La percepción del riesgo de la computación cuántica en la criptografía actual

Estudio realizado en el ámbito de la gran empresa en España

Índice

Introducción

La computación cuántica ha surgido como una tecnología prometedora y disruptiva que tiene el potencial de revolucionar diversos campos, incluyendo la seguridad y especialmente la criptografía, hasta el punto de que permitirá enfrentar problemas inabordables por la computación clásica.

La computación cuántica se basa en los principios de la mecánica cuántica, utilizando qubits en lugar de los bits tradicionales para procesar información. A diferencia de los bits clásicos, los qubits pueden existir en una combinación de estados simultáneamente gracias a la superposición cuántica que, junto con el entrelazamiento cuántico, permite realizar cálculos de manera exponencialmente más eficiente y resolver problemas complejos que, a día de hoy, son imposibles utilizando exclusivamente computación clásica.

Si bien la computación cuántica promete una capacidad de procesamiento sin precedentes, también plantea serios retos para la criptografía actual y, por tanto, a los mecanismos utilizados para la protección de la información confidencial.

Los algoritmos criptográficos actuales, que se basan en la dificultad para resolver ciertos problemas matemáticos debido a la limitación de capacidad de cómputo, serán vulnerables a ataques llevados a cabo con ordenadores cuánticos. Es decir, los ordenadores cuánticos podrán, en un futuro próximo, descifrar rápidamente los sistemas de criptografía asimétrica actuales y comprometer por tanto la integridad de los datos y la privacidad de la información.

Este desafío plantea la necesidad de desarrollar nuevas técnicas y algoritmos de criptografía, que sean resistentes tanto a la computación cuántica como a la clásica, conocidos como criptografía post-cuántica o Quantum Safe. Estos nuevos estándares criptográficos están diseñados para resistir potenciales ataques llevados a cabo mediante algoritmos cuánticos como Shor, y asegurar la confidencialidad y la integridad de la información en un mundo en el que la computación cuántica tenga capacidad para llevar a cabo este tipo de ataques.

En la actualidad, ya se están desarrollando investigaciones e invirtiendo esfuerzos en el desarrollo y estandarización de algoritmos de criptografía post-cuántica. Varios actores importantes, entre los que se cuentan gobiernos, instituciones académicas y empresas de tecnología están empleando recursos significativos en esta área, donde los esfuerzos se realizan en una doble vía: concienciar sobre el desafío que la computación cuántica representa para la criptografía, e impulsar la adopción de soluciones post-cuánticas basadas, por ejemplo, en modelos híbridos que combinen algoritmos actuales con los futuros estándares Quantum Safe. Del mismo modo, las organizaciones deben empezar a preparar agendas de trabajo que les permitan adaptar sus entornos IT, a través de metodologías crypto-agile, a los nuevos algoritmos criptográficos Quantum Safe. En este sentido, cabe resaltar que, como se ha podido observar en la ejecución de este estudio, algunas de estas organizaciones ya han iniciado la puesta en marcha de acciones para conocer su exposición a este riesgo criptográfico.

Este estudio, realizado mediante entrevistas a responsables de seguridad y tecnología de una treintena de grandes empresas de diversos sectores españolas, ha permitido, a partir de la percepción de esas grandes empresas, explorar los retos que plantea la computación cuántica, analizar su impacto en el paradigma actual, las tendencias emergentes, las oportunidades de mercado y las posibles soluciones a estos desafíos.

Este estudio de mercado examina la percepción del riesgo de los principales roles que, de una u otra manera, se están viendo afectados por los avances de la computación cuántica y el impacto sobre la criptografía en sus organizaciones. También evalúa el grado de avance de la criptografía post-cuántica y las tasas de adopción esperadas, lo que proporciona una visión completa y actualizada de las grandes empresas españolas que sirve como base para ayudar a los actores de los diferentes sectores del panorama empresarial español a tomar decisiones informadas.

En otras palabras, este estudio permite abordar cómo la computación cuántica plantea retos significativos para la criptografía moderna que pueden —y deben— ser palancas de cambio para que las organizaciones modernicen sus arquitecturas y procesos, orientándolos hacia un enfoque ágil que facilite futuros cambios criptográficos minimizando el impacto y los costes derivados.

Principales conclusiones

Hace un año, IBM España puso en marcha el que a la postre sería primer estudio sobre Quantum Safe en el país, entrevistando a una treintena de responsables de seguridad y tecnología de grandes empresas españoles de sectores como banca, seguros, energía, turismo o transporte, entre otros.

En concreto, este documento analiza las respuestas surgidas de 32 conversaciones en profundidad con responsables de seguridad (CISO) y tecnología (CTO) de algunas de las principales empresas españolas llevadas a cabo entre los meses de mayo y julio de 2023.

A día de hoy, la computación cuántica continúa siendo una gran desconocida para la mayor parte de los empleados de las empresas encuestadas. Normalmente las áreas de negocio desconocen las capacidades y beneficios que este nuevo modelo de computación puede proporcionarles. Al tiempo, las áreas de seguridad comienzan a tener nociones del impacto que estas nuevas capacidades de cómputo cuántico tendrán sobre la protección de la información (más concretamente sobre la criptografía afectada) y los desafíos que esto puede llegar a suponer.

La mayor parte de los equipos de seguridad de las organizaciones encuestados considera este escenario como un reto a largo plazo (+10 años). Sólo aquellas organizaciones más sensibilizadas con el riesgo criptográfico han comenzado a realizar las primeras acciones necesarias para migrar sus activos criptográficos (algoritmos, claves, etcétera).

Las respuestas de muchos de los entrevistados permiten concluir que el riesgo es principalmente percibido como tecnológico y, más concretamente, como un evento que podrá abordarse y subsanarse de forma sencilla en el ámbito de los componentes de infraestructura (balanceadores de carga, firewalls, terminadores VPN, etcétera). Sin embargo, lo cierto es que esto únicamente permitirá solventar aquellos riesgos asociados a la transferencia de información a través de medios como Internet.

Sólo un grupo pequeño y más maduro identifica también el riesgo en las aplicaciones de negocio y el uso que hacen de la criptografía en el propio código (funciones de firma digital, algoritmos de cifrado y ofuscación de la información, mecanismos de control, etcétera) algo sobre lo que es necesario realizar adaptaciones.

Además, hay un común denominador a las empresas encuestadas independientemente de su sector y es que esperan que los diferentes proveedores lleven al mercado soluciones (tecnológicas y de servicios) que les ayuden a iniciar la transformación a Quantum Safe. En la mayoría de casos, porque las organizaciones no tienen capacidad suficiente como para llevar a cabo un proyecto de transformación de estas características, por el trabajo del día a día y la falta de ancho de banda o capacidad presupuestaria necesarias para una transformación de esta envergadura.

