PROSEGUR RESEARCH

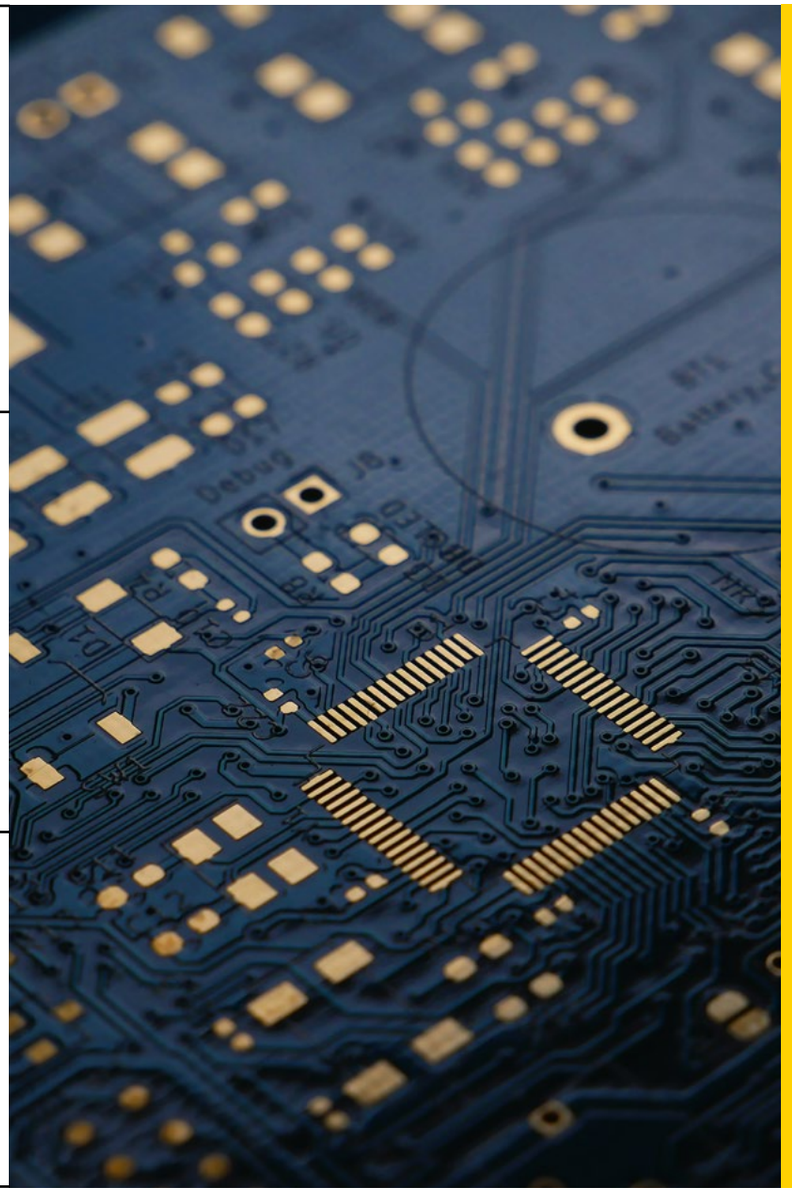
Highlights

Computación cuántica: out of the box

PROSEGUR

PROSEGUR RESEARCH
Highlights

Contenidos



01

Anatomía de lo imposible

PROSEGUR RESEARCH

Highlights

La constante evolución digital presente en nuestra sociedad, entendiéndola como un proceso de desarrollo de **herramientas y técnicas centradas en mejorar los medios de las personas,** mantiene activos numerosos frentes de innovación y progreso tecnológico. Entre estos se encuentra la conocida como **computación cuántica,** considerada por la **OTAN** – entre otras instituciones – como una de las tecnologías emergentes más prometedoras que existe en la actualidad.

De hecho, la potencia e impulso que tendrá esta tecnología supondrá una **revolución** en la forma en la que procesamos y almacenamos la información, que **se estima que alcanzará su culmen en el año 2035** con una **proyección de más de 2.000 zettabytes de información a nivel global,** cuando se pretende contar con hardware y software capaces de controlar estos sistemas.

