bien la UIT-T también puede hacer aportes valiosos, se considera aquí que el carácter no gubernamental de

la ISO le confiere mayor legitimidad, particularmente en un contexto de creciente rivalidad geopolítica.

En tercer lugar, como organismo internacional, el alcance y reconocimiento global de la ISO facilita la movilización de un amplio espectro de actores en la creación de estándares. Esta capacidad de convocatoria le permite abordar la estandarización de la criptografía post-cuántica desde una perspectiva multisectorial, considerando las necesidades y requisitos de todas las partes interesadas. Esto garantiza que las normas desarrolladas bajo su liderazgo se mantengan relevantes y efectivas en múltiples contextos y sectores industriales.

En cuarto lugar, el énfasis que la ISO pone en la certificación del cumplimiento de estándares se presenta como un método ideal para asegurar un compromiso más firme por parte de las entidades en cuanto a la adopción de estándares internacionales. Este aspecto es especialmente relevante en el ámbito de la criptografía post-cuántica, donde la conformidad y la interoperabilidad son fundamentales para la seguridad global y las transacciones internacionales.

Por último, cabe resaltar que la ISO cuenta con una extensa trayectoria de colaboración con otros organismos de normalización, como la IEC y la UIT, lo que se conoce como la Cooperación Mundial sobre Normas[95]. Esta experiencia en colaboración interinstitucional podría aprovecharse para establecer un marco de estandarización más robusto, integrando las fortalezas y conocimientos especializados de estas diversas organizaciones.

En este contexto, si bien es fundamental que una entidad asuma el liderazgo del proceso, resulta igualmente esencial mantener una coordinación cercana con las iniciativas nacionales de estandarización, como el proceso llevado a cabo por el NIST y los distintos proyectos de investigación de la Unión Europea en este campo. Atendiendo a estas consideraciones, se entiende que el modelo de trabajo aquí propuesto, fundamentado en un enfoque colaborativo bajo la dirección de la ISO, tiene el potencial de producir estándares más completos y ampliamente aceptados.

[95] *Vid.* Unión Internacional de Telecomunicaciones, "Cooperación Mundial sobre Normas", (disponible en: https://www.itu.int/es/ITU-T/extcoop/Pages/wsc.aspx, última consulta 20/10/2024).

5.2. CONSIDERACIONES REGULATORIAS: PROPUESTAS DE REFORMA EN POLÍTICAS Y NORMATIVAS INTERNACIONALES.

La eventual transición hacia soluciones criptográficas post-cuánticas plantea desafíos que van más allá de lo técnico y geopolítico, abarcando complejas cuestiones jurídicas y regulatorias. Expertos de todo el mundo, como el analista Arun Chandrasekaran, subrayan la necesidad de actualizar las políticas y marcos legales existentes, destacando la importancia de desarrollar regulaciones claras, que anticipen la eventual adopción de tecnologías emergentes como la criptografía post-cuántica[96].

Esta sección examinará cómo la adaptación de los marcos regulatorios debe abordar aspectos que incluyen desde la equidad en el acceso a estas tecnologías avanzadas y su impacto en la dinámica del mercado, a implicaciones relacionadas con la protección de datos y consideraciones sobre responsabilidad legal ante posibles fallos de seguridad.

5.2.1. La competencia del mercado internacional.

La criptografía post-cuántica promete transformar el mercado internacional, con el potencial de otorgar ventajas competitivas significativas en términos de seguridad y confiabilidad operativa a las empresas y naciones que lideren tanto su desarrollo como su implementación.

Sin embargo, la adopción desigual de estas tecnologías podría generar desequilibrios en la competencia internacional, lo que introducirá también nuevos desafíos regulatorios. Este escenario se ve agravado por la naturaleza altamente técnica de estas tecnologías, que limita el número de actores capaces de desarrollarlas, aumentando el riesgo de una concentración excesiva de propiedad intelectual. Tal concentración podría dar lugar a monopolios tecnológicos y exacerbar las barreras para una adopción uniforme y generalizada de las nuevas soluciones criptográficas.

[96] *Vid.* Perri, L., "Novedades del Hype Cycle de Gartner para las tecnologías emergentes de 2023", *Gartner*, 23 de agosto de 2023, (disponible en: https://www.gartner.es/es/articulos/novedades-del-hype-cycle-de-gartner-para-las-tecnologias-emergentes-2023, última consulta 22/10/2024).

Las recientes investigaciones iniciadas por la Comisión Europea contra Meta, Alphabet y Apple, por presuntas infracciones a la Ley de Mercados Digitales[97], así como las investigaciones del Departamento de Justicia de Estados Unidos y la Comisión Federal de Comercio sobre posibles prácticas antimonopolio de Nvidia, Microsoft y OpenAI en el ámbito de la IA[98], evidencian el potencial de las tecnologías emergentes para consolidar el poder de mercado de las grandes empresas tecnológicas. Estos casos ponen de manifiesto la necesidad de actualizar las leyes antimonopolio para establecer marcos normativos claros y comunes que aborden las ventajas competitivas que derivarán de las tecnologías post-cuánticas.

No obstante, la regulación en este ámbito presenta desafíos particulares, ya que requiere encontrar un delicado equilibrio que fomente la innovación y el libre comercio, salvaguardando la seguridad nacional y la competencia justa. El objetivo primordial es prevenir que organizaciones o países con recursos limitados para una adopción temprana de estas avanzadas soluciones de seguridad se vean perjudicados en el mercado.

Para mitigar estos riesgos, deberían establecerse programas internacionales que faciliten el intercambio de conocimientos y experiencias en el desarrollo e implementación de soluciones post-cuánticas, con énfasis en la transferencia de tecnología a países en desarrollo y apoyo a PYMES. Además, se debería considerar la creación de fondos internacionales para financiar la investigación y desarrollo en criptografía post-cuántica en países en desarrollo, así como programas de capacitación y educación para cerrar la brecha de conocimientos.

[97] Simonini, S., Regnier, T. y Bahrke, J. "La Comisión abre investigaciones de incumplimiento contra Alphabet, Apple y Meta en virtud de la Ley de Mercados Digitales", *Comisión Europea*, 25 de marzo de 2024, (disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689, última consulta 21/10/2024).

[98] ElEconomista.es, "EEUU investigará si Microsoft, Nvidia y OpenAI tienen el monopolio de la IA: a qué se enfrenta el trío", 6 de junio de 2024, (disponible en: https://www.eleconomista.es/tecnologia/noticias/12852448/06/24/eeuu-investigara-si-microsoft-nvidia-y-openai-tienen-el-monopolio-de-la-ia-a-que-se-enfrenta-el-trio.html, última consulta 22/10/2024).

5.2.2. Desafíos en el ámbito de la propiedad industrial.

Los sistemas criptográficos, como innovaciones que fusionan hardware, software y algoritmos avanzados, han sido tradicionalmente protegidos a través del sistema de patentes[99]. Estos son títulos de propiedad industrial que confieren a sus titulares derechos exclusivos sobre sus invenciones, otorgándoles el control sobre el acceso y uso de las mismas por parte de terceros[100].

No obstante, el escenario actual de protección de estos derechos[101] presenta notables dificultades, caracterizada por una significativa fragmentación en su regulación entre diferentes jurisdicciones, como señala la Organización Mundial de la Propiedad Intelectual (OMPI)[102].

[99] Los algoritmos criptográficos "en sí mismos" no son materia patentable según la legislación vigente. La Ley de Patentes española (art. 4.4 c) y el Convenio sobre la Patente Europea (art. 52 (3)) excluyen explícitamente la patentabilidad de "los descubrimientos, las teorías científicas y los métodos matemáticos". Sin embargo, los sistemas criptográficos pueden acceder a la protección de patentes cuando se presentan como soluciones que resuelven problemas técnicos específicos, siempre y cuando cumplan los criterios estándar de patentabilidad (novedad, actividad inventiva y aplicación industrial). *Vid.* Departamento de Patentes e Información Tecnológica, "Parte G: PATENTABILIDAD: Directrices externas de examen de solicitudes de patente (Ley 24/2015)", *Oficina Española de Patentes y Marcas*, marzo de 2023, pp. 51-53, (disponible en: https://www.oepm.es/export/sites/portal/comun/documentos_relacionados/PDF/Parte-G_Directrices-Patentes_Marzo-2023.pdf; Ley 24/2015, de 24 de julio, de Patentes; y Convenio de Munich sobre Concesión de Patentes Europeas, de 5 de octubre de 1973 (versión consolidada tras la entrada en vigor del Acta de revisión de 29 de noviembre de 2000). Como ejemplos de patentes en este ámbito *vid.* Díaz, A. Y Díaz, P., "Hybrid method of encryption and described electronic documents", *Oficina Española de Patentes y Marcas*, España, ES2613881, 2018, (disponible en: https://consultas2.oepm.es/InvenesWeb/detalle?referencia=P201630804, última consulta 06/11/2024); y Anderson, L., "CRIPTOGRAFÍA DE CAJA BLANCA FUERTE", *OMPI*, México, 2019006912, 2019, (disponible en: https://patentscope.wipo.int/search/es/detail.jsf?docId=MX283331696&_cid=P22-M33H2N-41084-1, última consulta 06/11/2024).

[100] Organización Mundial de la Propiedad Intelectual, "Patentes", (disponible en: https://www.wipo.int/es/web/patents, última consulta 22/10/2024).

[101] A efectos de este estudio se emplea el término propiedad intelectual en un sentido amplio, entendiendo que abarca las subcategorías de derechos de autor y propiedad industrial. No obstante, es preciso señalar que la terminología y la clasificación de estos derechos varía significativamente según la jurisdicción y el marco legal específico. La OMPI y el Parlamento Europeo consideran la propiedad intelectual como un concepto que incluye derechos de autor y propiedad industrial. Ahora bien, en derecho español la propiedad industrial se considera una categoría separada de la propiedad intelectual, pues el Texto Refundido de la Ley de Propiedad Intelectual española excluye la propiedad industrial de su ámbito de aplicación. Por su parte, el sistema jurídico anglosajón subdivide la propiedad intelectual en "copyright" (equivalente a los derechos de autor en sistemas de derecho civil) y propiedad industrial, manteniendo ambas dentro del ámbito más amplio de la propiedad intelectual. *Vid.* Organización Mundial de la Propiedad Intelectual, "¿Qué es la propiedad intelectual?", 2021, p.4, (disponible en: https://www.wipo.int/edocs/pubdocs/es/wipo_pub_450_2020.pdf, última consulta 06/11/2024); Mos, A., Maciejewski, M. Y Bux, U. "La propiedad intelectual, industrial y comercial", *Parlamento Europeo*, mayo de 2024, (disponible en:https://www.europarl.europa.eu/factsheets/es/sheet/36/la-propiedad-intelectual-industrial-y-comercial, última consulta 06/11/2024); y Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[102] La OMPI señala que en los últimos años se va logrando cierta convergencia en los criterios regulatorios en el ámbito de la propiedad intelectual. Ahora bien, persisten diferencias significativas entre el sistema de derecho

Esta diversidad normativa cobra especial relevancia ante la inminente transición hacia la criptografía post-cuántica, planteando dos desafíos fundamentales específicos.

Por un lado, porque es previsible que numerosas patentes de sistemas post-cuánticos se conviertan en elementos necesarios para el desarrollo de futuras normas técnicas. Esto sugiere que ciertas patentes de criptografía post-cuántica serían clasificadas como Patentes Esenciales para Normas (PEN), un término que engloba aquellas patentes que protegen tecnologías imprescindibles para el cumplimiento de estándares técnicos[103]. En este contexto, el desafío principal radica en cómo asegurar que se permita un uso justo y generalizado de estas tecnologías emergentes, pues las PEN plantean importantes complejidades en términos de concesión de licencias y prevención de prácticas abusivas como el *patent hold-up*.

Tradicionalmente, el monopolio concedido por las PEN se ha equilibrado mediante el compromiso de sus titulares de otorgar licencias bajo términos FRAND (justos, razonables y no discriminatorios). Sin embargo, como la Comisión Europea señaló en su Comunicación de 2017 sobre el establecimiento del enfoque de la Unión con respecto a las patentes esenciales para normas, no puede fijarse una metodología universal para aplicar los términos FRAND, ya que nociones como son la equidad y razonabilidad son variables en función del sector y evolucionan con el tiempo. Con esta observación se evidenció la urgente necesidad de desarrollar un marco regulatorio claro y coherente en materia de PEN[104], llevando a que el 27

continental y el *Common Law*. Este estudio se enfoca en examinar los desafíos que surgen en el desarrollo de nuevos sistemas criptográficos desde la perspectiva de la propiedad industrial en el marco del derecho continental. No obstante, es fundamental que el lector comprenda que existen variaciones significativas en la terminología y los niveles de protección según el sistema legal en cuestión. En el sistema de derecho continental, la propiedad intelectual y la propiedad industrial se consideran categorías distintas, mientras que en el *Common La*w, ambas se engloban bajo el concepto más amplio de "*intellectual property*", lo cual tiene implicaciones prácticas de cara a la protección y regulación de derechos de exclusiva. Véase Organización Mundial de la Propiedad Intelectual, "¿Qué es la propiedad intelectual?", 2021, p.1 y p.3, (disponible en: https://www.wipo.int/edocs/pubdocs/es/wipo_pub_450_2020.pdf, última consulta 06/11/2024).

[103] Un ejemplo de tecnologías que requiere numerosas patentes para ser implementadas son tecnologías como el 5G o el WiFi 6. La complejidad técnica de estos estándares hace que los mismos precisen de numerosas patentes para su desarrollo, de manera que la falta de acceso a alguna de ellas impediría el uso de estas tecnologías. Esto es especialmente problemático por la amplia variedad de aplicaciones y beneficios que traerán, aplicándose tanto a una potencial implementación en teléfonos móviles como a monitores cardíacos y otros dispositivos médicos. *Vid.* Instituto de Derecho de Patentes de Interés Público, "Comments of the Public Interest Patent Law Institute on the European Commission's Proposal for a Regulation of the European Parliament and of the Council on Standard Essential Patents and Amending Regulation (EU)2017/1001", Comisión Europea, 2023, p.4, (disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13109-Intellektuel-ejendomsret-ny-ramme-for-standard-essentielle-patenter/F3434472_da, última consulta 06/11/2024).

[104] *Vid.* Comisión Europea (COM 2017), Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo: Establecimiento del enfoque de la Unión con respecto a las patentes

de abril de 2023 la Comisión Europea publicara una propuesta legislativa específicamente diseñada para aumentar la transparencia en el licenciamiento de PEN. Entre las medidas propuestas destacan la creación de un registro obligatorio de patentes y una base de datos electrónica para mejorar el seguimiento de las patentes y sus condiciones de licencia, así como la creación de un "centro de competencia" especializado en la gestión de licencias y patentes relacionadas con PEN.

Aunque esta regulación aplicaría a nivel europeo, la recomendación ofrece un marco útil que puede servir como modelo para una regulación internacional más amplia de la criptografía post-cuántica. La primera cuestión a plantear sería la creación de un centro específico de patentes criptográficas dentro de la OMPI[105], que gestionaría disputas y consultas relacionadas con la implementación de sistemas y algoritmos de criptografía post-cuántica patentados. Además, se sugiere designar a una organización de normalización internacional, como la ISO, para desarrollar directrices comunes de concesión de licencias basadas en el marco FRAND adaptadas a las particularidades de cada sector. Esto facilitaría un enfoque más coherente en la concesión de licencias de tecnologías criptográficas post-cuánticas esenciales, lo que resulta particularmente relevante en un entorno empresarial cada vez más globalizado y dependiente de tecnologías avanzadas de seguridad pero caracterizado por la ausencia de una regulación internacional armonizada en esta materia[106].

Por otra parte, las diferencias en los requisitos de patentabilidad entre jurisdicciones pueden resultar en una protección inconsistente de las innovaciones criptográficas a nivel

esenciales para normas, (disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017DC0712, última consulta: 21/10/2024).

[105] La OMPI es el organismo especializado de Naciones Unidas en materia de propiedad intelectual, contando con 193 Estados miembros en la actualidad. Esta es la razón por la que se entiende la mejor instancia para gestionar las patentes de criptografía post-cuántica de manera que se asegure la interoperabilidad de sistemas en la mayor medida posible. Organización Mundial de la Propiedad Intelectual, "Estados miembros", (disponible en: https://www.wipo.int/members/es/, última consulta 22/10/2024).

[106] Tanto Estados Unidos, la Unión Europea, China y Japón han buscado abordar las problemáticas que presentan las PEN. Mientras se observa una creciente convergencia en el abordaje de las cuestiones relacionadas con las PEN y las condiciones FRAND, las diferencias en los enfoques regionales persisten.
En Estados Unidos, la División Antimonopolio del Departamento de Justicia emitió en diciembre de 2018 nuevas directrices que ampliaban la consideración del uso de mandamientos judiciales en el contexto de las condiciones FRAND. Por otro lado, China adopta una posición más restrictiva. Las nuevas directrices, hoy vigentes, desaprueban ampliamente el uso de mandamientos judiciales en litigios sobre PEN. Este enfoque prioriza la negociación y el acuerdo entre las partes, limitando las acciones legales a situaciones en que se demuestre mala fe por parte del presunto infractor. Véase Johnson, D. y Yang, M., "Actualidad mundial en materia de licencias de patentes esenciales", *OMPI revista*, febrero de 2019, (disponible en: https://www.wipo.int/wipo_magazine/es/2019/01/article_0003.html, última consulta 06/11/2024).

internacional. En este respecto, cabe entender que el sistema de concesión de licencias en el marco específico de la criptografía post-cuántica presenta desafíos particularmente complejos. En primer lugar, porque la estrecha vinculación que esta tecnología guarda con cuestiones de seguridad nacional se posiciona como un factor añadido a las consideraciones habituales de propiedad industrial y competencia de mercado, propiciando que los actores involucrados en el desarrollo de tecnologías post-cuánticas puedan ser especialmente reticentes a permitir su disponibilidad. Por otra parte, la naturaleza global y colaborativa de la investigación en este campo complica la determinación de la titularidad y regulación de las invenciones. Esto podría llevar a disputas sobre el acceso y regulación de patentes clave, especialmente en colaboraciones internacionales.

Para abordar estos desafíos, los marcos de propiedad industrial podrían actualizarse para favorecer la protección de innovaciones en este ámbito mediante patentes mancomunadas bajo el auspicio de un organismo internacional, promoviendo el desarrollo conjunto. El modelo que adopta el Medicines Patent Pool (MPP)[107] demuestra las ventajas de este enfoque; entre 2010 y enero de 2023, el MPP firmó 34 licencias para diversas tecnologías sanitarias y facilitó el acceso a 30 mil millones de dosis de tratamientos. Una organización análoga para la criptografía post-cuántica podría proporcionar seguridad jurídica al sistema de patentes y facilitar la adopción global de la criptografía post-cuántica.

[107] El MPP es una organización de salud pública respaldada por las Naciones Unidas que trabaja para ampliar el acceso a medicamentos esenciales en países con menos recursos. Su modelo de funcionamiento se basa en negociar licencias voluntarias con los titulares de patentes de medicamentos clave para crear una mancomunidad de patentes. Esto permite que otros fabricantes produzcan y distribuyan versiones más asequibles de estos medicamentos en países en desarrollo, mientras los titulares de las patentes reciben regalías por las ventas en distintos países. *Vid.* Medicines Patent Pool, "El Medicines Patent Pool pone en marcha una ambiciosa estrategia a tres años para aumentar el acceso a los medicamentos y las tecnologías sanitarias para las personas que los necesitan", 2023, (disponible en: https://medicinespatentpool.org/uploads/2023/01/Strategy_Launch_Statement_Spanish.pdf, última consulta: 21/10/2024).

