Preparados para el futuro

La transición hacia la seguridad poscuántica

Informe de Vanguard

Abril de 2022

Encargado por

IBM

451 Research

S&P Global
Market Intelligence

Sobre el autor

John Abbott

Analista de investigación principal de 4SIGHT

John Abbott cubre temas relacionados con infraestructura de sistemas, almacenamiento y software para 451 Research, una empresa propiedad de S&P Global Market Intelligence. A lo largo de sus más de 30 años de carrera, ha sido pionero en la cobertura de contenidos tecnológicos especializados en áreas como Unix, la supercomputación, la arquitectura de sistemas, el desarrollo de software y el almacenamiento.

Tras cofundar The 451 Group en octubre de 1999, John empezó a dirigir las operaciones de análisis desde la oficina de la empresa en San Francisco. Ha figurado como autor principal en muchos de los informes especiales de 451 Research, incluidos aquellos relativos a la virtualización de almacenamiento y los servidores de cuchilla, los cuales fueron los primeros estudios exhaustivos que se publicaron sobre estos temas. Más recientemente, se ha centrado en temas como la infraestructura convergente, las nuevas arquitecturas de sistema, la IA y los aceleradores de aprendizaje profundo. John contribuyó a establecer 4SIGHT, la infraestructura de 451 Research orientada a la cobertura vanguardista y a largo plazo de las tecnologías emergentes.

Comenzó a cubrir el sector tecnológico en 1984, apoyándose en su trayectoria previa como autor técnico y en su experiencia directa en el uso de sistemas principales, los primeros PC y las estaciones de trabajo de Unix. Ha colaborado como periodista independiente en publicaciones como ***Computing***, ***Computer Weekly***, ***The Financial Times*** y ***The Times***. En 1987 fue nombrado editor de ***Unigram.X***, el boletín semanal sobre Unix de ComputerWire, y posteriormente se convirtió en editor del servicio diario ***Computergram International*** de la empresa, primero en Londres y después en San Francisco. Estableció la oficina de 451 Research en San Francisco y ha vivido en esa ciudad durante más de una década.

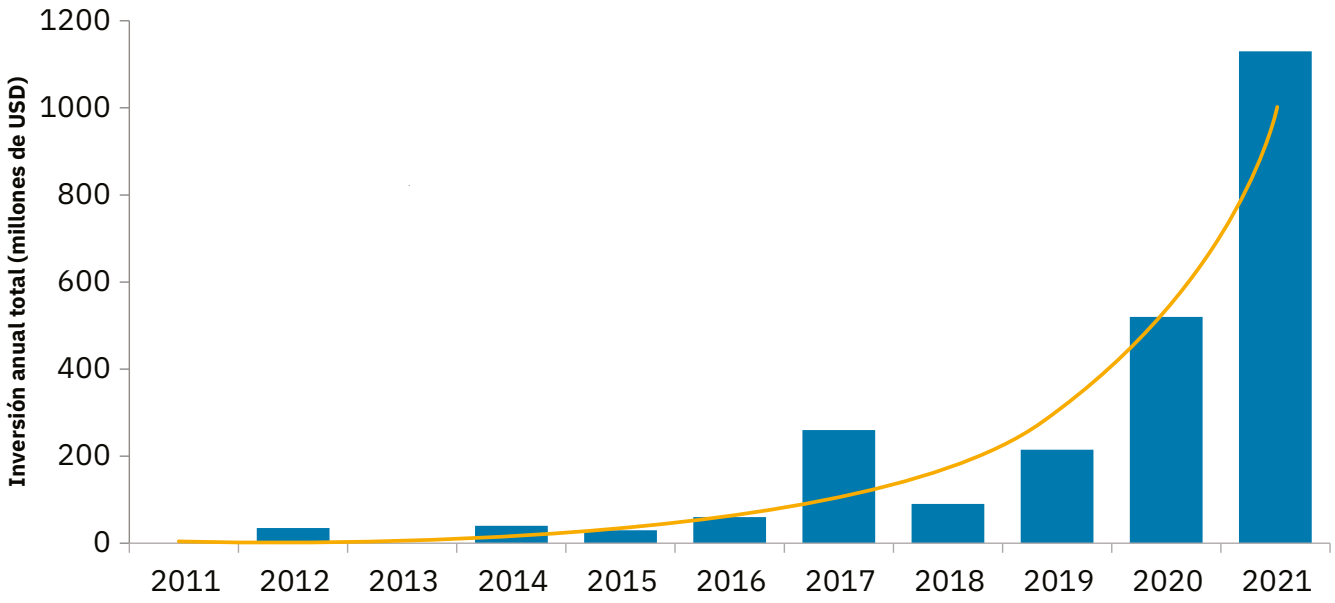
John estudió música en la Universidad de Keele y tiene un máster en Literatura Inglesa Moderna por la Universidad de Londres.