A **Pero ¿qué es exactamente la computación cuántica y por qué es tan revolucionaria?**

Puede afirmarse que el concepto de computación cuántica nace con Richard Feynman, físico estadounidense que, en un importante **paper** publicado en el año 1982, introdujo la idea de **crear un entorno basado en la mecánica cuántica a fin de poder resolver algoritmos complejos o imposibles** para los ordenadores convencionales. Así pues, atendiendo al concepto de computación cuántica ofrecido por **IBM,** esta tecnología hace referencia a un **sistema informático que, basándose en principios físicos de la mecánica cuántica, ofrece la posibilidad de desarrollar o resolver problemas y algoritmos de elevada complejidad.**

PROSEGUR RESEARCH
Highlights

En palabras de Seth Lloyd – en su libro *Programando el universo*[1] – la **computación clásica** es una voz **solista,** en la que una serie de tonos suceden al anterior, mientras que la **computación cuántica** es una **sinfonía:** un sistema en el que los elementos se entrelazan, interfieren y complementan entre sí.

B ¿Cómo se pueden resolver ahora cálculos antes considerados imposibles?

Su fundamento radica en una **nueva aproximación a las unidades mínimas en las que se basa la lógica computacional,** los bits, los cuales pueden configurarse como ceros o unos. A diferencia de la computación clásica, la computación cuántica utiliza **qubits** (*quantum bits,* en inglés), que pueden representar el 0, el 1 o una teórica superposición simultánea gracias a un fenómeno llamado **superposición cuántica.** Además, los qubits pueden estar **entrelazados,** lo que significa que el estado de un qubit puede depender del estado de otro, **interaccionando e interfiriendo entre sí** y ofreciendo la posibilidad de **ejecutar algoritmos multidimensionales.**

De este modo, los qubits se pueden representar metafóricamente como **interruptores** que pueden estar apagados, encendidos o en una posible superposición al mismo tiempo, de la misma manera que no se puede saber si un dormitorio tiene o no luz hasta el momento que se accede a su interior.

C ¿Y esto qué implica?

La computación cuántica se desenvuelve en un **dominio extraordinariamente más extenso** que la computación clásica. Mientras que la clásica realiza cálculos individuales que llevan a resultados únicos y un solo cambio en alguna de las variables produce una nueva operación, **el sistema cuántico genera un abanico de resultados procesando numerosas operaciones de forma simultánea y más rápida.** Siguiendo la analogía de Aaronson y Weinersmith[2], la computación cuántica se basa en una coreografía en la que **los caminos que llevan a respuestas incorrectas interfieren y se cancelan entre sí, mientras que los caminos correctos se refuerzan,** aumentando la capacidad de los ordenadores en determinados problemas concretos.

---

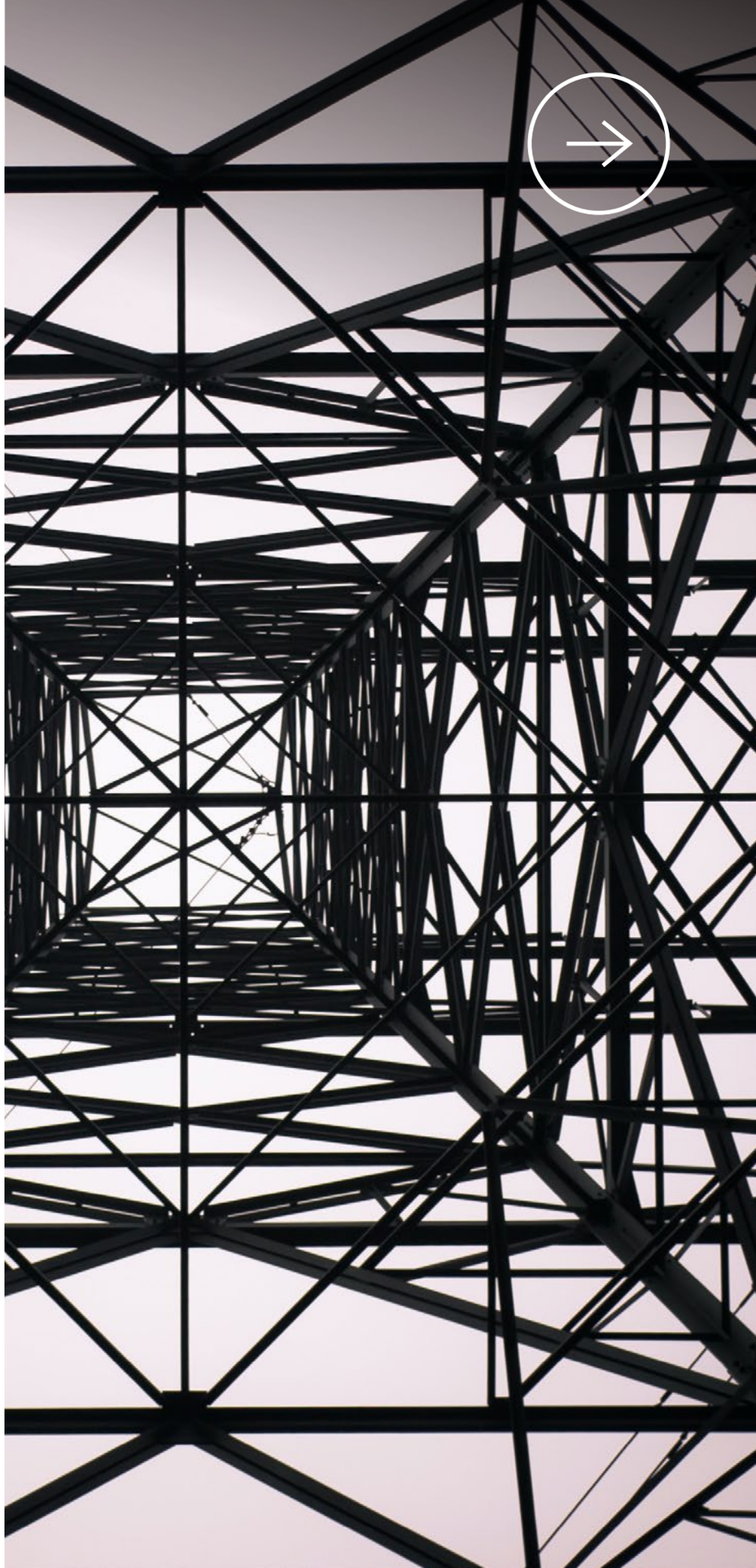
[1] Véase la **versión original:** *Programming the Universe: a quantum computer scientist takes on the Cosmos.*
[2] Véase **The Talk.**

PROSEGUR RESEARCH

Highlights

Todo ello, junto a su reducido tamaño, permite precisar de un **menor consumo de energía** con respecto a la tecnología más parecida que existe en la actualidad: los superordenadores. No obstante, **no se debe reducir la computación cuántica a una simple mejora en la velocidad de procesamiento,** puesto que pueden existir determinadas tareas para los que un ordenador convencional sea más eficiente.

Por tanto, dada la potencial repercusión que esta extraordinaria revolución de lo antes considerado imposible presenta para nuestra sociedad, desde **Prosegur Research** analizamos sus posibles **implicaciones para el futuro,** tanto en avances para el progreso como en aspectos a considerar en su seguridad para que ese avance sea positivo.



02

Del qubit a la revolución de las oportunidades

PROSEGUR RESEARCH

Highlights

Los científicos informáticos consideran que, para visualizar el **verdadero potencial de los ordenadores cuánticos,** estos deben de incluir la capacidad de **1 millón de qubits.** A fecha actual, junio de 2023, la computadora que más se aproxima a dicha cifra es Osprey de IBM, con 433 qubits. No obstante, un **estudio** reciente ha constatado que, aunque de forma restringida, un ordenador cuántico de tan solo 127 qubits es capaz de superar las capacidades de un superordenador de última generación. Por otro lado, si bien es cierto que se han desarrollado sistemas con hasta una arquitectura de 5.000 qubits, como el Advantage System de D-Wave, algunos autores consideran que no se trata de computación cuántica[3], puesto que no actúan como ordenadores de propósito general – capaces de realizar diversas tareas y operaciones –.