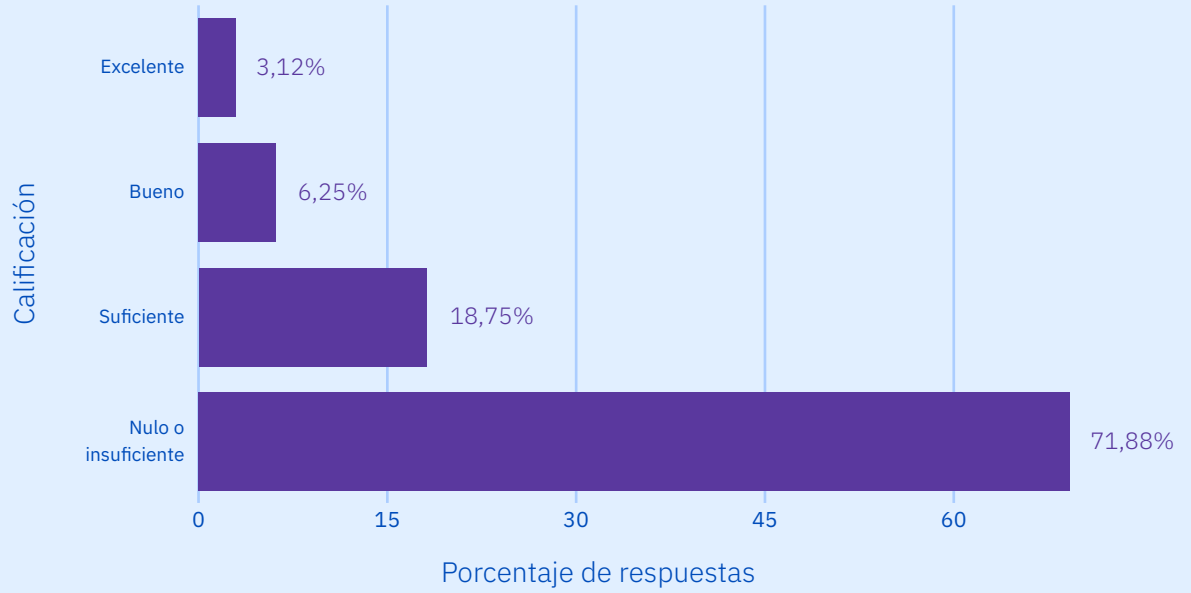
Por último, entre las conclusiones del estudio sobresale una clara preocupación entre todos los encuestados por cómo se va a llevar a cabo esta adaptación criptográfica de forma coordinada. En este sentido, todos tienen claro que se trata de una acción que no podrá llevarse a cabo de forma unilateral, debido a los problemas de incompatibilidad que se pueden llegar a producir (comunicaciones en tiempo real, verificaciones históricas, etcétera) y que será necesario establecer mecanismos que permitan a las organizaciones realizar su transformación de forma organizada.

La cuántica en las organizaciones

La mayor parte de las organizaciones encuestadas desconoce el potencial de la computación cuántica y sus capacidades

Para una amplia mayoría de entrevistados, el grado de familiaridad y conocimiento de la tecnología cuántica dentro de sus organizaciones resulta bajo: más de un 71% de los encuestados considera que el conocimiento que existe sobre esta tecnología en sus organizaciones es insuficiente.

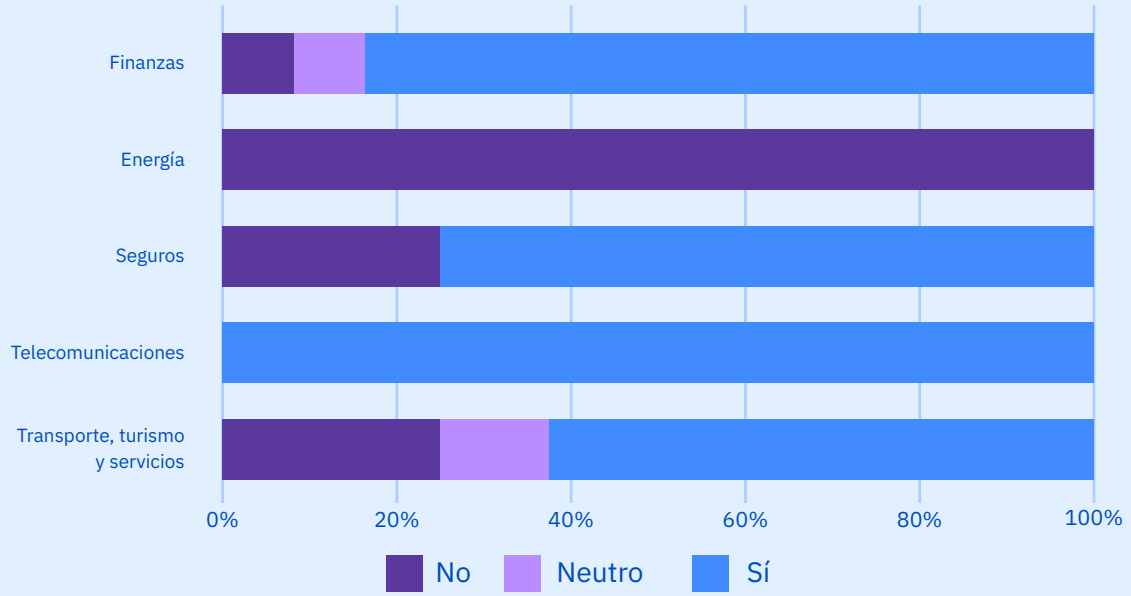
Grado de conocimiento de la computación cuántica dentro de la organización



Como era de esperar, existe una fuerte correlación entre el nivel de facturación de las organizaciones y su conocimiento sobre la tecnología, siendo aquellas con mayor volumen de facturación las que más conocimiento dicen tener sobre la materia. Tampoco sorprende que las empresas del sector Financiero sean las que mayor conocimiento tienen sobre la cuestión ya que la computación cuántica tiene, al menos por ahora, una mayor aplicabilidad y potencial de ofrecer numerosas ventajas en las que la industria ya está trabajando, como la realización de análisis de riesgo y optimización de carteras mucho más precisos, rápidos y eficientes.

De hecho, los encuestados del sector Financiero han manifestado su expectación porque la computación cuántica tenga un impacto significativo en el campo de la inteligencia artificial (IA), lo que podría facilitar la detección de fraudes y mejorar la toma de decisiones en este ámbito empresarial.

¿Cree que la adopción de la computación cuántica de su compañía podría suponer una ventaja competitiva en su sector?



Merece la pena destacar que la computación cuántica, a pesar de que la mayoría de las veces es una tecnología poco conocida, es considerada como una ventaja estratégica por la mayoría de los entrevistados.

Percepciones diferenciadas por sectores

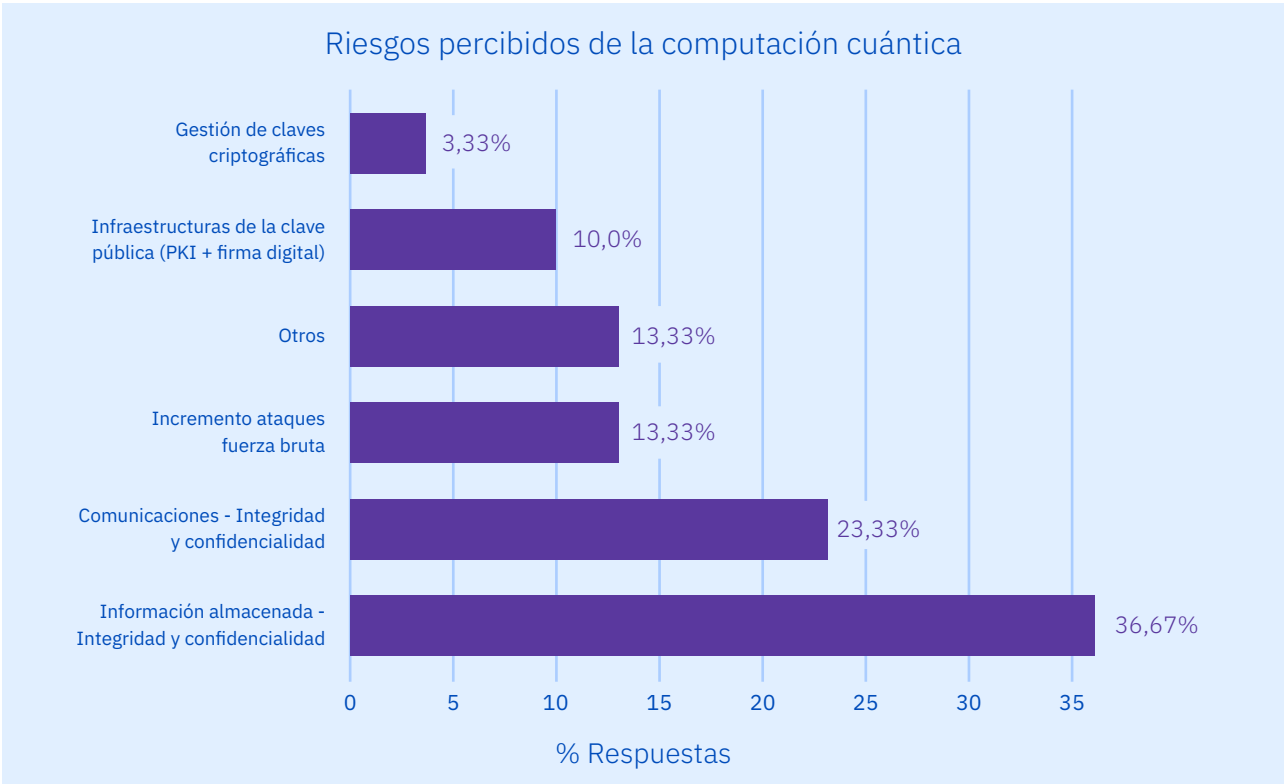
En concreto, los encuestados del ámbito de las Telecomunicaciones y los Servicios se muestran plenamente convencidos de que la computación cuántica supondrá una ventaja competitiva para sus sectores, debido a las potenciales beneficios que puede aportar en campos como la optimización de redes de comunicaciones, lo que permitiría a las empresas de Telecomunicaciones mejorar sus eficiencias.

Se abre además, aunque todavía de forma teórica, un nuevo mercado basado en las comunicaciones cuánticas —conocido como Internet Cuántico — que permitirá a las empresas del sector de las Telecomunicaciones la transmisión de grandes cantidades de información de manera casi inmediata, aunque la tecnología necesaria para poder llevarlo a cabo se encuentra actualmente en fase de experimentación.

En el lado opuesto, los sectores Energético e Inmobiliario consideran que la computación cuántica no supondrá una ventaja competitiva. Esto se debe a que estas industrias se basan en infraestructuras físicas y procesos más tradicionales, donde los potenciales beneficios de la computación cuántica no resultan todavía tan evidentes. Debe tenerse en cuenta que estos sectores tienden a tener ciclos de inversión a largo plazo, lo que reduce la relevancia inmediata de la tecnología cuántica en su competitividad. Sin embargo, es importante señalar que la tecnología avanza con rapidez y que probablemente en un futuro próximo surgirán casos de uso de la computación cuántica que beneficien también a estos sectores, como por ejemplo el desarrollo de nuevos materiales o la interrelación de la cuántica con la IA.

Esta visión estratégica de la computación cuántica impacta de forma clara en las iniciativas que muchas compañías están poniendo en marcha para formar a sus equipos y generar talento en torno a esta tecnología. Lo que se traduce principalmente en la ejecución de planes de capacitación en el corto plazo (el 42% de las organizaciones encuestadas indica que los llevarán a cabo dentro de uno o dos años) para que los empleados comiencen a entender, de forma adecuada a sus roles, la computación cuántica así como el impacto en sus sectores, comenzando con la identificación de casos de uso y aplicabilidad. Este punto es especialmente relevante en las áreas de ciberseguridad, donde resulta crítico comprender los retos que esta nueva tecnología puede suponer transversalmente a los diferentes sectores y, debido a sus peculiaridades, en cada organización de forma particular.

Más del 90% de los entrevistados considera que la aplicabilidad de la computación cuántica puede generar nuevos retos para su organización.



La mayor parte de las empresas encuestadas reconoce no haber formalizado los riesgos relacionados con la computación cuántica.

La mayor parte de las empresas encuestadas reconoce no haber formalizado los riesgos relacionados con la computación cuántica dentro de sus sistemas de gestión corporativos, existiendo además un claro consenso entre todos los encuestados en que la computación cuántica supondrá, de una u otra manera, un riesgo para su organización.

Profundizando en los potenciales riesgos específicos que identifican las compañías, la intrusión y el acceso no autorizado a información confidencial aparece como el más relevante.

IA generativa y cuántica

La posibilidad de que un atacante pueda acceder a la información confidencial protegida mediante mecanismos de cifrado (tanto para aquella información almacenada como para la que se transmite a través de diferentes redes de comunicación) es el riesgo identificado con mayor frecuencia por parte de los encuestados. Además, el estudio ha permitido identificar otro riesgo relevante: el potencial incremento en las capacidades de los atacantes para llevar a cabo acciones ofensivas basadas en mecanismos de fuerza bruta apoyándose en modelos de IA generativa para acceder a sistemas y/o entornos de la organización.

Cabe destacar que únicamente un 10% de los encuestados ha mencionado un potencial riesgo o amenaza contra las infraestructuras de clave pública (PKI, por sus siglas en inglés, *Public Key Infrastructure*) y los mecanismos de firma digital existentes en la actualidad. Desde nuestro punto de vista, consideramos importante sensibilizar sobre las implicaciones que este tipo de riesgo tiene para las organizaciones desde un punto de vista legal, ya que un atacante podría falsificar firmas digitales y comprometer la autenticidad e integridad de documentos y transacciones en línea.

Las respuestas recopiladas durante el estudio permiten además pensar en un escenario en el que el impacto de estos riesgos se comenzará a materializar en el corto plazo (de 1 a 5 años), tal y como ha señalado la mayoría de los encuestados (65%).

En cualquier caso, merece la pena destacar que todas las organizaciones participantes en el estudio consideran que estos riesgos puedan materializarse antes de los 10 próximos años. Por este motivo, algunas compañías (focalizadas sobre todo en el sector Financiero) ya se encuentran definiendo su hoja de ruta para transformarse en organizaciones Quantum Safe.

Particularidades sectoriales

De acuerdo con las estimaciones de todos los entrevistados, la información que hoy se maneja seguirá siendo válida, y por tanto un activo empresarial, cuando existan ordenadores cuánticos capaces de descifrarla

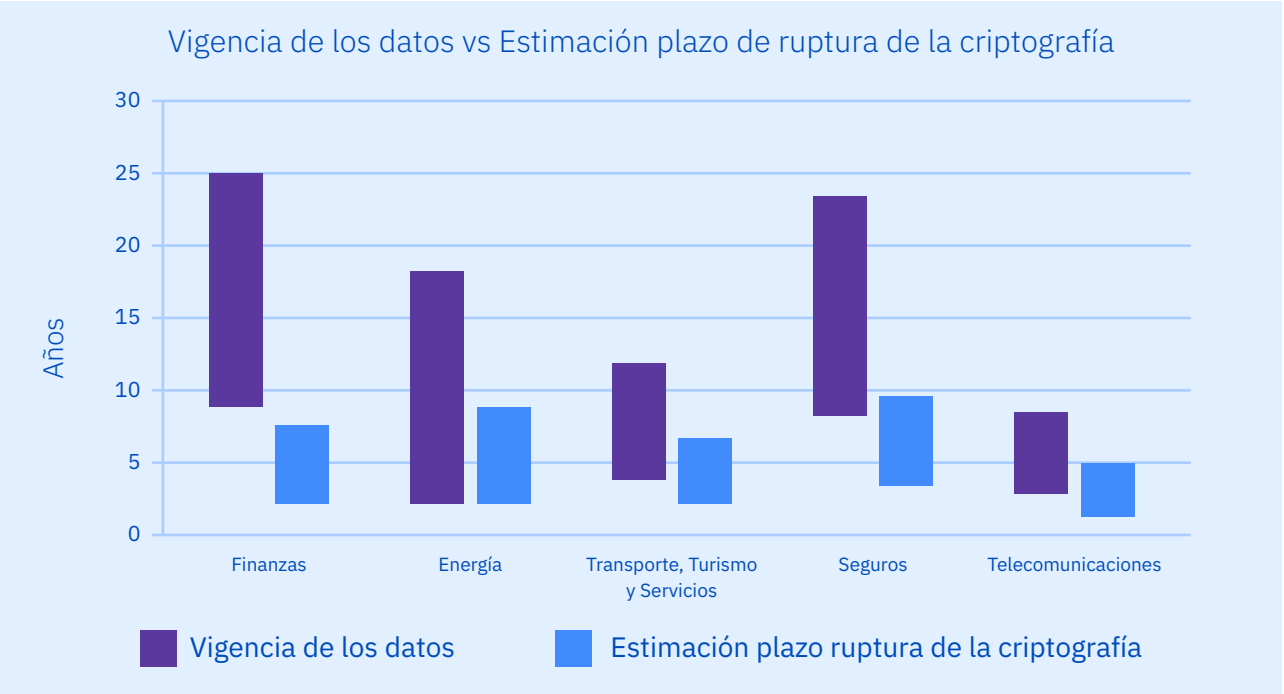
A pesar de que los riesgos que arroja la computación cuántica sobre la criptografía sean comunes para todas las organizaciones, es importante destacar que variarán en función de las características propias de cada una de ellas. Factores como la tecnología empleada, la tipología de información que manejan, la vigencia de sus sistemas e infraestructuras, entre otros, determinarán el nivel de exposición y vulnerabilidad ante futuros ataques.

Por ello, resulta esencial que cada organización evalúe de manera individualizada su situación y tome las medidas adecuadas para garantizar la protección de sus activos y la continuidad de sus operaciones en el futuro. Este estudio ha permitido constatar que el tiempo de validez de la información gestionada difiere notablemente entre sectores y está estrechamente relacionado con lo establecido por las distintas regulaciones específicas de cada sector.

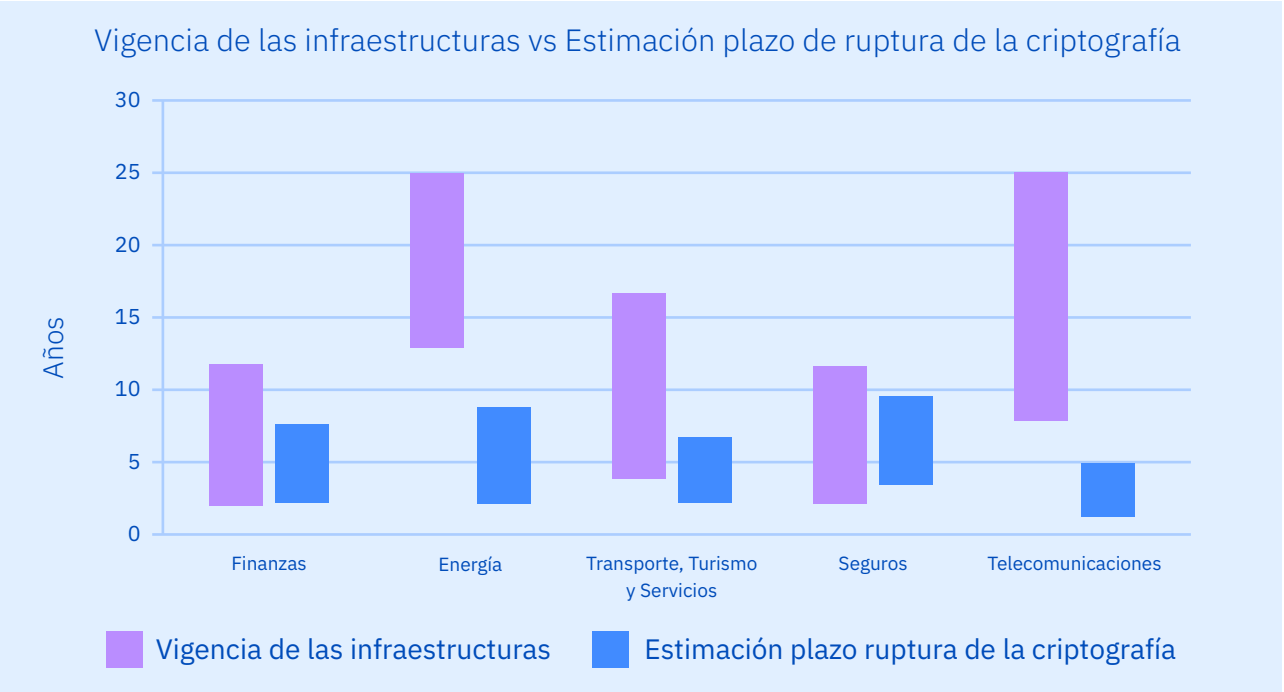
Y es que uno de los aspectos fundamentales a la hora de valorar el impacto es el tiempo de vigencia de la información clasificada como confidencial, ya que un atacante dispondrá tarde o temprano de la capacidad de descifrar dicha información. Si el objetivo es mantener la información protegida, debe llevarse a cabo, cuando sea necesario, un recifrado de la misma antes de que el desarrollo de la computación cuántica permita ejecutar este tipo de ataques contra el cifrado actual.

Un activo empresarial de larga duración

En este sentido, el estudio permite afirmar que todos los sectores consideran, de acuerdo con sus propias previsiones, que la información con la que trabajan en la actualidad seguirá siendo relevante, y por tanto un activo empresarial vulnerable, incluso después de que el desarrollo de la computación cuántica permita romper la criptografía con la que está protegida en la actualidad. La razón es que muchos de esos datos, como información personal, registros financieros, secretos comerciales y propiedad intelectual, mantendrán su valor a lo largo del tiempo.



En este contexto, es recomendable como *best practice* que las organizaciones revisen y actualicen periódicamente sus políticas de gestión de la información, implementen estrategias de almacenamiento y retención adecuadas, eliminen la información que ya no sea relevante y recifren aquella que siga siendo necesaria con algoritmos resistentes a ataques cuánticos.



De igual modo que a la información, este situación impactará también en los sistemas e infraestructuras de las organizaciones, que deberán actualizarse para ser compatibles con los nuevos algoritmos. En muchos casos, la actualización de estos sistemas e infraestructuras puede resultar complicada debido a su tipología. Por ejemplo, aquellas infraestructuras críticas como plantas de energía, sistemas de transporte o redes de comunicación requieren de un alto nivel de seguridad y estabilidad, lo cual puede dificultar la implementación de cambios y actualizaciones. También nos encontramos con que los largos ciclos de vida de algunos activos (aviación, sistemas logísticos, etcétera) pueden generar desafíos al momento de llevar a cabo su renovación o sustitución.

Por ello, ante estas situaciones las organizaciones deben llevar a cabo una planificación y gestión cuidadosa de sus recursos, tanto técnicos como de información, estableciendo estrategias y enfoques tácticos que permitan la actualización y adaptación para confrontar de forma eficaz y proactiva a los desafíos que plantea la era cuántica en materia de seguridad y protección de sus activos.

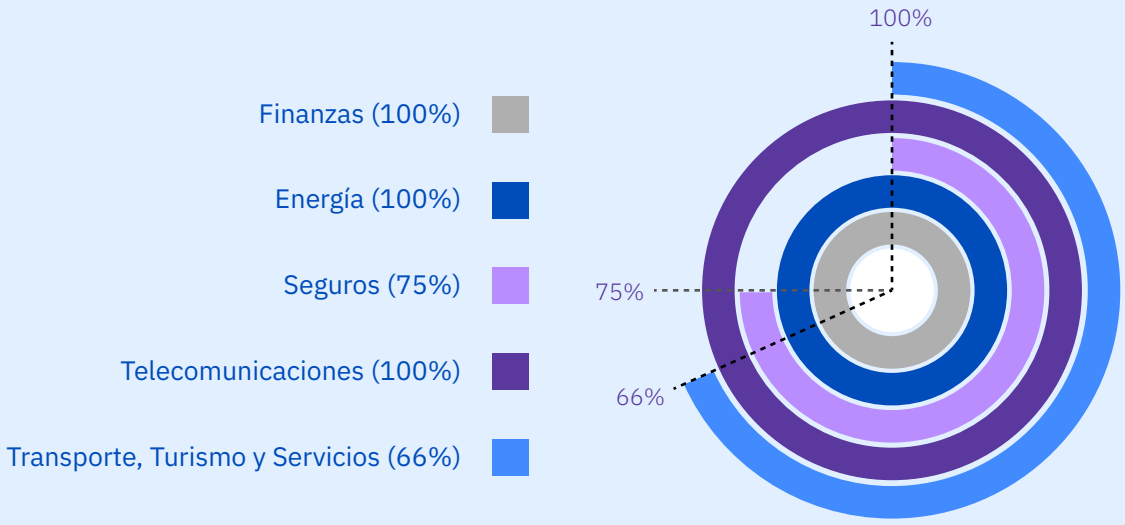
El reto que supone la computación cuántica para los actuales algoritmos de firma digital impacta en casi todos los sectores.

Autenticidad e identidad de partes

Otro aspecto relevante en el que las regulaciones establecen requerimientos criptográficos es en todo lo relativo a la identidad y la firma digital. En este contexto, la integridad, autenticidad y confidencialidad de las transacciones digitales podrían verse comprometidas, lo que generaría desconfianza en las comunicaciones y operaciones digitales. Los sistemas de firma digital, que garantizan la autenticidad de los documentos y la identidad de las partes involucradas, resultarán vulnerables a la computación cuántica, lo que afectará a su validez y, por tanto, a la seguridad de estos procesos.

Este estudio ha permitido contrastar que prácticamente todas las compañías, independientemente del sector y características propias, se encuentran sometidas a estos requisitos regulatorios relativos a la firma digital.

Compañias con Regulación sobre Firma Digital



Por tanto, todas estas organizaciones deberán afrontar la tarea de transformar sus actuales infraestructuras de clave pública (PKI) a algoritmos Quantum Safe, para poder garantizar así que los procesos de autenticación y firma digital mantengan su robustez y seguridad ante los futuros computadores cuánticos.

En general, las compañías consideran tener un inventario suficientemente maduro que les permitirá identificar los activos sobre los que deben llevar cabo acciones de protección ante los riesgos derivados de la computación cuántica.

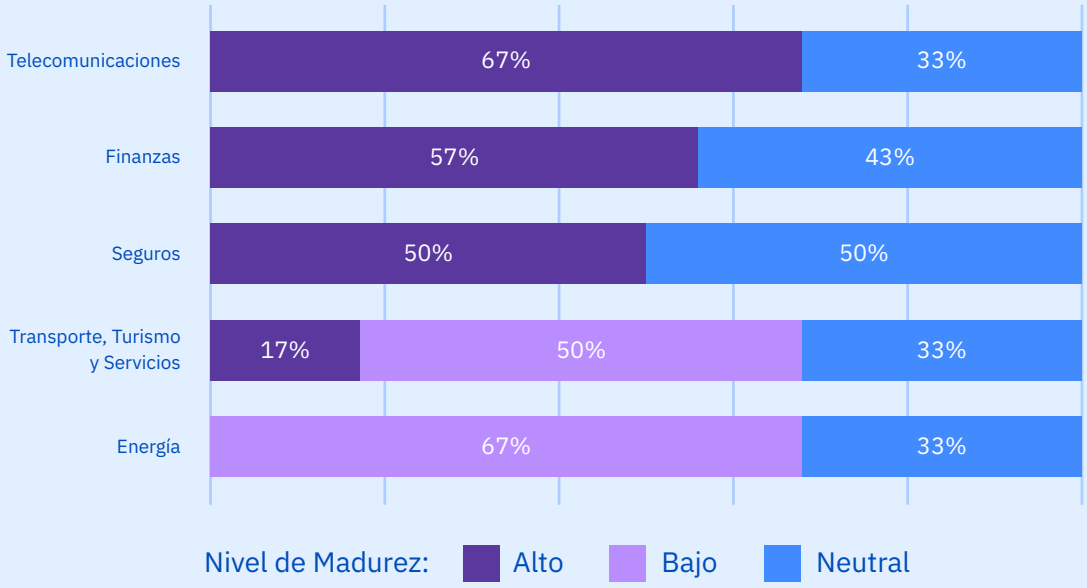
Inventario de activos criptográficos

Un elemento fundamental para poder abordar la transformación de las organizaciones es disponer de un inventario de activos criptográficos (claves, algoritmos, etcétera) adecuadamente contextualizado que proporcione una visión clara y detallada de todos los recursos y sistemas que utilizan criptografía en una organización.

Dicho inventario permite identificar, evaluar y priorizar los componentes que requieren atención y sobre los que deberá evaluarse si es necesario actuar durante el proceso de transformación a Quantum Safe, lo que permitirá ejecutar dicha transformación de manera verdaderamente eficiente y efectiva.

La mayor parte de las compañías encuestadas considera que disponen de un inventario lo suficientemente maduro de sus infraestructuras, información y claves criptográficas. Sin embargo, la experiencia llevada a cabo con diferentes organizaciones permite afirmar que estos inventarios deberán revisarse para incluir en ellos información adicional referida a los algoritmos empleados, el tamaño de las claves, los protocolos y otros datos relevantes como los que se identifican en el estándar CBOM, por sus siglas en inglés *Cryptography Bill Of Materials* (https://github.com/IBM/CBOM). Además, será necesario enriquecer dichos inventarios con información de contexto sobre el uso de la criptografía en sus sistemas y procesos, la clasificación de la información protegida, su nivel de exposición y prioridad frente al desafío que supone el desarrollo de la computación cuántica.

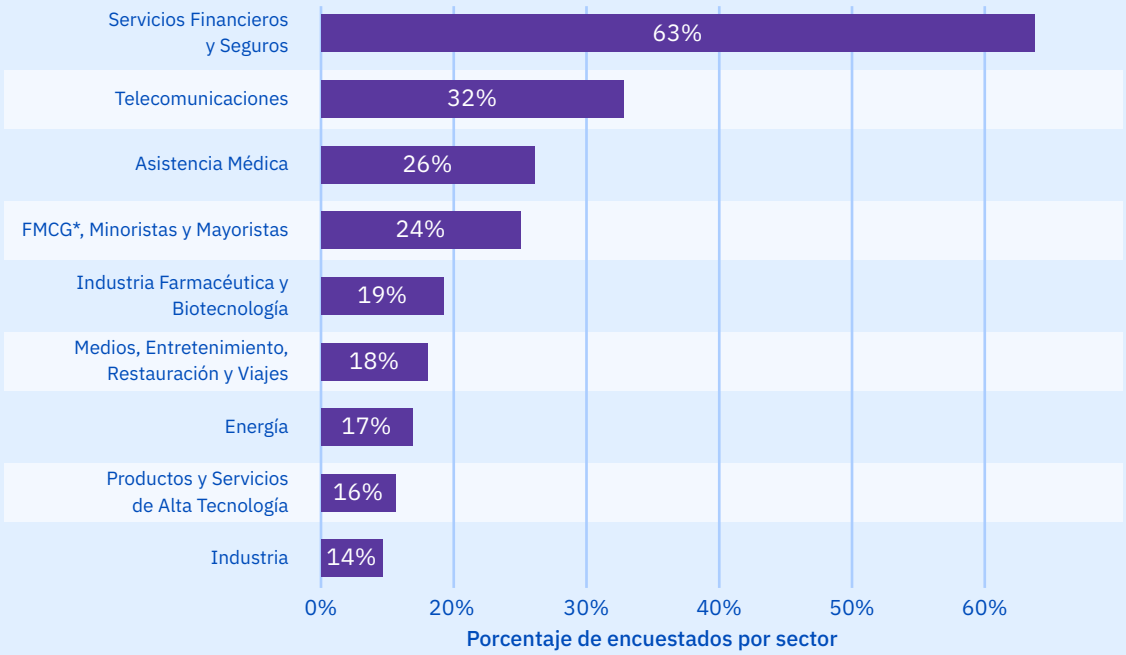
¿Cómo de maduro considera el inventario de estos datos e infraestructuras para que permita identificar aquellos considerados críticos?



Cerca del 40% de las compañías considera la criptografía un elemento crítico dentro de su transformación digital.

Como es lógico, existe una clara relación entre aquellos sectores con una mayor orientación a la digitalización (Financiero, Seguros y Telecomunicaciones) y la importancia que la criptografía tiene dentro de las organizaciones de estos ámbitos.

Sectores más orientados a la digitalización en los que existe mayor interés e inversión



*Bienes de consumo de alta rotación

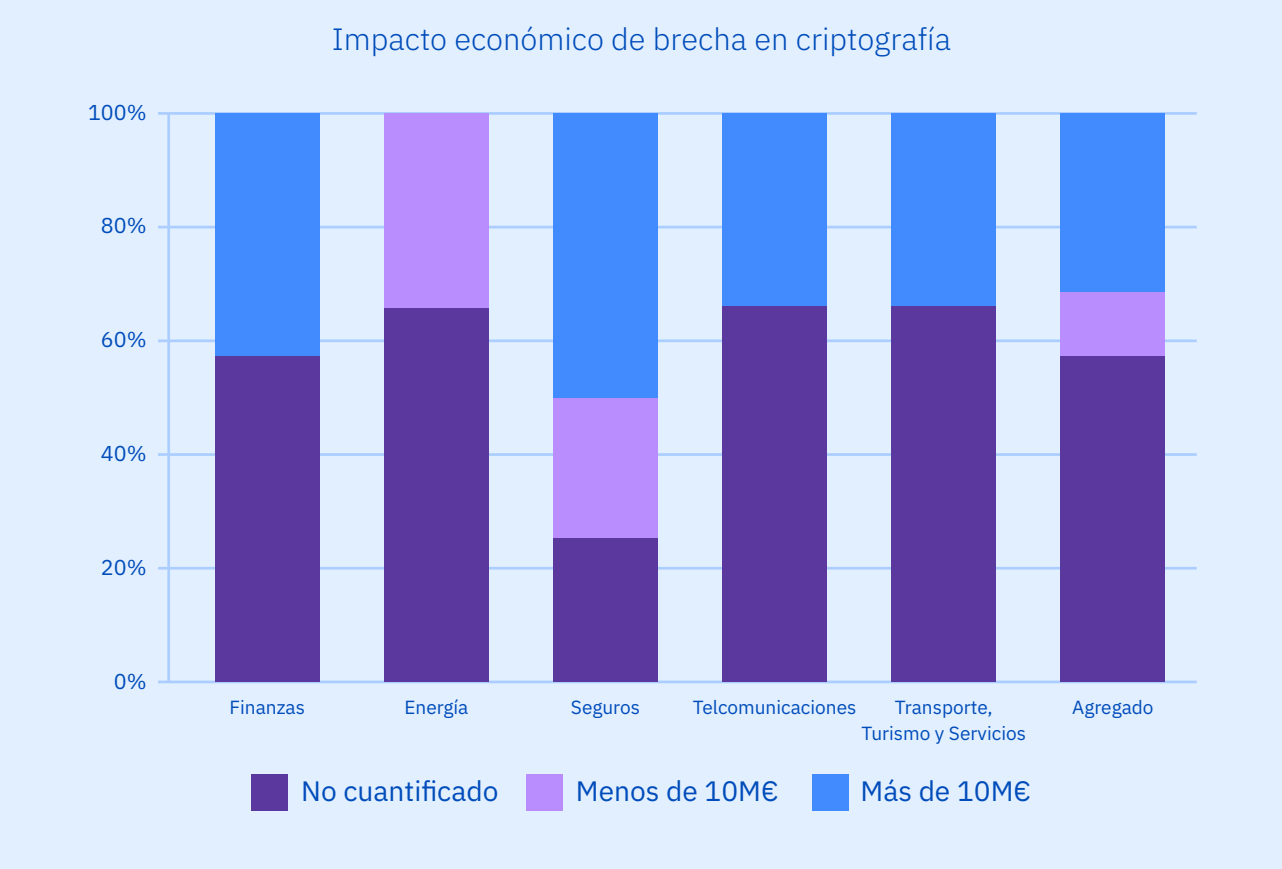
Fuente: The paradox of digital disruption KPMG

www.mapfreglobalrisks.com/gerencia-riesgos-seguros/articulos/las-tech-revolucionan-la-economia/

Estos procesos de transformación digital o digitalización, movimiento de cargas al Cloud, procesos paperless, etcétera suponen escenarios ideales para llevar a cabo un rediseño de la arquitectura criptográfica.

Aprovechar estas iniciativas permite abordar de manera integral el rediseño de las arquitecturas de las aplicaciones de negocio y de la criptografía en un solo proceso, lo que resulta muy eficiente. Al hacer coincidir en el tiempo ambas actuaciones se genera una mayor sinergia, tanto en tiempo como en costes, ya que se puede llevar a cabo la revisión, adaptación y validación de distintos componentes y sistemas en un único cambio.

A pesar del importante papel que la criptografía tiene dentro de la transformación digital, gran parte de los entrevistados de todos los sectores indica no poder cuantificar el impacto económico que produciría una brecha de seguridad criptográfica en su organización, a excepción del sector Seguros, que rompe esta tendencia.



La falta de cuantificación de los posibles impactos dificulta el análisis económico y, por lo tanto, la priorización de las iniciativas relacionadas con la seguridad criptográfica. Es decir, que las organizaciones deben tratar de llevar a cabo dicha cuantificación pese a la dificultad que conlleva, pues los obstáculos que genera son importantes.

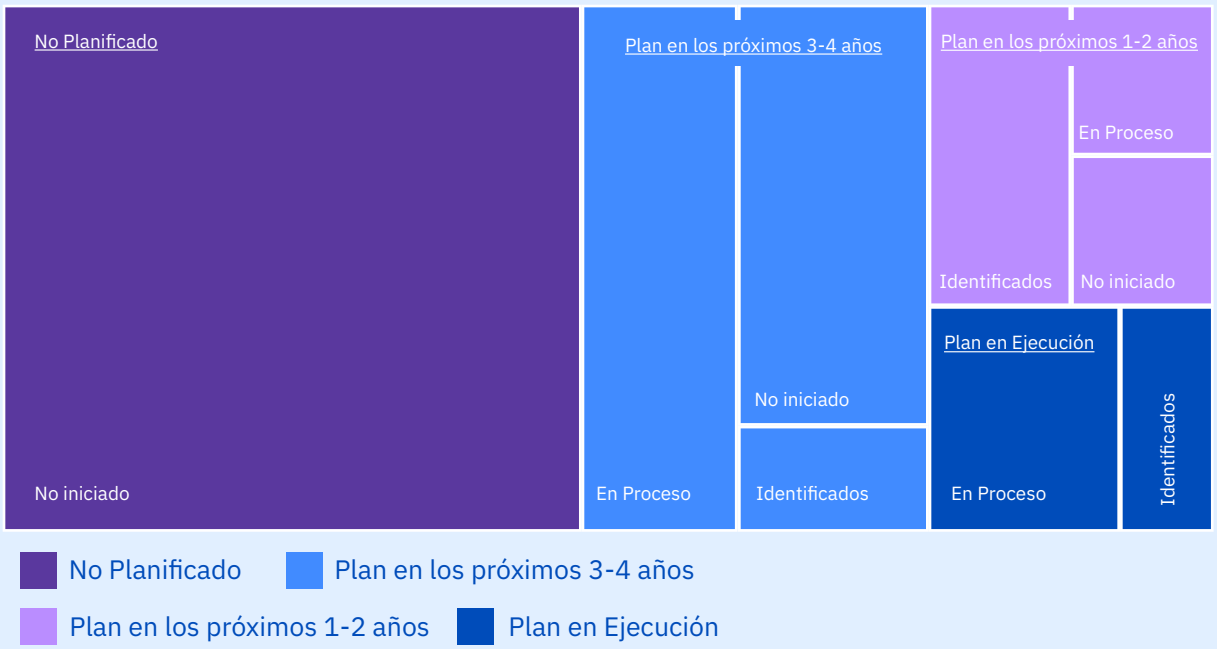
Camino a la transformación

Una de cada cuatro compañías tiene un plan para iniciar su transformación a una organización Quantum Safe en un periodo inferior a 2 años.