Introducción

Actualmente, la computación cuántica podría describirse como una inversión de alto riesgo y alto retorno. No existe ninguna garantía de que crear un sistema cuántico universal y práctico sea factible en nuestros tiempos. Sin embargo, los laboratorios de investigación —y cada vez más empresas privadas del sector tecnológico— están rompiendo barreras todos los días e innovando a la vanguardia de la ciencia. Además, los beneficios podrían ser enormes y permitirían resolver problemas que actualmente sobrepasan la capacidad de cualquier superordenador (clásico). Esto explica por qué vendedores y usuarios están asumiendo riesgos con esta tecnología potencialmente disruptiva. Los datos de S&P Capital IP Pro (Figura 1) indican que las empresas emergentes cuánticas obtuvieron 2400 millones de dólares en inversiones a lo largo de la última década. En 2021 se registró un mayor interés, y la inversión en empresas cuánticas alcanzó un valor de 1100 millones de dólares. Y esos datos no incluyen las inversiones masivas realizadas por empresas de TI consolidadas, entre otras IBM, Amazon, Google y Honeywell.

Esta oportunidad conlleva algunos problemas importantes. Puede que el más acuciante de todos sea la amenaza que supone para las prácticas de seguridad actuales. Utilizando la computación cuántica, los ciberdelincuentes podrían falsificar las firmas digitales y descifrar los niveles actuales de criptografía y cifrado, incluida la infraestructura de claves públicas que, a día de hoy, está profundamente integrada en los sistemas de TI del mundo. Y lo que es peor, incluso los datos cifrados que actualmente están protegidos podrían ser almacenados para su posterior descodificación cuando se desarrolle la computación cuántica práctica. Es un problema que no se puede posponer. Cuanto más esperemos, más datos en riesgo crearemos.

Figura 1: Inversión en empresas emergentes de computación cuántica



Fuente: S&P Capital IQ Pro

El enfoque 451

Es imposible pronosticar con exactitud cuándo habrá un sistema cuántico capaz de ejecutar el algoritmo de Shor de forma efectiva disponible para el gran público, de forma que un ciberdelincuente pueda tener acceso a él. Hasta el momento, ningún proveedor de TI ha proporcionado un plazo definitivo para que la computación cuántica desbanque de forma efectiva a los sistemas clásicos. Sin embargo, los rápidos avances tecnológicos que se han producido a lo largo de los últimos cinco años, junto con las cuantiosas inversiones que hay en marcha, sugieren que ese día llegará, posiblemente al final de esta década. Cuando lo haga, toda la información que actualmente está protegida por algoritmos de claves públicas podría quedar expuesta. Para las agencias de defensa e inteligencia gubernamentales y los proveedores de sistemas y servicios en la nube cuyos clientes pertenecen a sectores regulados, el riesgo ya es demasiado elevado como para ignorarlo. A pesar de las falsas alarmas que se generaron en el pasado (como en el caso del Y2K, en el que uno de los atajos de programación informática más utilizados amenazaba con sembrar el caos durante el cambio de 1999 al 2000) y de las incertidumbres del futuro, una cosa es evidente: El peligro que conllevan los ciberataques constituye un gran problema hoy en día, y la naturaleza de las amenazas y las vulnerabilidades no deja de evolucionar. Las políticas de seguridad deben revisarse y actualizarse constantemente, y las tecnologías de criptografía poscuántica, junto con la implementación de la agilidad criptográfica y de un inventario criptográfico, han pasado a ser una parte fundamental de la ecuación.