El principal escollo para la máxima explotación del potencial cuántico se debe a que, hasta el momento, **la tecnología desarrollada no tiene la capacidad suficiente como para controlar estos sistemas,** provocando **situaciones de inestabilidad** cuando se realizan operaciones más sofisticadas. Así, los **desafíos** que esta tecnología presenta en la actualidad son diversos:

Gráfico 1
Desafíos de la computación cuántica en la actualidad

01 **Mejorar la estabilización y error** que presentan los qubits para así aumentar su cantidad en los procesos.

02 **El desarrollo de herramientas y técnicas** de programación y software capaces de adaptarse a la aplicación cuántica.

03 **La reducción del coste** que supone la construcción y mantenimiento de estas computadoras, pues actualmente se requiere una gran capacidad financiera para involucrarse en este tipo de proyectos.

Fuente: Prosegur Research, 2023 basado en KPMG

[3] Véase **Protocol.**

No obstante, a pesar del gran margen de mejora, la computación cuántica presenta en la actualidad **enormes beneficios[4],** cubriendo así un **amplio abanico dominios y ofreciendo aplicaciones** en planos de diversa índole. Algunos de las principales aplicaciones son la optimización de procesos y creación de nuevos modelos o materiales, ciberseguridad mejorada en la creación de protocolos de encriptación más avanzados, descubrimiento de nuevos medicamentos, mejora en las capacidades de la inteligencia artificial, o mejora en la operatividad de la logística y el transporte, entre otros.

[4] Véase **Telos.**
[5] Véase **Supervisor Europeo de Protección de Datos** (SEPD).
[6] Véase **Airbus.**
[7] Véase **IEEE – Spectrum.**

Beneficios y oportunidades que puede brindar la computación cuántica

1 Criptografía: privacidad en alza

La computación cuántica tiene el potencial de **reforzar la seguridad** al proporcionar la capacidad de crear algoritmos y protocolos más complejos, lo que se erige como un pilar fundamental tanto en el ámbito militar como civil, donde resulta de especial interés en materia de protección de **datos personales[5].**

2 Optimización de procesos en múltiples industrias

La computación cuántica puede ayudar a abordar problemas de optimización complejos, **explorando soluciones de forma más eficiente y encontrando resultados óptimos más rápido y de mayor diversidad.** Así, esta optimización se prevé que tenga un gran impacto en operaciones relacionadas con la **simulación,** como la **planificación de rutas aeronáuticas** o la elaboración de **procesos químicos.** En el corto plazo, puede tener un gran impacto en el sector aeronáutico[6] y energético[7]. En último término, la optimización de procesos puede derivar en una notable **reducción de costes** para las empresas.

PROSEGUR RESEARCH
Highlights

3 Aprendizaje automático e inteligencia artificial: convergencia tecnológica

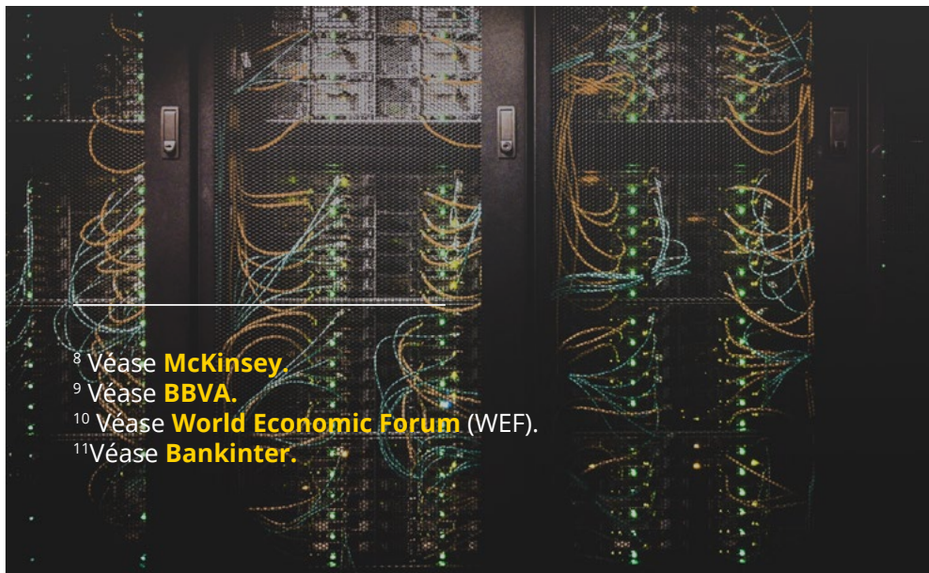
La computación cuántica puede mejorar los algoritmos de aprendizaje automático y ofrecer nuevas técnicas para **analizar grandes conjuntos de datos y reconocer patrones complejos,** aumentando las capacidades de la convergencia tecnológica en la actualidad. Esto puede llevar a avances en aplicaciones como el **diagnóstico médico,** la **traducción automática** y, en general, en las **capacidades de instrumentos electrónicos** que hagan uso de la inteligencia artificial; de especial interés para el **desarrollo armamentístico**.

4 Gestión de riesgos y escenarios: creatividad potenciada

La computación cuántica puede mejorar el análisis y la gestión de riesgos mediante su capacidad para **medir e interconectar una gran cantidad de variables con un alto grado de incertidumbre,** así como por la consideración y elaboración de múltiples **escenarios.** Esta aplicación puede aplicarse en diversos contextos, entre los que se destaca, por su potencial mayor beneficio, el **análisis financiero[8].**

5 La sostenibilidad como eje de futuro

La **preservación de los ecosistemas** y la acción contra el desafío climático debe ser una de las mayores líneas de actuación para casi todas las compañías del mundo. Al respecto, la computación cuántica puede beneficiar a numerosos sectores como la **industria energética y los data center,** utilizando menos consumo para mantener su funcionamiento[9], la **investigación y la industria química,** en la búsqueda de nuevos fertilizantes y diversos catalizadores que disminuyan las emisiones de CO2 a la atmósfera[10], o el **sector automovilístico,** en la simulación de nuevos modelos de electrólisis de agua para generar hidrógeno verde y, además, diseñar nuevas baterías con más potencia de almacenamiento[11].



[8] Véase **McKinsey.**
[9] Véase **BBVA.**
[10] Véase **World Economic Forum** (WEF).
[11] Véase **Bankinter.**

PROSEGUR RESEARCH
Highlights

“La computación cuántica es como un territorio inexplorado que ofrece multitud de aplicaciones a la espera de ser descubiertas.”

David Sadek
Doctor en Computer Science

03

Hotspots de seguridad relacionados con computación cuántica

PROSEGUR RESEARCH

Highlights

Por sus características técnicas, la computación cuántica presenta una serie de **importantes bondades** pero también de **riesgos y amenazas propios.** Adicionalmente, como todo avance tecnológico, **ayuda al empoderamiento de la ciudadanía,** desde sus aplicaciones para cubrir necesidades de particulares o **potenciar negocios** de empresas y sectores hasta el **aprovechamiento criminal de su uso.**

EN SU **DISEÑO**

Precisión cuántica

Los qubits son frágiles y propensos a errores debido a diversos factores, como las interacciones con el entorno y los efectos de la decoherencia, que produce la pérdida del entrelazamiento cuántico y genera un estado físico clásico – sin entrelazamiento –. Estos errores cuánticos pueden propagarse **y deteriorar la precisión y la confianza de los cálculos cuánticos;** consecuentemente, esto es susceptible de generar un elevado impacto en áreas donde la precisión es decisiva, como en el diseño de medicamentos o en la toma de decisiones financieras[12].

Sensación térmica -273º

Un ordenador cuántico necesita unas condiciones específicas de temperatura ambiente próxima al cero absoluto (-273 °C) y aislarse del campo magnético terrestre para evitar que los átomos se muevan y colisionen entre sí o interactúen con el entorno. A la particularidad de estas condiciones se le suma que, para lograrlas, el sistema cuántico necesita hacer uso de helio[13]. Así, en este sentido cobran importancia los **riesgos asociados a la cadena de suministro del computador cuántico,** donde junto a la complejidad de la infraestructura, las posibles alteraciones en el **abastecimiento de helio** – como la escasez o las fluctuaciones de precios – suponen un riesgo para la operatividad de estas máquinas y sus operadores.

[12] Véase **Medium.**
[13] Véase **IBM.**

Latencia legislativa

El **habitual letargo legal con respecto a la regulación de tecnologías emergentes** puede materializarse en el caso de la computación cuántica. Teniendo en cuenta su rápido desarrollo y potenciales capacidades, la ausencia de marcos reguladores adecuados a su implementación y uso podría permitir **abusos o prácticas irresponsables** que afecten a la **privacidad, seguridad y derechos humanos**[14]**.** Sin un marco regulatorio sólido, el riesgo de que actores estatales y no estatales utilicen esta tecnología de manera agresiva y sin restricciones se potencia, **aumentando la vulnerabilidad** de los sistemas expuestos.

EN SU **IMPLEMENTACIÓN**

Convergencia existencial

Aunque se han logrado avances significativos en la construcción de computadoras cuánticas, todavía hay desafíos importantes para hacerlas prácticas y accesibles. Los sistemas cuánticos actuales se enfrentan a problemas como la decoherencia, la falta de estabilidad y la **alta sensibilidad a las interferencias externas.** Además, la disponibilidad y el acceso a la computación cuántica es limitado y está muy restringido, ya que los sistemas cuánticos se encuentran en una **etapa temprana de desarrollo** – para lo cual es necesario contar con unos medios tecnológicos de alto nivel–, lo que deriva en que estos se encuentren en manos de un número limitado de organizaciones[15].

Asimetría cuántica

Bien por su mencionado desarrollo prohibitivo para la mayoría de actores o bien por su elevado coste final de adquisición, la **adopción de la computación cuántica de forma asimétrica** entre usuarios, empresas e instituciones puede provocar situaciones

[14] Véase **Supervisor Europeo de Protección de Datos** (SEPD).
[15] Véase **The Quantum Insider.**

de desigualdad en el mercado y el orden socioeconómico. Además, esta **brecha tecnológica** puede ser explotada por las capacidades maliciosas de la computación cuántica, acentuando esta desigualdad en el apartado de la seguridad, potenciando la vulnerabilidad de entidades o consumidores que no hayan adoptado esta tecnología y creando situaciones de privilegio a la hora de acceder a los recursos y beneficios derivados de su uso.

Superordenadores necesitan superempleados

A medida que la computación cuántica avanza y se convierte en una realidad tangible, **la demanda de profesionales altamente capacitados superará a la oferta en el caso de que esta no se adapte al ritmo de desarrollo.** Esta falta de talento cualificado con conocimientos podría **obstaculizar la implementación efectiva** y el desarrollo de aplicaciones cuánticas en diversos campos, desde la investigación científica hasta la industria y la seguridad nacional. Adicionalmente, la ausencia de profesionales debidamente capacitados potencia el **riesgo de implementar soluciones defectuosas** que podrían ser explotadas por actores malintencionados o que simplemente no cumplan con los estándares de seguridad requeridos.

EN SU **USO**

Integridad de las comunicaciones

La economía global de Internet depende de la criptografía como elemento base para una red segura, sistema que, hasta la fecha, se muestra vulnerable a las capacidades de la computación cuántica. Así, la existencia de una tecnología que permite la posibilidad de **vulnerar de forma rápida los sistemas de encriptado tradicionales,** unido a la inexistencia de nuevas metodologías capaces de dar respuesta a esta situación, supone un elevado riesgo tanto para la seguridad de los usuarios como de toda la infraestructura informática[16].

[16] Véase **IBM.**

PROSEGUR RESEARCH

Highlights

Privacidad de los qubits

Dado su valor en la sociedad actual, la vulneración de los sistemas de encriptado puede tener como uno de sus principales objetivos la **obtención de información protegida[17].** En este sentido, la protección de los datos personales se ve expuesta a una mayor amenaza, pues la **información sensible almacenada o transmitida estaría expuesta a accesos no autorizados,** lo que puede tener un severo impacto sobre sectores que gestionan los datos personales de mayor valor, como la banca, el comercio electrónico o la sanidad.