5.2.3. Transparencia en la gestión de datos y problemas de atribución de responsabilidad.

La gestión y el tratamiento de datos digitales se ha convertido en un tema de controversia internacional, con diferentes posturas adoptadas por las potencias mundiales generando obstáculos al comercio internacional y provocando tensiones geopolíticas.

En este contexto, se hace necesario establecer acuerdos internacionales sobre niveles mínimos de transparencia respecto a la información proporcionada a los usuarios sobre la seguridad criptográfica que protege sus transacciones y comunicaciones. Para ello, los marcos de protección de datos existentes, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, requerirán actualizaciones para incorporar estándares de seguridad post-cuánticos en sus requisitos.

Estas modificaciones tendrán implicaciones significativas en el ámbito contractual y de responsabilidad legal por fallos de seguridad. Anticipando posibles disputas sobre la responsabilidad de las empresas que no implementen adecuadamente protecciones post-cuánticas, será necesario modificar los acuerdos de confidencialidad para reflejar los nuevos requisitos de protección de datos mediante criptografía post-cuántica. Asimismo, las cláusulas de cumplimiento con proveedores y socios comerciales deberán adaptarse a estos nuevos estándares.

Este escenario podría dar lugar a nuevos tipos de litigios por negligencia o incumplimiento de contrato, lo que exigirá una actualización de conceptos doctrinales, particularmente en lo referente a la "debida diligencia" empresarial en el nuevo panorama de seguridad de las transacciones comerciales internacionales. En el marco de la transición criptográfica, este concepto deberá incorporar consideraciones relacionadas con las medidas tomadas por los operadores para revisar sus políticas de almacenamiento, transferencia y eliminación de datos, alineando dichas consideraciones con los nuevos requisitos de seguridad e identificando posibles vulnerabilidades[108].

[108] Conforme a la Guía para empresas multinacionales de la OCDE, la debida diligencia se puede entender como un proceso a través del cual las entidades identifican y gestionan los posibles riesgos asociados a operaciones comerciales. Véase Organización para la Cooperación y el Desarrollo Económico, "Guía de la OCDE de Debida Diligencia para una Conducta Empresarial Responsable", 2018, pp.19-22, (disponible en:

Un análisis comparativo de diversas iniciativas nacionales muestra que tanto gobiernos como empresas, como es el caso de Estados Unidos con la "Ley de Preparación para la Ciberseguridad Cuántica" o IBM con su "Hoja de Ruta Quantum Safe"[109], ya reconocen la necesidad de establecer plazos de migración y que entidades públicas y privadas realicen una relación de los sistemas criptográficos que emplean

Siguiendo estas pautas, se entiende que los marcos regulatorios deberían modificarse para incorporar medidas más estrictas y específicas. Esto podría incluir la imposición de la adopción obligatoria de estándares post-cuánticos en sectores particularmente vulnerables, así como sistemas de certificación que garanticen el cumplimiento de los mismos. Paralelamente, se deberían definir plazos de migración armonizados y de carácter vinculante para la transición hacia algoritmos post-cuánticos, lo cual resulta esencial para evitar los vacíos de seguridad que derivarían de una implementación desigual.

6. CONCLUSIONES.

En un contexto de creciente multipolaridad, potencias de todo el mundo han advertido el creciente papel que las tecnologías emergentes cobran desde un punto de vista geopolítico. Esto ha cristalizado en un cambio de dinámicas en los procesos de estandarización de normas técnicas, pues en los últimos años es cada vez mayor la influencia que actores estatales y no estatales han buscado acaparar.

Dentro de este marco general, la presente investigación se ha centrado en el estudio de la criptografía post-cuántica, adoptando un enfoque analítico distintivo al explorar las dimensiones geopolíticas y regulatorias vinculadas a la estandarización de esta tecnología. Mientras que la literatura existente se había centrado principalmente en analizar las dificultades técnicas inherentes a las tecnologías emergentes, esta investigación llega más allá, identificando cómo la creciente politización en la gobernanza de estándares tecnológicos genera desafíos adicionales para la estandarización internacional.

https://mneguidelines.oecd.org/Guia-de-la-OCDE-de-debida-diligencia-para-una-conducta-empresarial-responsable.pdf, última consulta 21/10/2024).

[109] Véase el Gráfico 6, en la sección 3.1.2. "Principales actores en la competencia por el liderazgo post-cuántico".

A continuación, se presentan las principales conclusiones que pueden derivarse del análisis, cuya toma en consideración resulta fundamental para abordar las dificultades geopolíticas, técnicas y regulatorias que caracterizan el proceso de estandarización de la criptografía post-cuántica:

1. El análisis expuesto permite prever ciertas tendencias que seguirán las dinámicas geopolíticas futuras. Las ventajas económicas asociadas al liderazgo en el desarrollo de estándares técnicos son cada vez más evidentes, lo que se ve reflejado a medida que las principales potencias mundiales intensifican sus esfuerzos por dominar los foros de estandarización. Esta situación anticipa una dinámica en la que el control sobre los estándares tecnológicos será una cuestión determinante para definir quién liderará el mercado internacional.

2. Se presenta una propuesta práctica para canalizar la estandarización internacional de la criptografía post-cuántica, por la cual se identifica que la ISO sería una plataforma óptima para facilitar dicho proceso. El marco desarrollado se basa en un estudio comparativo de iniciativas internacionales, regionales y nacionales, proponiendo elementos concretos como la obligatoriedad de realizar inventarios de sistemas criptográficos a nivel organizacional y la implementación inicial de soluciones híbridas como estrategia de mitigación de riesgos.

3. Al identificar conexiones significativas entre la competencia por el liderazgo en la estandarización de la criptografía post-cuántica y las dinámicas más amplias de poder en el ámbito global, este estudio abre nuevas líneas de investigación. Por un lado, se sugiere explorar cómo la cooperación tecnológica en el ámbito concreto de la criptografía post-cuántica podría reconfigurar las alianzas internacionales y las estrategias de seguridad nacional en el contexto contemporáneo. Por otro lado, se anima a profundizar en cómo la competencia en el ámbito concreto de la criptografía post-cuántica se entrelaza con la competencia en torno al desarrollo de otras tecnologías emergentes. Si bien el presente estudio se acota al proceso de estandarización de la criptografía post-cuántica, el mismo permite identificar dinámicas geopolíticas más

amplias que habrá que tomar en consideración para una regulación comprehensiva del mercado internacional.

7. FUENTES Y REFERENCIAS.

7.1. FUENTES INSTITUCIONALES.

7.1.1. Estados Unidos.

Barker, W., Polk, W. y Souppaya, M., "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms", *National Institute of Standards and Technology,* 2021, (disponible en: https://doi.org/10.6028/NIST.CSWP.04282021, última consulta 21/10/2024).

Brandao, L. y Peralta, R., "Normas, Investigación y Aplicaciones en Criptografía en NIST: Algunas notas sobre PEC y PQC", *National Institute of Standards and Technology*, 2019, (disponible en: https://csrc.nist.gov/CSRC/media/Presentations/standards-research-and-applications-in-cryptograph/images-media/20191007-uchile--slides-nist-pec-pqc--rev-oct-14.pdf, última consulta 22/10/2024).

Chen, L. *et al*, "Report on Post-Quantum Cryptography", *National Institute of Standards and Technology*, 2016, (disponible en: http://dx.doi.org/10.6028/NIST.IR.8105, última consulta 21/10/2024).

Congreso de los Estados Unidos, Quantum Computing Cybersecurity Preparedness Act, 2022, (disponible en: https://www.congress.gov/bill/117th-congress/house-bill/7535, última consulta 20/10/2024).

La Casa Blanca, National Cybersecurity Strategy, 2023, (disponible en: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, última consulta: 21/10/2024).

La Casa Blanca, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 2022, (disponible en: https://www.whitehouse.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/, última consulta 20/10/2024).

National Institute of Standards and Technology, "*Post-Quantum Cryptography: PQC*", 25 de octubre de 2024, (disponible en: *https://www.nist.gov/pqcrypto*, última consulta 25/10/2024).

National Institute of Standards and Technology, "What Is Post-Quantum Cryptography", 13 de agosto de 2024, (disponible en:https://www.nist.gov/cybersecurity/what-post-quantum-cryptography, última consulta 21/10/2024).

National Institute of Standards and Technology, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards", 13 de agosto de 2024, (disponible en: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, última consulta 21/10/2024).

National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ", 2024, (disponible en: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF, última consulta 20/10/2024).

National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", 2022, (disponible en: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF, última consulta 20/10/2024).

U.S. Department of State, "United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future", 2024, (disponible en: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/, última consulta 21/10/2024).

7.1.2. Europa.

7.1.2.1. Unión Europea.

Bernstein, D.J., Hülsing, A. y Lange, T., "Post-Quantum Cryptography: Integration study", *European Union Agency for Cybersecurity*, 2022, (disponible en: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study, última consulta: 21/10/2024).

Campagna, M. *et al,* "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges", *ETSI White Paper,* nº8, 2015, (disponible en: https://www.etsi.org/media-library/white-papers, última consulta 21/10/2024).

Comisión Europea, "European Quantum Communication Infrastructure (EuroQCI) Initiative", 2023, (disponible en: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci, última consulta: 21/10/2024).

Comisión Europea, "OPENQKD - Open European Quantum Key Distribution Testbed", *CORDIS EU Research Results*, 2023, (disponible en:10.3030/857156, última consulta: 21/10/2024).

Comisión Europea (COM 2022), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de la UE en materia de normalización; Establecer normas mundiales para apoyar un mercado único de la Unión resiliente, ecológico y digital, (disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031, última consulta 21/10/2024).

Comisión Europea (COM 2017), Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo: Establecimiento del enfoque de la Unión con respecto a las patentes esenciales para normas, (disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017DC0712, última consulta: 21/10/2024).

Consejo de la Unión Europea, "Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE en el próximo decenio", 2024, (disponible en: https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/, última consulta: 21/10/2024).

Instituto de Derecho de Patentes de Interés Público, “Comments of the Public Interest Patent Law Institute on the European Commission’s Proposal for a Regulation of the European Parliament and of the Council on Standard Essential Patents and Amending Regulation (EU)2017/1001”, *Comisión Europea*, 2023, (disponible en: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13109-Intellektuel-ejendomsret-ny-ramme-for-standard-essentielle-patenter/F3434472_da, última consulta 06/11/2024).

Instituto Europeo de Normas de Telecomunicaciones, “CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation”, 2021, (disponible en: https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.01_60/tr_103823v010101p.pdf, última consulta: 21/10/2024).

Instituto Europeo de Normas de Telecomunicaciones, “Quantum Computing and the risk to security and privacy”, 2018, (disponible en: https://www.etsi.org/images/files/ETSITechnologyLeaflets/QuantumSafeCryptography.pdf, última consulta 20/10/2024).

Mos, A., Maciejewski, M. Y Bux, U. “La propiedad intelectual, industrial y comercial”, *Parlamento Europeo*, mayo de 2024, (disponible en:https://www.europarl.europa.eu/factsheets/es/sheet/36/la-propiedad-intelectual-industrial-y-comercial, última consulta 06/11/2024).

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. (DOUE 12 de abril de 2024).

7.1.2.2. España.

Asociación Española de Normalización, “Conocimiento para afrontar los desafíos de las organizaciones”, *La revista de la normalización española*, n.7, 2018, (disponible en:

https://revista.une.org/7/conocimiento-para-afrontar-los-desafios-de-las-organizacione.html, última consulta 20/10/2024).

Asociación Española de Normalización, "UNE publica un informe con las ventajas para sus miembros", 2020, (disponible en: https://www.une.org/la-asociacion/sala-de-informacion-une/noticias/une-publica-un-informe-con-las-ventajas-para-sus-miembros/, última consulta 20/10/2024).

Centro Criptológico Nacional, "Recomendaciones para una transición postcuántica segura", 2022 (disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file, última consulta 20/10/2024).

Departamento de Patentes e Información Tecnológica, "Parte G: PATENTABILIDAD: Directrices externas de examen de solicitudes de patente (Ley 24/2015)", *Oficina Española de Patentes y Marcas*, marzo de 2023, (disponible en: https://www.oepm.es/export/sites/portal/comun/documentos_relacionados/PDF/Parte-G_Directrices-Patentes_Marzo-2023.pdf, última consulta: 9/11/2024).

Díaz, A. Y Díaz, P., "Hybrid method of encryption and described electronic documents", *Oficina Española de Patentes y Marcas*, España, ES2613881, 2018, (disponible en: https://consultas2.oepm.es/InvenesWeb/detalle?referencia=P201630804, última consulta 06/11/2024).

García, A. *et al.*, "Report: Spain Quantum Industry", *Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones*, 2023, (disponible en: https://biblio.ontsi.red.es/cgi-bin/koha/opac-detail.pl?biblionumber=7476, última consulta: 21/10/2024).

Instituto Nacional de Ciberseguridad, "Glosario de términos de ciberseguridad: una guía de aproximación para el empresario", 2021, (disponible en:https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el, última consulta 21/10/2024).

López Chamorro, N., “El camino hacia la supremacía cuántica: oportunidades y desafíos en el ámbito financiero, la nueva generación de criptografía resiliente”, *Banco de España*, n.2421, 2024, (disponible en: https://doi.org/10.53479/36696, última consulta 21/10/2024).

Maydeu-Olivares, S., “Geopolítica de la tecnología: actores, procesos y dinámicas”, *Dirección de Justicia Global del Ayuntamiento de Barcelona*, 2023, (disponible en: https://cdn2.hubspot.net/hubfs/426027/Oxfam-Website/oi-informes/Geopolitica-Tecnologia-es.pdf, última consulta 20/10/2024).

Ministerio de Industria y Turismo, “Legislación básica e infraestructura para la calidad y seguridad industrial”, (disponible en: https://industria.gob.es/es-es/Servicios/calidad/Paginas/legislacion-basica.aspx?Faq=Normalizaci%C3%B3n, última consulta 21/10/2024).

UNE, “Publicadas las nuevas normas UNE-ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para impulsar la ciberseguridad y digitalización”, 17 de mayo de 2023, (disponible en: https://www.une.org/la-asociacion/sala-de-informacion-une/notas-de-prensa/nuevas-normas-une-isoiec-27001-y-27002-ciberseguridad-digitalizacion, última consulta 20/10/2024).

7.1.2.3. Otros países europeos.

Agence nationale de la sécurité des systèmes d'information, “ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)”, 2023, (disponible en: https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography, última consulta 21/10/2024).

Federal Office for Information Security, “Cryptographic Mechanisms: Recommendations and Key Lengths”, 2024, (disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile, última consulta 21/10/2024).

Federal Office for Information Security, “Quantum-safe cryptography: fundamentals, current developments and recommendations”, 2021, (disponible en:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6, última consulta 20/10/2024).

Seaman, J., "China and the New Geopolitics of Technical Standardization", *Notes de l'Ifri*, French Institute of International Relations, 2020, (disponible en: https://www.ifri.org/en/papers/china-and-new-geopolitics-technical-standardization, última consulta 21/10/2024).

7.1.2. Otros organismos.

Agencia de noticias Xinhua, "El Comité Central del Partido Comunista de China y el Consejo de Estado publicaron el Esquema de desarrollo de la normalización nacional", *Red del Gobierno de China,* 10 de octubre de 2021, (disponible en: https://www.gov.cn/zhengce/2021-10/10/content_5641727.htm, última consulta: 21/10/2024).

Allende, L., "Tecnologías Cuánticas: una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social", *Banco Interamericano de Desarrollo*, 2019, (disponible en: https://publications.iadb.org/es/publications/spanish/viewer/Tecnolog%C3%ADas_cu%C3%A1nticas_Una_oportunidad_transversal_e_interdisciplinar_para_la_transformaci%C3%B3n_digital_y_el_impacto_social.pdf, última consulta 21/10/2024).

Anderson, L., "CRIPTOGRAFÍA DE CAJA BLANCA FUERTE", *OMPI*, México, 2019006912, 2019, (disponible en: https://patentscope.wipo.int/search/es/detail.jsf?docId=MX283331696&_cid=P22-M33H2N-41084-1, última consulta 06/11/2024).

Comisión Electrotécnica Internacional, "National Committees", (disponible en: https://www.iec.ch/national-committees, última consulta: 21/10/2024).

Gadia, J. *et al.*, "ASPI's Critical Technology Tracker: The global race for future power", *Australian Strategic Policy Institute*, nº 69, 2023, (disponible en: https://www.aspi.org.au/report/critical-technology-tracker, última consulta 21/10/2024).

Hull, J., "La protección de los secretos comerciales: cómo pueden las organizaciones hacer frente al desafío de adoptar medidas razonables", Organización Mundial de la Propiedad Intelectual, 2019, (disponible en: https://www.wipo.int/wipo_magazine/es/2019/05/article_0006.html, última consulta 21/10/2024).

Medicines Patent Pool, "El Medicines Patent Pool pone en marcha una ambiciosa estrategia a tres años para aumentar el acceso a los medicamentos y las tecnologías sanitarias para las personas que los necesitan", 2023, (disponible en: https://medicinespatentpool.org/uploads/2023/01/Strategy_Launch_Statement_Spanish.pdf, última consulta: 21/10/2024).

Naciones Unidas, "Global Digital Compact", 2024, (disponible en: https://www.un.org/global-digital-compact/en , última consulta 20/10/2024).

Organización Internacional de Normalización, "¿Qué es la criptografía?", (disponible en: https://www.iso.org/es/seguridad-informacion/criptografia, última consulta 21/10/2024).

Organización Internacional de Normalización, "Miembros", (disponible en: https://www.iso.org/es/sobre/miembros, última consulta 21/10/2024).

Organización Internacional de Normalización y Comisión Electrotécnica Internacional, "Uso y referencia a normas ISO e IEC en la reglamentación técnica", *Asociación Española de Normalización y Certificación*, 2007, (disponible en: https://www.une.org/normalizacion_documentos/referencia_normas_iso_iec_reg_tecnica.pdf, última consulta 21/10/2024).

Organización Mundial de la Propiedad Intelectual, "¿Qué es la propiedad intelectual?", 2021, (disponible en: https://www.wipo.int/edocs/pubdocs/es/wipo_pub_450_2020.pdf, última consulta 06/11/2024).

Organización Mundial de la Propiedad Intelectual, "Estados miembros", (disponible en: https://www.wipo.int/members/es/, última consulta 22/10/2024).

Organización Mundial de la Propiedad Intelectual, "Patentes", (disponible en: https://www.wipo.int/es/web/patents, última consulta 22/10/2024).

Organización Mundial del Comercio, "Acuerdo sobre Obstáculos Técnicos al Comercio", 1994, (disponible en: https://www.wto.org/spanish/docs_s/legal_s/17-tbt_s.htm, última consulta 21/10/2024).

Organización para la Cooperación y el Desarrollo Económico, "Guía de la OCDE de Debida Diligencia para una Conducta Empresarial Responsable", 2018, (disponible en: https://mneguidelines.oecd.org/Guia-de-la-OCDE-de-debida-diligencia-para-una-conducta-empresarial-responsable.pdf, última consulta 21/10/2024).

Reding, D.F. y Eaton, J., "Science & Technology Trends 2020-2040: Exploring the S&T Edge", *NATO Science & Technology Organization*, 2020, (disponible en: https://www.nato.int/cps/en/natohq/news_175574.htm, última consulta 21/10/2024).

Sector de Estandarización de la Unión Internacional de Telecomunicaciones, "Consideraciones de seguridad para redes de distribución de claves cuánticas", 2020, (disponible en: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf, última consulta: 21/10/2024).

Unión Internacional de Telecomunicaciones, "Elaboración de normas", (disponible en: https://www.itu.int/es/ITU-T/about/Pages/development.aspx, última consulta 20/10/2024).

Unión Internacional de Telecomunicaciones, “Security for/by emerging technologies including quantum-based security”, (disponible en: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Q15.aspx, última consulta 20/10/2024).

Unión Internacional de Telecomunicaciones, “Cooperación Mundial sobre Normas”, (disponible en: https://www.itu.int/es/ITU-T/extcoop/Pages/wsc.aspx, última consulta 20/10/2024).

7.2. OTROS RECURSOS.

Avaro, D., “La industria de la inteligencia artificial: una carrera por su liderazgo”, *Problemas del desarrollo*, vol.54, n.212, 2023, pp.105-127, (disponible en: https://doi.org/10.22201/iiec.20078951e.2023.212.69959, última consulta 22/10/2024).

Bernardi-Espín, E.O., y Quimiz-Moreira, M.A, “Incidencia de la computación cuántica en los algoritmos criptográficos”, *Código Científico Revista De Investigación*, vol. 5, n.1, 2024, pp.627-650, (disponible en: https://doi.org/10.55813/gaea/ccri/v5/n1/401, última consulta: 21/10/2024).

Blázquez, I., “tecnología y geopolítica: sobre una teoría del cambio en las relaciones internacionales”, Información Comercial Española, *Revista de Economía*, n.935, 2024, pp.135-150, (disponible en: https://doi.org/10.32796/ice.2024.935.7797, última consulta 22/10/2024).

Bogobowicz, M. *et al*., “Quantum Technology Monitor 2024”, *McKinsey Digital*, 2024, (disponible en: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage, última consulta: 21/10/2024).

Da Ponte, A., “Geopolítica de los espacios tecnológicos emergentes”, *Revista de la Escuela Superior de Guerra*, 2021, pp.88-101, (disponible en: http://www.esg.iue.edu.ar/revistas/RevEdEsp21.pdf#page=88, última consulta: 21/10/2024).

ElEconomista.es, “EEUU investigará si Microsoft, Nvidia y OpenAI tienen el monopolio de la IA: a qué se enfrenta el trío”, 6 de junio de 2024, (disponible en:

https://www.eleconomista.es/tecnologia/noticias/12852448/06/24/eeuu-investigara-si-microsoft-nvidia-y-openai-tienen-el-monopolio-de-la-ia-a-que-se-enfrenta-el-trio.html, última consulta 22/10/2024).

Escribano Pablos, J.I., "Criptografía segura frente a adversarios cuánticos: Análisis y variantes de propuestas para estandarización", *Universidad Rey Juan Carlos*, Madrid, 2022.

Feijóo, C., "El consenso internacional sobre los estándares", *el Alcázar de las Ideas*, 2022, (disponible en: https://www.elalcazardelasideas.es/el-consenso-internacional-sobre-los-estandares/#_ednref21 última consulta 21/10/2024).

Fonfría, A. y Duch Brown, N. (2021). "La geopolítica de la transformación digital y sus efectos en el tejido industrial", *Economía industrial*, 2021, n.420, pp.25-34.

Fundación Innovación Bankinter, "El futuro de la ciberseguridad: Criptografía Post-Cuántica (PQC)", 4 de octubre de 2023, (disponible en: https://www.fundacionbankinter.org/noticias/criptografia-post-cuantica/?_adin=0202186489, última consulta 21/10/2024).

Global Data's Patent Analytics, "Q2 2024 update: quantum computing related patent activity in the technology industry", *Verdict*, 2024, (disponible en: https://www.verdict.co.uk/patent-activity-quantumcomputing-technology-industry/?cf-view&cf-closed, última consulta 21/10/2024).

Global System for Mobile Communications Association, "Post Quantum Telco Network Impact Assessment: Whitepaper", 2023, (disponible en: https://www.gsma.com/newsroom/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper/, última consulta: 21/10/2024).

GMV, " Criptografía en la era cuántica", *IT User*, 2021, (disponible en: https://www.ituser.es/whitepapers/content-download/a55caf39-4cf8-4712-93de-6aea4b1bc29e/itu67-especial-gmv.pdf?s=portada, última consulta 21/10/2024).

Hernández, S. “Fortalece estrategias y Políticas de Ciberseguridad: ISO 27032:2023”, *Global Suite Solutions*, 2024, (disponible en: https://www.globalsuitesolutions.com/es/estrategias-politicas-de-ciberseguridad-iso-iec-27032-2023/, última consulta 20/10/2024).

Horvath, M. *et al*., “Postquantum Cryptography: The Time to Prepare Is Now!*”, Gartner,* 1 de julio de 2024, (disponible en: https://www.gartner.com/en/documents/5550295, última consulta 21/10/2024).

IBM, “Algoritmos desarrollados por IBM son los primeros estándares de criptografía post-cuántica del mundo”, 13 de agosto de 2024, (disponible en: https://latam.newsroom.ibm.com/2024-08-13-Algoritmos-desarrollados-por-IBM-son-los-primeros-estandares-de-criptografia-post-cuantica-del-mundo, última consulta: 21/10/2024).

IBM, “Make the world quantum safe”, (disponible en: https://www.ibm.com/quantum/quantum-safe#roadmap, última consulta: 21/10/2024).

Kasperen, A. y Wallach, W., “La gobernanza tecnológica y el papel del multilateralismo, con Amandeep Singh Gill: Iniciativa sobre Inteligencia Artificial e Igualdad”, *Carnegie Council para la Ética en los Asuntos Internacionales,* 7 de febrero de 2023, (disponible en: https://es.carnegiecouncil.org/media/series/aiei/technology-governance-multilateralism, última consulta 22/10/2024).

León, G., “*Relevancia geopolítica de las tecnologías duales: consecuencias y oportunidades para reforzar la soberanía tecnológica de la Unión Europea*”, *UPM Press*, 2023, (disponible en: https://oa.upm.es/76650/1/AF_GONZALO_LEON_Relevancia.pdf, última consulta 20/10/2024).

León, G., “Soberanía e interdependencias tecnológicas en el contexto geopolítico: hacia una gobernanza tecnológica inteligente”, *Anales de la Real Academia de Doctores de España*, vol.8, n.2, 2023, pp.405-433, (disponible en: https://www.rade.es/imageslib/ACADEMICOS/DISCURSOS/V8N2%20-%2013%20-

%20TPC%20-%20LE%C3%93N_gobernanza%20tecnol%C3%B3gica.pdf, última consulta 20/10/2024).

Liaudat, S., "Estándares técnicos, desarrollo y geopolítica: historia, actualidad y desafíos", *Centro de Investigaciones de Política Internacional*, 2023, (disponible en: https://www.cipi.cu/wp-content/uploads/2023/02/Trabajo.-Estandares-tecnicos-geopolitica-y-desarrollo.pdf, última consulta 21/10/2024).