Escenarios de resistencia a la computación cuántica y seguridad poscuántica

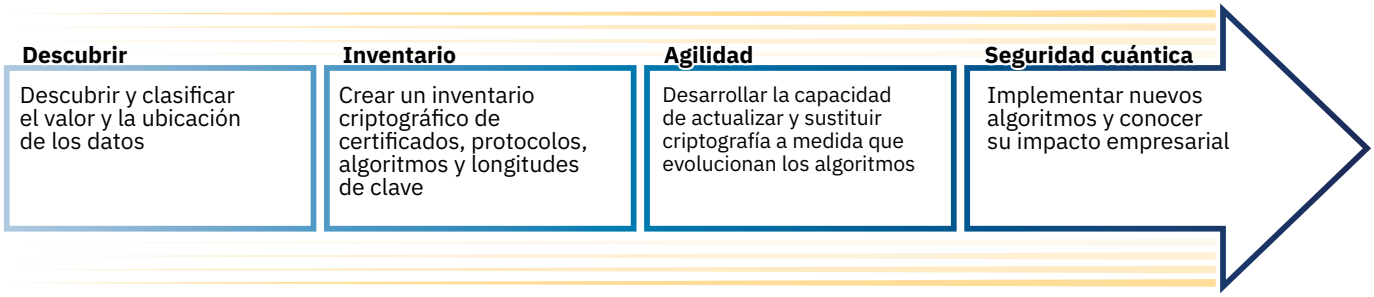
El problema consiste en lo siguiente: La generación actual de algoritmos de seguridad de uso frecuente se basa en problemas matemáticos de gran dificultad, demasiado complejos para que los sistemas clásicos los resuelvan. Sin embargo, estos problemas podrían ser resueltos fácilmente por un sistema cuántico lo suficientemente potente, una premisa que ha sido ampliamente aceptada desde 1994, cuando el matemático americano Peter Shor descubrió el algoritmo de tiempo polinómico que hoy conocemos como “algoritmo de Shor”. El primer sistema cuántico se creó tres años más tarde. El desarrollo de algoritmos resistentes a la computación cuántica ha progresado considerablemente a lo largo de la última década. Sin embargo, convertir en un nuevo conjunto de algoritmos los sistemas de criptografía de clave pública más utilizados hoy en día por los gobiernos y por la industria podría llevar décadas.

Por ello, organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) y el Departamento de Seguridad Nacional de EE. UU. han estado trabajando en el proceso de estandarización de los propios algoritmos y en una serie de recomendaciones para ayudar a las empresas a prepararse para la transición a la criptografía poscuántica. Este trabajo provocó que la Casa Blanca difundiera en enero un memorando en el que ordenaba a los servicios de defensa e inteligencia gubernamentales que iniciaran el cambio.

Descifrar un número entero compuesto de 2048 bits (descomponiéndolo en factores primos) llevaría millones de años en los sistemas más potentes de los que disponemos en la actualidad. Teóricamente, un sistema cuántico permitiría completar esta tarea en cuestión de horas. Entre los actuales esquemas de clave pública descifrados por el algoritmo de Shor se incluyen el respetado algoritmo RSA —el cual ha cumplido ya 45 años, pero continúa usándose en casi todas las transacciones basadas en Internet—, el Estándar de Seguridad de Datos, el sistema criptográfico Paillier, el algoritmo de firma digital de curva elíptica y los cifrados de curva elíptica Diffie-Hellman y ElGamal. Una larga lista de estándares establecidos por el NIST, la ISO/IEC, el ETSI y el IETF se han visto afectados, lo que indica que se trata de un problema de alcance internacional: El algoritmo de firma digital chino SM2 y el estándar de criptografía nacional SM9 también han sido descifrados.

El proceso de estándares del NIST, que comenzó en 2016 con una solicitud de propuestas, ha identificado un nuevo conjunto de candidatos resistentes a la tecnología cuántica. Estos candidatos se agrupan en una amplia variedad de enfoques —como la criptografía basada en retículos, multivariante, hash o basada en código—, y entre ellos se incluyen el mecanismo de encapsulación de claves CRYSTALS-Kyber basado en retículos (KEM), el cifrado de McEliece (KEM basado en código) y los esquemas de firma poscuánticos Falcon (de celosía) y Rainbow (multivariante). Estos y otros finalistas serán estandarizados de forma preliminar después de la tercera ronda de competición, la cual ya ha finalizado. La cuarta ronda, que incluye algoritmos alternativos y una solicitud de esquemas de firma adicionales, comienza este año y concluirá a finales de 2024.