Hacking cuántico

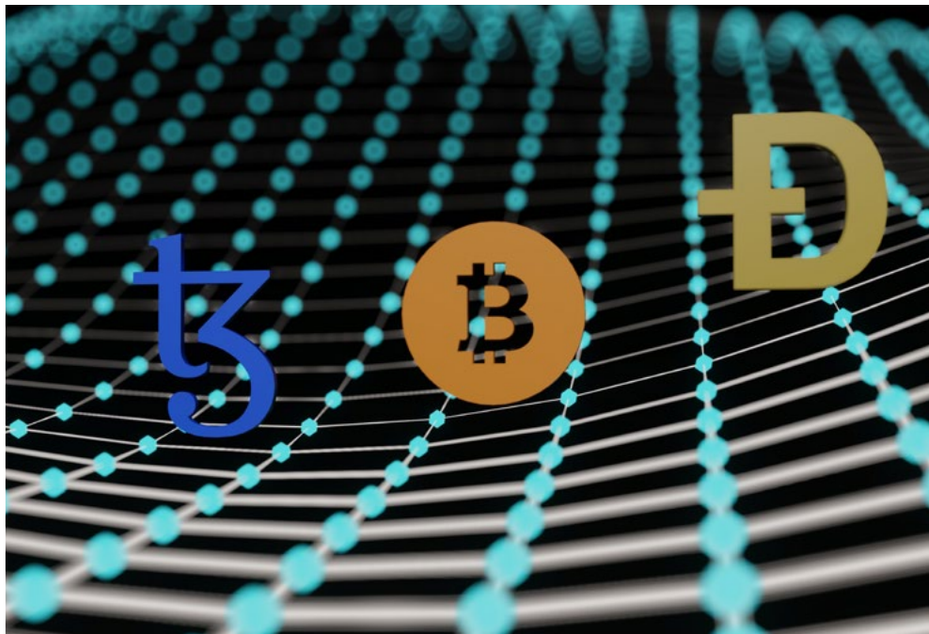
El uso de sistemas cuánticos ofrece mayores capacidades a la hora de llevar a cabo **hackeos contra sistemas informáticos** más allá del apartado criptográfico. Las técnicas de computación cuántica para explotar vulnerabilidades son superiores a las que ofrece un computador clásico, generando una amenaza de mayor impacto dada la **menor capacidad de detección y análisis** que ofrecen los sistemas de defensa actuales[18].

Seguridad del blockchain

Las capacidades de la computación cuántica también pueden poner en riesgo el núcleo del éxito de la tecnología blockchain: su seguridad. La **vulneración de su encriptado y posterior manipulación maliciosa** puede suponer no solo el declive de esta tecnología, sino un gran riesgo para empresas y usuarios que hagan uso de esta. Por ejemplo, actualmente se estima que un **25% de las criptomonedas** en circulación –basadas en el blockchain– estarían altamente expuestas a un robo perpetrado a través de un ordenador cuántico.

---

[17] Véase **Supervisor Europeo de Protección de Datos** (SEPD).
[18] Véase **Cloud Security Alliance.**



PROSEGUR RESEARCH
Highlights

Incertidumbre multidimensional

El mayor riesgo de la tecnología cuántica es su carácter imprevisible. **El desconocimiento y la incapacidad para medir completamente sus capacidades impide realizar previsiones completas y eficaces sobre las potenciales amenazas e implicaciones derivadas de sus usos maliciosos** en la enorme variedad de campos de aplicación. Por este motivo, el posible desarrollo **de nuevos modus operandi criminales** a la seguridad de los usuarios y de toda la industria resultarán particularmente difíciles de detectar[19].

[19] Véase **Forbes.**

PROSEGUR RESEARCH

Highlights

Como se ha puesto de manifiesto, la computación cuántica es una auténtica revolución de lo imposible, y nos presenta un **futuro prometedor** gracias a los trascendentes avances técnicos que nos permitirá alcanzar, antes impensables. En ellos, está implícito el **empoderamiento tecnológico de los humanos con visión de seguridad,** y también un **impacto positivo** desde un enfoque sistémico, que deriva del buen hacer de tecnólogos, empresarios, legisladores y de la ciudadanía en su conjunto.

Generar **ecosistemas de responsabilidad** integrando las perspectivas y necesidades de todos los stakeholders involucrados, así como promover la **sostenibilidad en cada paso** para hacer del avance una verdadera contribución al bienestar global serán dos desafíos clave de ese futuro positivo.

PROSEGUR

Garantizamos la seguridad de las personas, las empresas y la sociedad en su conjunto.

research@prosegur.com PROSEGUR RESEARCH www.prosegurresearch.com