Mota, A., "SGSI y PDCA: Gestiona con Éxito la Implementación de la ISO 27001", *INNEVO*, 2024, (disponible en: https://blog.innevo.com/sgsi-pdca-iso27001, última consulta 20/10/2024).

Perri, L., "Novedades del Hype Cycle de Gartner para las tecnologías emergentes de 2023", *Gartner*, 23 de agosto de 2023, (disponible en: https://www.gartner.es/es/articulos/novedades-del-hype-cycle-de-gartner-para-las-tecnologias-emergentes-2023, última consulta 22/10/2024).

Rambaut Lemus, D.F., "Introducción a la Criptografía post-cuántica basada en teoría de códigos", *Universidad del Rosario*, Bogotá, 2021.

Ricart, R.J., "Innovación en defensa y tecnologías profundas en la OTAN: cuestión de disposición y eficacia*", Real Instituto Elcano,* 2023, (disponible en https://www.realinstitutoelcano.org/comentarios/innovacion-en-defensa-y-tecnologias-profundas-en-la-otan-cuestion-de-disposicion-y-eficacia/*,* última consulta 21/10/2024).

Rühling, T., "Implicaciones y riesgos del poder tecnológico de China", *Diálogo Político*, n.1, 2023, pp.84- 95, (disponible en: https://dialogopolitico.org/edicion-especial-2024-claves-para-entender-a-china/implicaciones-y-riesgos-del-poder-tecnologico-de-china/, última consulta 21/10/2024).

Sanz Bayón, P., "Desafíos jurídicos del mercado ante la revolución digital", en A. Thomson Reuters (Ed.), *Estudios de Derecho Mercantil y Derecho Tributario*. *Derechos de los socios*

en las sociedades de capital, consumidores y productos financieros y financiación de empresas en el nuevo marco tecnológico, Estudios, pp.251-282.

Shapiro, C. "Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting", *Innovation Policy and the Economy*, vol. 1, 2001, pp.119-150, (disponible en: https://doi.org/10.1086/ipe.1.25056143 , última consulta: 21/10/2024).

Simonini, S., Regnier, T. y Bahrke, J. "La Comisión abre investigaciones de incumplimiento contra Alphabet, Apple y Meta en virtud de la Ley de Mercados Digitales", *Comisión Europea*, 25 de marzo de 2024, (disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689, última consulta 21/10/2024).

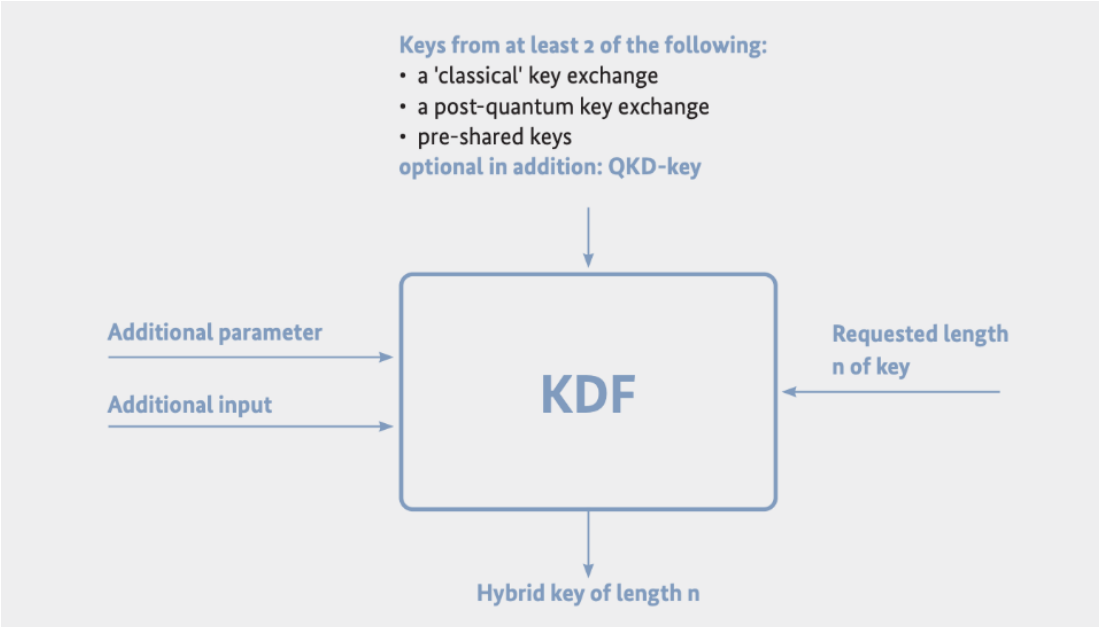
Vega Clemente, V., "Revolución tecnológica y derecho mercantil", *Revista de Estudios Económicos y Empresariales*, n.30, 2018, pp.149-169.

10. ANEXOS:

ANEXO I - DIFERENCIAS DE PROCESAMIENTO ENTRE COMPUTADORES TRADICIONALES Y CUÁNTICOS[110].

[110] Allende, L., "Tecnologías Cuánticas: una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social", *Banco Interamericano de Desarrollo*, 2019, p.13 (disponible en: https://publications.iadb.org/es/publications/spanish/viewer/Tecnolog%C3%ADas_cu%C3%A1nticas_Una_oportunidad_transversal_e_interdisciplinar_para_la_transformaci%C3%B3n_digital_y_el_impacto_social.pdf, última consulta 21/10/2024).

ANEXO II- REPRESENTACIÓN ESQUEMÁTICA DEL FUNCIONAMIENTO DE UN SISTEMA HÍBRIDO DE ACUERDO DE CLAVES[111].



[111] Federal Office for Information Security, "Quantum-safe cryptography: fundamentals, current developments and recommendations", 2021, p.38, (disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626, última consulta 21/10/2024).

ANEXO III- ALGORITMOS SELECCIONADOS DEL CONCURSO DEL NIST[112].

Criptosistema asimétrico y KEM	Área y problema matemático
CRYSTALS-Kyber	Retículo estructurado (MLWE)

Firma digital	Área y problema matemático
CRYSTALS-Dilithium	Retículo estructurado (MLWE)
Falcon	Retículo estructurado (SIS)
SPHINCS$^+$	Funciones hash

[112] Centro Criptológico Nacional, Recomendaciones para una transición postcuántica segura, 2022, pp.6-7, (disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/495-ccn-tec-009-recomendaciones-transicion-postcuantica-segura/file, última consulta 20/10/2024).

ANEXO IV- SUITE DE ALGORITMOS DE SEGURIDAD NACIONAL COMERCIAL 2.0[113].

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

[113] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", 2022, p.9, (disponible en: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF, última consulta 20/10/2024).