Figura 2: Hoja de ruta para la seguridad cuántica



Fuente: 451 Research

La transición hacia la criptografía poscuántica

¿Qué medidas deben tomar ahora las organizaciones para prepararse para la incorporación de la criptografía poscuántica en las arquitecturas de seguridad de la información a lo largo de la próxima década? El primer paso, que ya ha comenzado, es participar en el proceso de estandarización. Es importante que todas las organizaciones interesadas en prevenir la autenticación fraudulenta, proteger la integridad del cifrado y evitar la exposición de firmas digitales participen activamente para asegurarse de que la lista aprobada de algoritmos, procesadores y herramientas finales satisface sus requisitos. A pesar de los progresos realizados por parte de los organismos de estandarización, se trata de una tarea continua: Harán falta más algoritmos. Dejando a un lado este hecho, la siguiente hoja de ruta ha sido diseñada para alcanzar la seguridad cuántica.

- **Descubrimiento y clasificación de datos:** realice un inventario de los datos críticos. ¿Cuáles tienen mayor valor? ¿Dónde se encuentran los datos? ¿Cuáles son los requisitos de cumplimiento? Comprender esto es fundamental, porque muchas organizaciones no son plenamente conscientes de lo que tienen ni de su valor. Sin esta información, no pueden identificar sus vulnerabilidades más graves. Es imprescindible que creen y gestionen un inventario de datos de propiedad definida.
- **Inventario criptográfico:** un inventario criptográfico detalla dónde y cómo se utiliza la criptografía de clave pública vulnerable y contiene detalles como certificados, protocolos de cifrado, algoritmos y longitudes de clave. El inventario debe gestionarse de forma que cubra la totalidad del ciclo de vida de los certificados y las claves de cifrado.
- **Agilidad criptográfica:** las organizaciones deben tener en cuenta la agilidad criptográfica en sus planes y procesos de transición para poder realizar ajustes de forma menos traumática a medida que la tecnología evoluciona y las circunstancias cambian. Deben diseñar e implantar procesos de un modo que les permita actualizar y sustituir la criptografía de la generación actual —y después probarla— más fácilmente y dentro de unos plazos bien definidos.
- **Seguridad cuántica:** las organizaciones deben implementar nuevos algoritmos sin perder de vista el impacto que la criptografía poscuántica puede tener sobre el rendimiento de su negocio.

Cada organización es diferente, y no todas estarán en posición (o adoptarán la mentalidad necesaria) para cambiar todo, por ejemplo, debido a los costes o a los problemas de gestión del ciclo de vida. No obstante, ser capaces de actualizar o sustituir los protocolos de seguridad es fundamental tanto a corto como a largo plazo. Dado que está estrechamente relacionada con la infraestructura de sistemas, alcanzar la agilidad criptográfica requerirá la cooperación de los diseñadores de sistemas, los desarrolladores de aplicaciones y los expertos en seguridad. Actualmente, hay una escasez de herramientas disponibles para contribuir a este proceso.

Las organizaciones utilizarán diversos factores para priorizar los sustitutos criptográficos poscuánticos, como el valor de los activos protegidos, la vulnerabilidad de los elementos a proteger (p. ej., almacenes de claves y contraseñas), el tipo de sistemas conectados que podrían verse afectados (p. ej., el uso compartido de información con entidades externas, incluidas agencias federales) y el tiempo que deben protegerse los datos. Los esquemas híbridos, que combinan los algoritmos clásicos y los algoritmos poscuánticos, serán necesarios durante este largo periodo de transición.

Implementación, motivación e impulsores

Los proveedores de sistemas y los grandes proveedores de servicios en la nube cuyos equipos e infraestructuras albergan cargas de trabajo empresariales decisivas no pueden permitirse el lujo de esperar a que los estándares de criptografía poscuántica estén totalmente terminados. Hace años que trabajan en este problema, y han contribuido a seleccionar los algoritmos y los protocolos que más probabilidades tienen de formar parte de la lista de estándares finalizados en 2024. Hay varios servicios de gestión de claves basados en la nube que ya son compatibles con los algoritmos de la segunda y la tercera ronda. Los clientes están empezando a utilizar estos servicios para medir el impacto que puede tener en sus aplicaciones la probable sobrecarga adicional de la utilización y la latencia del ancho de banda, así como para mitigar los posibles errores de conexión en el nivel de las capas de proxy de seguridad de la capa de transporte. Sin embargo, todos coinciden en que la transición a la tecnología poscuántica se extenderá a lo largo de varios años —dado que los estándares y la tecnología evolucionan—, y en que el primer paso debe ser la protección de la infraestructura principal.