A pesar de haber expresado desconocimiento sobre la computación cuántica, casi una cuarta parte de las compañías entrevistadas cree que, desde el punto de vista criptográfico, esta tecnología supone una amenaza que requiere cambiar la forma de encriptar la información que manejan y tienen planes que o bien ya están ejecutando (10% de encuestados) o planean ejecutar en 1 o 2 años (13%). Adicionalmente, un 30% tiene planificado convertirse en Quantum Safe en los próximos 3 o 4 años.

En todos los casos e independientemente de si ya están ejecutando estos planes o proyectan hacerlo en el corto plazo, se ha identificado que el modelo de innovación criptográfica debe llevarse a cabo en colaboración con algún partner con experiencia en este ámbito. Sin embargo, la mayor parte de los entrevistados no ha cerrado con qué proveedores, universidades y/o organismos públicos colaborará en el desarrollo de su plan de transformación para convertirse en Quantum Safe.

Plan Quantum Safe e Identificación de Colaboradores



Entre las compañías entrevistadas, un 23% ya está realizando tareas de descubrimiento de activos, es decir, más que aquellas que ya se están ejecutando su plan para convertirse en Quantum Safe, y un 6% se encuentra ejecutando pruebas de concepto (PoC, por sus siglas en inglés, Proof of Concept) o productos mínimos viables (MVP, por sus siglas en inglés, Minimum Viable Product) de los nuevos algoritmos postcuánticos que el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) estandarizará a lo largo de 2024.

De acuerdo con el estudio, los equipos de Seguridad y Tecnología deben ser los que más se involucren en la definición de la estrategia.

En relación a los perfiles que deben involucrarse en la definición de la estrategia, existe casi unanimidad en incluir a los responsables de Seguridad y Tecnología. Además, 4 de cada 5 compañías encuestadas consideran necesario involucrar al Chief Data Officer (CDO), 2 de cada 3 al Departamento Legal y casi el 50% encuentra necesaria la participación del CEO, de forma directa o a través de la esponsorización del programa de implantación.

Incluso entre aquellas empresas que no cuentan en la actualidad con un plan (un 6% del total), es residual el número de compañías que esperan tener problemas para conseguir el apoyo del Comité de Dirección, lo que indica que, si bien las compañías cuentan con pocos perfiles con conocimiento de computación cuántica, el riesgo que ésta supone para la criptografía sí es conocido.

Todas las compañías encuestadas consideran necesario disponer de un observatorio que informe de las innovaciones y riesgos emergentes en el mundo de la criptografía.

Para la totalidad de las compañías encuestadas (el 45% se mostraba de acuerdo y el 55% totalmente de acuerdo) es necesaria la creación de un organismo, como por ejemplo un observatorio tecnológico, para la monitorización, análisis y divulgación de las innovaciones y riesgos existentes y que surjan en relación con la computación cuántica y la criptografía.

Además, las organizaciones participantes en este estudio consideran que este organismo debe también servir como foro de debate y coordinación entre las diferentes empresas, organizaciones y administraciones públicas para garantizar que esta transformación se lleve a cabo de forma ordenada y con la involucración de todos los actores relevantes.

Líneas de actuación

En este estudio se ha analizado la percepción de las principales empresas españolas sobre el riesgo que supone la computación cuántica para la criptografía moderna. En este sentido, IBM propone que las empresas adopten medidas proactivas de protección contra los riesgos derivados de la computación cuántica y cualquier otra amenaza criptográfica presente o futura. La transformación a un modelo Quantum Safe es un proceso complejo que requiere la colaboración de expertos en múltiples ámbitos, desde la seguridad (especialmente en criptografía) a las infraestructuras, pasando por el desarrollo de aplicaciones.

A continuación, se plantean una serie de recomendaciones iniciales que IBM considera que las organizaciones deben llevar a cabo para comenzar su transformación a Quantum Safe. Esta acciones se pueden clasificar en dos grandes clases: aquella comunes que deben desarrollarse de forma colectiva para asegurar que las medidas funcionan y aquellas otras que deben realizar las organizaciones como iniciativas propias:

Acciones comunes y colectivas

- **Fomentar el talento** mediante campañas de concienciación sobre la importancia de la criptografía en los procesos de negocio y los retos criptográficos generados. Este conocimiento es fundamental para entender y evaluar los riesgos que representa la computación cuántica sobre la criptografía para las organizaciones.

  La computación cuántica está en constante evolución y se espera que siga siendo así en el futuro más inmediato, por lo que es imprescindible mantenerse al día con las últimas tendencias y riesgos potenciales. Esto permitirá ir adaptando los planes de transformación a la criptografía resistente a la computación cuántica en función de las particularidades de cada sector.

- **Creación de un observatorio,** cuya misión sea monitorizar y analizar las últimas tendencias sobre la tecnología cuántica en diferentes ámbitos como son la evolución de los ordenadores cuánticos, la corrección de errores o las mejoras en la implantación de los algoritmos de Shor y Grover. También deberá llevar a cabo actividades para analizar el impacto que estos cambios pueden tener en el ámbito de la criptografía y la ciberseguridad en general para los diferentes sectores y organizaciones.

  Este observatorio debe actuar como un punto de contacto entre diferentes actores (universidades, empresas, startups, organismos de investigación, gobiernos, etcétera) para fomentar la colaboración, la coordinación de acciones y el intercambio de conocimientos entre sus miembros. Dichos conocimientos se deberán también difundir mediante publicaciones, eventos, conferencias, cursos, etcétera para sensibilizar y concienciar sobre los potenciales riesgos derivados de este nuevo modelo de computación al conjunto de la sociedad.

Acciones propias de cada organización:

- **Realizar un assessment inicial**, que permita conocer cuál es su nivel de exposición actual (AsIs) respecto a la criptografía en sus diferentes dominios como políticas y procesos, gestión de claves, el cifrado de las comunicaciones o las infraestructuras de clave pública.

  Con este punto de partida, las organizaciones podrán definir cuál quieren que sea su estado futuro (ToBe) y las iniciativas (proyectos, actividades, etcétera) que necesitan ejecutar para alcanzarlo.

  Disponer de una hoja de ruta claramente definida y priorizada es esencial para que los diferentes equipos de trabajo conozcan cuáles serán sus focos de actuación, el presupuesto necesario para poder ejecutarlos correctamente y los *partners* adecuados.

- **Inventario de activos criptográficos**, esencial para una organización que busca protegerse contra los riesgos derivados de la computación cuántica, al proporcionar múltiples ventajas directas desde su implantación:

  - Ayuda a identificar los activos críticos de la organización que deben ser protegidos contra ataques criptográficos, especialmente aquellos relacionados con los algoritmos no resistentes a este nuevo tipo de computación. Esto incluye información confidencial y/o crítica como datos de clientes, información financiera o propiedad intelectual, entre otros.

  - Contribuye a evaluar las vulnerabilidades de la organización en términos de criptografía e identificar las áreas que necesitan mejoras en la seguridad, no únicamente relacionadas con algoritmos Quantum Safe. Esto ayuda a la organización a focalizarse en las áreas más críticas y a tomar medidas para mitigar o resolver dichas vulnerabilidades.

  - Ayuda a seleccionar soluciones criptográficas adecuadas para la organización, incluyendo la elección de algoritmos de cifrado, protocolos de comunicación segura y otras soluciones criptográficas resistentes a los ataques cuánticos a partir de las necesidades de cada uno de los procesos de negocio.

  - Permite conocer, de forma automática y en cada momento, los algoritmos, claves y protocolos utilizados por las aplicaciones de negocio facilitando así verificar el cumplimiento de las políticas criptográficas de la organización, detectando vulnerabilidades motivadas por posibles errores de implantación o configuración e incrementando las capacidades Crypto-agility de la organización.

  - Facilita a la organización cumplir con los procesos de certificación de las diferentes regulaciones y normativas relativas a ciberseguridad y criptografía (por ejemplo, el estándar PCI), ya que disponer de esta información correctamente inventariada y centralizada permite automatizar la obtención de evidencias. Además, cada vez que estas normativas se actualizan y exigen cambios sobre los elementos criptográficos pueden identificarse con agilidad para su adaptación.

  - Posibilita responder de manera más efectiva a los incidentes de seguridad que puedan sufrir las organizaciones al permitir la identificación de los activos afectados, la evaluación de la gravedad del incidente y la implementación de medidas automatizadas para mitigar el daño y prevenir futuros incidentes (por ejemplo, realizar un rotado de claves de cifrado).

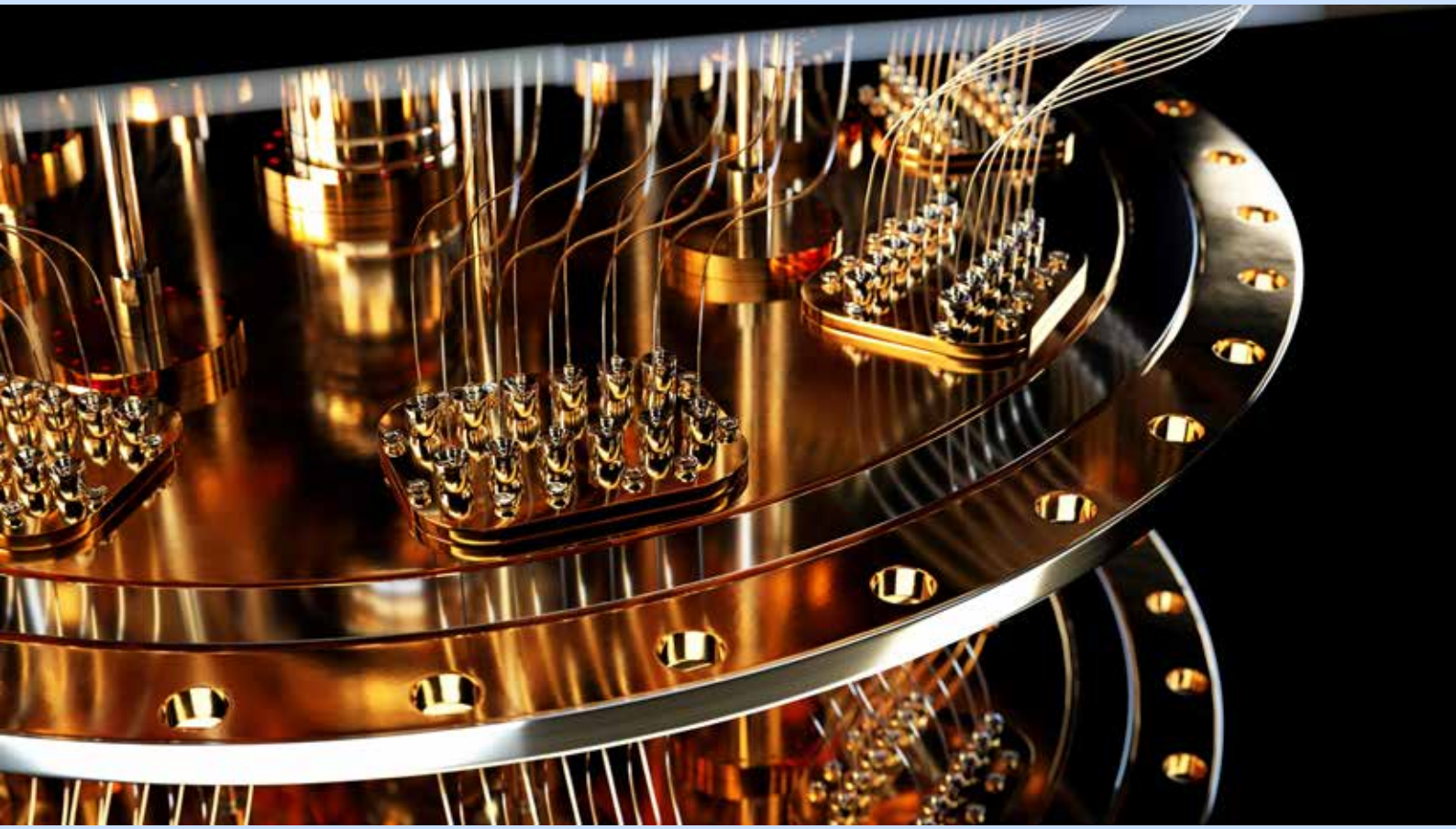
- **Transformar la arquitectura criptográfica de las aplicaciones**, pasando de un modelo en el que la criptografía es un componente o librería embebido dentro de las aplicaciones de negocio a otro en el que se convierte en un microservicio consumible por dichas aplicaciones.

La velocidad de desarrollo tecnológico y la creciente complejidad de las aplicaciones de negocio obliga al uso de soluciones criptográficas flexibles y escalables, que permitan integrar fácilmente nuevas tecnologías y soluciones de criptografía como son los futuros algoritmos Quantum Safe.

Es importante destacar que también las regulaciones y normativas en materia de ciberseguridad y privacidad están en constante evolución, y las empresas deben adaptarse a estos cambios para poder cumplir con las leyes y normas aplicables. Un modelo de *Crypto as a Service* permite a las empresas adaptarse rápidamente a cambios en las regulaciones y normativas, garantizando la conformidad y evitando posibles sanciones.

Adicionalmente, el modelo criptográfico facilita una segregación de funciones entre los equipos de desarrollo, responsables de la creación y el mantenimiento de las aplicaciones de negocio, y el equipo de criptografía que será responsable de la generación y custodia de las claves necesarias, publicación de los servicios criptográficos o el control de acceso a los mismos.

En este sentido, desde IBM Consulting vamos a seguir trabajando para profundizar en los aspectos clave que permitan a las organizaciones ejecutar un programa de transformación de estas características. Estamos comprometidos con la innovación y el desarrollo de soluciones seguras y eficientes para enfrentar los desafíos que plantea el avance de la criptografía postcuántica.



Sobre los autores

José Cándido Carballido López,

CTO Cybersecurity Services SPGI

IBM Consulting

jccarballidol@es.ibm.com

CTO de los Servicios de Ciber Seguridad de SPGI para IBM Consulting, cuenta con más de 15 años de experiencia en el diseño de arquitecturas y ejecución de programas complejos de ciberseguridad. Líder técnico de los proyectos que ayudan a comprender los riesgos cuánticos, priorizar acciones de mitigación y ejecutar programas de transformación criptográfica a largo plazo.

David Quero Callado,

Senior Manager Consultant

IBM Consulting

david.quero@es.ibm.com

Quantum Ambassador de IBM con más de 20 años de experiencia implementando proyectos de tecnología en entornos corporativos complejos. Se encuentra especializado en implantaciones de tecnología innovadora.

Carlos Creus Olgado,

Cybersecurity Services Market Leader

IBM Consulting

carlos.creus@es.ibm.com

Responsable de los Servicios de Ciber Seguridad en IBM Consulting, ha desarrollado su carrera alrededor del mundo del dato y la inteligencia artificial, habiendo liderado distintos proyectos de transformación en algunas de las principales empresas del país. Ha sido punta de lanza en el desarrollo de nuevos modelos operativos y la adopción de tecnologías emergentes por parte de los negocios.

Colaboradores en la realización del documento:

- **Ginés Carrascal de las Heras,** Computational Scientist and Architect - IBM Quantum
- **Bryan Ramírez Correa,** Data Scientist
- **Daniel Horcajo de la Cruz,** Senior Data Scientist
- **Enrique Vasallo Fernández,** IA and Data Analist
- **Patricia Samper,** Associate Consultant

Por último, IBM Consulting quiere expresar su más sincero agradecimiento a todos los participantes en el estudio. Su tiempo, conocimiento y dedicación han sido fundamentales para el éxito de este proyecto.

IBM **Consulting**

Cybersecurity Services