En el mundo de los sistemas, los sistemas principales siguen siendo ampliamente utilizados como infraestructura principal segura y de alta disponibilidad por los principales bancos, aseguradoras y empresas de telecomunicaciones, distribución y transporte del mundo, una posición que han mantenido durante más de medio siglo. La nueva generación de sistemas principales dispondrá de módulos de seguridad de hardware poscuánticos que trabajarán en combinación con los componentes actualizados de los sistemas operativos y las API de gestión de claves, y serán compatibles con una serie de nuevos algoritmos resistentes a la computación cuántica. La tecnología de arranque seguro poscuántica, junto con una raíz de confianza de hardware, se utilizará para proteger la integridad del firmware de arranque de los sistemas, y se proporcionarán mecanismos poscuánticos para el intercambio seguro de claves criptográficas con socios mediante interfaces de programación de aplicaciones.

Los proveedores —incluidos los proveedores de servicios en la nube— deben desempeñar un rol fundamental a la hora de ayudar a sus clientes a realizar el cambio a la criptografía poscuántica. Las resoluciones normativas no son suficientes por sí mismas, en parte debido a que no suelen ser lo suficientemente prescriptivas como para proporcionar unas directrices claras a las organizaciones de usuarios que carecen de grandes conocimientos técnicos. Los proveedores que ya están en el centro de la infraestructura crítica pueden facilitar el proceso proporcionando protección a los sistemas empresariales principales sin tener que realizar cambios adicionales a nivel de sistema para habilitarla. Asimismo, también pueden proporcionar herramientas de descubrimiento imprescindibles para el análisis de aplicaciones de criptografía. Las organizaciones responsables de los datos deben asegurarse de que estos están protegidos a lo largo de su ciclo de vida —tanto hoy como en el futuro—, porque los datos que han sido cifrados en la actualidad mediante algoritmos clásicos pueden ser descodificados utilizando un sistema cuántico avanzado en el futuro. Si los datos deben protegerse durante un periodo de 20 años, eso significa que caducarán a mediados de la década de 2040. Incluso los escépticos que consideran que aún tardaremos muchos años en desarrollar una computación cuántica práctica se han visto obligados a reconocer que, dada la tasa de progreso actual, la probabilidad habrá aumentado significativamente para entonces.

Conclusiones

Existen numerosos argumentos a favor de la computación cuántica; por ejemplo, un sistema cuántico totalmente operativo ofrecería la posibilidad de realizar avances en el ámbito de la química, el aprendizaje automático, las finanzas, el transporte, la sanidad y mucho más. Los sistemas cuánticos acelerarían exponencialmente el procesamiento de ecuaciones cuya ejecución resulta inviable en los sistemas clásicos deterministas que se utilizan hoy en día.

La otra cara de la moneda es el efecto que la computación cuántica podría ejercer sobre las amenazas para la protección y la privacidad de los datos frente a ciberataques, las cuales ya han comenzado a aumentar. A medida que se incrementa el valor de los datos de una empresa, también lo hace la escala y el coste de los requisitos de protección de datos. Además, dado que los datos tienen un valor duradero, hay que tener en cuenta que la probabilidad de que la computación cuántica se convierta en una realidad tangible en un futuro próximo es cada vez mayor. Actuar con prontitud redundaría en una evolución más segura y controlada hacia la infraestructura principal poscuántica, la implementación de herramientas capaces de descubrir las vulnerabilidades de la capa de aplicación, la protección de los sistemas de intercambio de claves utilizados entre organizaciones y la protección continua de los secretos duraderos almacenados en los datos.

CONTACTO

América
+1 877 863 1306
market.intelligence@spglobal.com

Europa, Oriente Medio y África
+44 20 7176 1234
market.intelligence@spglobal.com

Asia Pacífico
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence