

Criptografía Cuántica

TechReport

El cifrado basado en la física, la transición hacia los estándares poscuánticos y lo que ese cambio significa para la confianza digital en América Latina y el Caribe.



Copyright © 2026 Banco Interamericano de Desarrollo (BID). Esta obra se encuentra sujeta a una Licencia Internacional Pública de Atribución/Reconocimiento 4.0 de Creative Commons CC BY 4.0 (<https://creativecommons.org/licenses/by/4.0/legalcode.es>). Se deberá cumplir los términos y condiciones señalados en el enlace URL y otorgar el respectivo reconocimiento al BID.

Todas las disputas que surjan en relación con esta licencia y que no puedan resolverse de manera amistosa se resolverán de acuerdo con el siguiente procedimiento. Mediante una notificación de mediación comunicada por medios razonables por usted o el licenciante a la otra parte, la disputa será sometida a mediación no vinculante de conformidad con el Reglamento de Mediación de la Organización Mundial de la Propiedad Intelectual (OMPI). Cualquier disputa que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo, y el uso del logotipo del BID no están autorizados por esta licencia y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones que forman parte integral de esta licencia.

Las opiniones expresadas en esta obra son exclusivamente de los autores y no necesariamente reflejan el punto de vista del BID, su Directorio Ejecutivo ni de los países que representan.



AUTORES Y COLABORADORES

Los TechReports son una iniciativa del Techlab, el Laboratorio de Tecnologías Emergentes del Departamento de Tecnología y Transformación del Banco Interamericano de Desarrollo (BID). El TechLab es responsable de explorar, experimentar y difundir información sobre nuevas tecnologías para comprender su impacto en el Grupo BID y en la región de América Latina y el Caribe.

AUTORES

Belén Girardo

Fernando Puerto Mendoza

COLABORADORES

Ignacio Cerrato

Daniel Gammell Ibañez

SUPERVISOR

Mariana Gutiérrez

TABLA DE CONTENIDOS

1. Resumen ejecutivo	7
2. Introducción: por qué la criptografía importa ahora más que nunca	10
2.1 El rol de la criptografía en la infraestructura digital global.....	10
2.2 La computación cuántica como punto de inflexión.....	11
2.3 Urgencia para la región: vulnerabilidades y oportunidades de ALC	11
3. Marco conceptual: un campo, dos respuestas	14
3.1 La criptografía clásica.....	14
3.2 Criptografía cuántica	14
3.3 Criptografía post-cuántica	15
3.4 Glosario de términos clave	16
4. Criptografía cuántica: fundamentos y protocolos	19
4.1 Principios físicos base: superposición, entrelazamiento y el “no-cloning theorem”	19
4.2 Distribución cuántica de claves (QKD)	19
4.3 Generación cuántica de números aleatorios (QRNG).....	21
4.4 Verificación cuántica de posición (QPV) y autenticación	22
4.5 Cifrado homomórfico y protocolo cuántico ciego	22
4.6 Estado de madurez tecnológica actual	24
5. La amenaza cuántica a la seguridad digital existente	27
5.1 Por qué las computadoras cuánticas vulneran el cifrado RSA y de clave pública	27
5.2 El algoritmo de Shor: la mecánica de la amenaza	28
5.3 “Almacenar ahora, descifrar después”: la amenaza que ya está activa.....	29
5.4 Horizonte temporal: ¿cuándo es real el riesgo?	30
6. Aplicaciones sectoriales	33
6.1 Sector financiero y banca central.....	33
6.2 Gobierno y administración pública.....	33
6.3 Salud	33
6.4 Infraestructura crítica y energía	34
6.5 Cadenas de suministro y comercio exterior	34

7. Recomendaciones	37
7.1 El teorema de Mosca	37
7.2 Recomendaciones para gobiernos e instituciones de la región	38
7.3 Actores multilaterales y posición institucional del BID	40
7.3.1 <i>Tecnología corporativa en el BID</i>	41
8. Conclusión	43
9. Referencias	45

CHAPTER

1

Resumen ejecutivo

1. Resumen ejecutivo

La criptografía sostiene buena parte de la infraestructura de la que dependen hoy en día todos los sistemas digitales del mundo, incluyendo los países de América Latina y el Caribe: transferencias bancarias, comunicados de gobierno, registros clínicos electrónicos y cadenas de suministro globales, entre otros casos. Cada uno de ellos se apoya en esquemas de cifrado de clave pública que llevan más de cuatro décadas protegiendo la confianza digital.

En el horizonte, ese equilibrio está a punto de ser desafiado. El avance de la computación cuántica amenaza con volver vulnerables esos mismos esquemas, en un escenario que, según las estimaciones disponibles, podría materializarse dentro de cinco a veinte años (Veritasium, 2023).

El riesgo, sin embargo, no es solo futuro. Diferentes actores, con capacidad técnica y recursos suficientes, interceptan y almacenan hoy información cifrada apostando a poder descifrarla en cuanto exista una computadora cuántica suficientemente potente. Cada año que transcurre sin una migración hacia esquemas de cifrado resistentes, se amplía el volumen de información hoy protegida que quedará expuesta cuando esa amenaza se materialice.

Este reporte presenta la criptografía cuántica, que utiliza principios de la física como superposición, entrelazamiento y el teorema de no clonación, para proteger la información y detectar cualquier intento de interceptación, mediante protocolos como la distribución cuántica de claves (QKD). A su vez, introduce la noción de criptografía post-cuántica, como hoja de ruta a seguir.

El reporte traslada luego este marco conceptual a los sectores donde la migración resulta más urgente y examina sus implicancias éticas y de gobernanza: la irreversibilidad de los datos ya expuestos bajo la lógica del Store now, decrypt later (SNDL), los riesgos de una vigilancia estatal potenciada por capacidades de descifrado cuántico y los dilemas que plantea una transición tecnológica cuyo desarrollo está hoy concentrado en un número reducido de países.

Para América Latina y el Caribe, el mensaje de este reporte es doble. Por un lado, la región enfrenta un riesgo estructural: no lidera el desarrollo del hardware cuántico ni la definición de los nuevos estándares post-cuánticos, lo que la expone a una dependencia externa en decisiones que afectarán la seguridad de su información más sensible. Por otro, la naturaleza temprana del proceso global de estandarización y migración representa una oportunidad concreta de incidencia: participar activamente en los procesos de agilidad criptográfica y gobernanza de datos que hoy se están definiendo, en lugar de adoptar pasivamente sus resultados.



5–20 AÑOS

horizonte estimado hasta
que una computadora
cuántica pueda romper RSA



MÁS DE 20×

menos qubits necesarios
hoy para romper RSA-2048
que lo estimado en 2019



2030 / 2035

plazos de la NSA para migrar
a algoritmos resistentes a la
computación cuántica



26 > 12

plazos de la NSA para migrar
a algoritmos resistentes a la
computación cuántica



Introducción

2. Introducción: por qué la criptografía importa ahora más que nunca

2.1 El rol de la criptografía en la infraestructura digital global

La criptografía constituye, en gran medida, la infraestructura invisible sobre la que se sostiene la economía digital contemporánea. Cada transferencia bancaria, cada comunicación oficial entre agencias de gobierno, cada historia clínica almacenada en un servidor y cada transacción dentro de una cadena de suministro global dependen de mecanismos matemáticos que garantizan que la información viaje y se almacene sin ser leída, alterada o suplantada por terceros no autorizados. Esta dependencia no es un fenómeno reciente. Durante buena parte del siglo XX, proteger un mensaje exigía que emisor y receptor compartieran previamente, y en persona, una misma clave secreta (un esquema conocido como criptografía simétrica), lo que resultaba impracticable a la escala y velocidad que exige el intercambio de información en un mundo interconectado.

La solución a ese problema llegó en 1977, cuando los investigadores Ronald Rivest, Adi Shamir y Leonard Adleman propusieron un esquema que lleva sus iniciales: RSA. Su innovación consistió en separar la clave utilizada para cifrar de la utilizada para descifrar, lo que se conoce como criptografía asimétrica o de clave pública, de modo que cualquier persona pudiera enviar un mensaje cifrado a un destinatario sin necesidad de haberse puesto de acuerdo previamente sobre un secreto compartido.

El esquema se apoya en una asimetría computacional: es sencillo multiplicar dos números primos muy grandes para obtener una clave pública, pero es extraordinariamente difícil, para cualquier computadora clásica, revertir esa operación y descubrir cuáles son esos dos primos originales. En el caso de RSA-2048, el estándar de seguridad vigente, el número resultante tiene alrededor de 617 dígitos y factorizarlo mediante el mejor algoritmo clásico conocido requeriría, según las estimaciones disponibles, cientos de billones de años. Sobre esa asimetría, aparentemente inquebrantable, se construyó la confianza digital de las últimas cuatro décadas (Veritasium, 2023).

617 dígitos

la longitud de un módulo RSA-2048
— factorizarlo de forma clásica
tomaría cientos de billones de años

2.2 La computación cuántica como punto de inflexión

Ese equilibrio, sin embargo, no fue diseñado para resistir un tipo de computadora fundamentalmente distinta. Mientras un bit clásico solo puede representar un valor (cero o uno) en un momento dado, un qubit puede existir en una superposición de ambos estados simultáneamente. Esta propiedad tiene una consecuencia práctica considerable: un sistema de pocos qubits ya puede representar y operar sobre múltiples valores a la vez, y ese número de estados crece exponencialmente con cada qubit adicional. Basta con veinte qubits para representar más de un millón de estados simultáneos.

Esa capacidad de cómputo paralelo no vuelve a las computadoras cuánticas superiores para cualquier tarea, de hecho, extraer información útil de una superposición sigue siendo, en general, extraordinariamente difícil, pero en 1994 el investigador Peter Shor identificó que uno de los pocos problemas donde ese paralelismo cuántico ofrece una ventaja decisiva es, precisamente, la factorización de números grandes: el mismo problema matemático en el que se apoya la seguridad de RSA. Desde entonces, el desafío dejó de ser puramente teórico.

Las estimaciones sobre los recursos cuánticos necesarios para quebrar RSA-2048 se han reducido de forma drástica a medida que avanzan los algoritmos y las técnicas de corrección de errores. En 2019, se calculaba que factorizar una clave RSA-2048 requeriría alrededor de 20 millones de qubits físicos ruidosos. Seis años después, una revisión de Craig Gidney, investigador de Google Quantum AI, redujo esa cifra a menos de un millón de qubits, un recorte de más de veinte veces respecto de la estimación anterior (Gidney, 2025). Aunque las computadoras cuánticas actuales todavía están lejos de alcanzar esa escala, la velocidad con la que disminuyen los recursos necesarios refuerza la urgencia de avanzar hacia sistemas criptográficos resistentes a la computación cuántica.

Esa urgencia ya se traduce en plazos concretos. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) recomienda comenzar la transición antes de que los algoritmos vulnerables sean retirados de sus estándares hacia 2035. Por su parte, la Agencia de Seguridad Nacional de Estados Unidos (NSA), a través de su estándar Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), fijó 2030 como un hito para la migración de los sistemas de seguridad nacional hacia algoritmos resistentes a la computación cuántica. Estos cronogramas muestran que la transición ya no se concibe como una respuesta a una amenaza lejana, sino como un proceso tecnológico y regulatorio que ya está en marcha y que también afectará a los países y organizaciones que dependen de los estándares, proveedores e infraestructuras de sus principales socios internacionales.

2.3 Urgencia para la región: vulnerabilidades y oportunidades de ALC

Frente a esta perspectiva, la pregunta para América Latina y el Caribe no es únicamente técnica, sino de tiempos y prioridades. La región enfrenta una ventana finita para migrar los sistemas críticos de los sectores financiero, gubernamental, de salud e infraestructura hacia esquemas

resistentes a la computación cuántica, antes de que este alcance la madurez necesaria para vulnerar el cifrado de clave pública que protege hoy esas mismas infraestructuras. Esa ventana se reduce, además, por un fenómeno que ya está activo: la práctica de interceptar y almacenar hoy información cifrada con la expectativa de descifrarla en el futuro, una vez que exista hardware cuántico suficientemente potente.

Al mismo tiempo, esa misma etapa temprana en la que los procesos de agilidad criptográfica y los marcos de gobernanza de datos apenas comienzan a definirse a nivel global, representa una oportunidad concreta de participación para los países de la región, en la medida en que todavía es posible influir sobre cómo se diseñan e implementan esos procesos, en lugar de simplemente adoptarlos una vez cerrados.



Marco conceptual

3. Marco conceptual: un campo, dos respuestas

3.1 La criptografía clásica

Para comprender por qué la computación cuántica genera tanta preocupación, resulta útil distinguir con precisión entre los dos paradigmas que hoy compiten por convertirse en la respuesta a esa amenaza, y contrastarlos primero con el paradigma que buscan reemplazar: la criptografía clásica.

Como se describió en la sección anterior, la criptografía de clave pública (el estándar dominante desde fines de la década de 1970) no oculta la clave utilizada para cifrar un mensaje, sino que la hace pública, y basa su seguridad en la dificultad práctica de resolver un problema matemático específico, como la factorización de números primos grandes en el caso de RSA.

Esa dificultad no es absoluta: es una dificultad computacional, es decir, depende de la potencia de cómputo disponible para intentar resolverla por fuerza bruta o mediante algoritmos más sofisticados. Mientras esa potencia estuvo limitada a computadoras clásicas, el margen de seguridad (16 millones de años para factorizar una clave típica) resultó más que suficiente. La limitación de fondo de la criptografía clásica, entonces, no es conceptual sino temporal: su seguridad es tan sólida como lo sea la brecha entre la dificultad del problema matemático subyacente y la capacidad de cómputo disponible para atacarlo. Es esa la brecha que la computación cuántica amenaza con cerrar.

3.2 Criptografía cuántica

La primera de las dos respuestas, la criptografía cuántica, no busca reemplazar el problema matemático de la criptografía clásica por uno más difícil, sino cambiar por completo el fundamento de la seguridad: en lugar de apoyarse en supuestos sobre la dificultad computacional, se apoya en las leyes de la física cuántica.

Utiliza dispositivos capaces de generar, transmitir y registrar partículas individuales (típicamente fotones) para codificar información, aprovechando dos propiedades centrales de la mecánica cuántica: la superposición, que permite que una partícula exista en más de un estado a la vez hasta el momento en que es medida, y el entrelazamiento, que vincula el estado de dos partículas de forma tal que medir una determina instantáneamente el estado de la otra, sin importar la distancia que las separe (NIST, 2025).

Entre las aplicaciones prácticas de estos principios, la más consolidada es la distribución cuántica de claves (QKD), que se examina en detalle en el capítulo 4: en ella, la clave de cifrado se transmite, no mediante bits clásicos, sino mediante fotones, mientras que el propio acto de medir un fotón para interceptarlo altera irreversiblemente su estado, revelando la intrusión a emisor y receptor. Esta propiedad, conocida como el teorema de no clonación, es la que distingue a la criptografía cuántica de cualquier esquema clásico: un atacante clásico puede copiar bits sin ser

detectado, mientras que un atacante cuántico, al intentar copiar o medir un qubit, necesariamente lo altera y deja evidencia de su intento.

3.3 Criptografía post-cuántica

La segunda respuesta, la criptografía post-cuántica (PQC), parte de una premisa distinta: no requiere hardware cuántico ni infraestructura fotónica especializada, sino que consiste en el diseño de nuevos algoritmos matemáticos ejecutables en computadoras clásicas convencionales cuya seguridad no dependa de problemas que un algoritmo cuántico pueda resolver de forma eficiente.

La mayoría de estos algoritmos se basan en la matemática de las retículas: estructuras geométricas formadas por combinaciones enteras de un conjunto de vectores, en las que encontrar el punto de la retícula más cercano a un punto arbitrario resulta un problema manejable en pocas dimensiones, pero se vuelve extraordinariamente difícil de resolver, incluso para las computadoras más potentes, cuando la retícula se define en el orden de las mil dimensiones, tal como se prevé en los esquemas de cifrado propuestos.

Consciente de la urgencia de contar con alternativas validadas antes de que la amenaza cuántica se vuelva operativa, el NIST estructuró un proceso de evaluación formal en varias etapas cuyos resultados ya constituyen el nuevo estándar global:

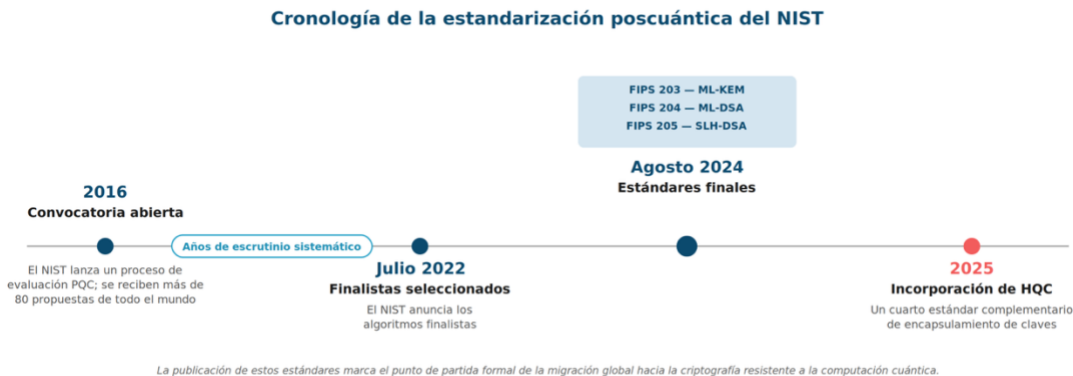


Figura 1. Línea de tiempo del proceso de estandarización post-cuántica del NIST: desde la convocatoria abierta de 2016 hasta la incorporación del HQC en 2025 como cuarto estándar post-cuántico.

La publicación de este conjunto de estándares no es solo un hito técnico: representa el punto de partida formal de la migración global de la infraestructura criptográfica hacia esquemas diseñados para resistir el cómputo cuántico (NIST, 2025).

3.4 Glosario de términos clave

Para facilitar la lectura del resto de este reporte, se resumen a continuación los términos técnicos centrales introducidos hasta aquí.

Término	Definición
Qubit	unidad básica de información cuántica. A diferencia de un bit clásico, que solo puede tomar el valor 0 o 1, un qubit puede existir en una superposición de ambos valores simultáneamente.
Superposición	propiedad por la cual una partícula cuántica (un fotón, un átomo, un electrón) puede encontrarse en dos o más estados a la vez, hasta que es medida u observada, momento en el cual el estado “colapsa” a uno solo de los valores posibles.
Entrelazamiento	fenómeno por el cual dos o más partículas cuánticas quedan vinculadas de tal forma que medir el estado de una determina instantáneamente el estado de la otra, incluso si se encuentran físicamente distantes.
Teorema de no clonación	principio según el cual es imposible copiar el estado de un qubit sin alterarlo, lo que permite detectar cualquier intento de interceptación en un canal de comunicación cuántico.
QKD (distribución cuántica de claves)	protocolo que utiliza partículas cuánticas, generalmente fotones, para transmitir una clave de cifrado entre dos partes, de forma que cualquier intento de interceptación resulte detectable.
Retícula (lattice)	estructura matemática compuesta por todos los puntos alcanzables mediante combinaciones enteras de un conjunto de vectores; su versión de alta dimensión constituye la base de los algoritmos post-cuánticos hoy estandarizados por el NIST.

Algoritmo de Shor	algoritmo cuántico desarrollado en 1994 por Peter Shor y Don Coppersmith, capaz de factorizar números grandes de forma exponencialmente más rápida que los mejores algoritmos clásicos conocidos, lo que representa la principal amenaza cuántica al cifrado RSA.
Store now, decrypt later (SNDL)	práctica mediante la cual actores estatales o no estatales interceptan y almacenan hoy información cifrada, apostando a poder descifrarla en el futuro una vez que exista una computadora cuántica suficientemente potente.

CHAPTER

4

Fundamentos y protocolos

4. Criptografía cuántica: fundamentos y protocolos

4.1 Principios físicos base: superposición, entrelazamiento y el “no-cloning theorem”

Antes de detallar los protocolos cuánticos aplicados a la seguridad de la información, conviene precisar cómo operan en la práctica los dos fenómenos mencionados en el capítulo anterior. La superposición puede observarse, por ejemplo, en un fotón que atraviesa un filtro polarizador: antes de chocar con el filtro, el fotón se encuentra en una combinación simultánea de polarización horizontal y vertical, y solo al interactuar con el material “decide” por uno de los dos estados. Esa colisión con el filtro, sea física o, en un canal de comunicación, provocada por un intento de interceptación, colapsa la superposición y dificulta que un intruso reconstruya el estado original sin ser detectado (NIST, 2025).

Ese mismo principio permite ilustrar la diferencia entre el mundo cuántico y la intuición cotidiana. En el experimento mental del gato de Schrödinger, un felino encerrado en una caja se encuentra, en un sentido estrictamente cuántico, simultáneamente vivo y muerto hasta que la caja se abre y alguien lo observa: el acto de observación es el que fuerza al sistema a “decidirse” por uno de los dos estados posibles. El entrelazamiento lleva esa misma lógica un paso más allá, como se ilustra en el Recuadro 4.1, y es, junto con el teorema de no clonación, lo que permite construir canales de comunicación en los que cualquier intento de copia o interceptación deja un rastro detectable.

Recuadro 4.1 — La analogía de los guantes

Para entender el entrelazamiento sin recurrir a la matemática cuántica, resulta útil un ejemplo simple. Si una persona tiene dos guantes, uno negro y uno blanco, guardados en una caja y extrae uno de ellos, no sorprende que, al comprobar que es blanco, el que queda en la caja sea necesariamente negro: la información ya estaba definida previamente.

La diferencia con el caso clásico no es de grado: allí, el resultado ya estaba determinado antes de abrir la caja; en el caso cuántico, ninguno de los dos guantes tenía un color definido hasta el instante de la medición. El valor del entrelazamiento para la criptografía no radica, entonces, en la posibilidad de comunicarse más rápido, sino en la existencia de correlaciones que no pueden reproducirse ni copiarse sin alterar el sistema. Cualquier intento de un tercero por interceptar o medir las partículas modifica esas correlaciones y puede revelar la intrusión.

4.2 Distribución cuántica de claves (QKD)

Como se adelantó en el capítulo 3, el protocolo más consolidado que se apoya en estos principios es la distribución cuántica de claves. En su forma más simple, dos partes intercambian una

secuencia de fotones cuya polarización codifica los bits de una clave de cifrado; como cualquier intento de medir esos fotones altera su estado, un tercero que intente interceptar la transmisión introduce errores detectables, lo que permite descartar la clave comprometida antes de usarla.

El caso de uso más citado del protocolo, documentado desde 2004, fue su empleo para asegurar una transferencia de fondos entre una entidad bancaria austríaca y el ayuntamiento de Viena (NIST, 2025). Su principal limitación práctica es la distancia: la absorción de fotones en la fibra óptica reduce la tasa de generación de claves a medida que crece el recorrido, y esa pérdida no puede compensarse copiando y amplificando la señal, porque el teorema de no clonación lo impide. Para superarla, se investigan “repetidores cuánticos”, dispositivos que distribuyen e intercambian entrelazamiento entre tramos cortos de fibra hasta construir una conexión segura de mayor alcance.

La vía alternativa más avanzada hasta la fecha esquiva el problema de la fibra trasladando el canal al espacio. A diferencia del medio terrestre, la atmósfera libre por encima de su capa densa atenúa los fotones de forma mucho más leve, lo que permite mantener tasas de transmisión viables a distancias que serían inaccesibles para cualquier cable. China lidera esta trayectoria desde 2016, cuando lanzó Micius, el primer satélite de comunicaciones cuánticas del mundo. En 2021, científicos de la Universidad de Ciencia y Tecnología de China publicaron en Nature los resultados de la primera red integrada de comunicación cuántica a escala intercontinental: una infraestructura que combina más de 700 fibras ópticas terrestres con dos enlaces al satélite Micius, cubriendo 4.600 kilómetros en total y dando servicio a más de 150 usuarios institucionales, entre ellos bancos estatales, redes eléctricas municipales y organismos gubernamentales.

Vale precisar que en esta arquitectura el satélite opera como nodo de confianza, es decir, gestiona las claves en tránsito, lo que traslada parte del requisito de seguridad a la integridad del propio satélite; investigaciones en curso apuntan a reemplazar este modelo por distribución de entrelazamiento directo, que eliminará esa dependencia (Chen et al., 2021).



4.600 km

extensión de la primera red de
comunicación cuántica
intercontinental integrada, con más
de 150 instituciones

La aplicación práctica de estos principios enfrenta, sin embargo, limitaciones que no son menores. Ningún instrumento es perfecto: no existen detectores capaces de registrar absolutamente todos los fotones que los alcanzan, ni fuentes de luz que emitan, sin excepción, un único fotón por pulso, lo que introduce falsos negativos y falsos positivos que deben mantenerse en un mínimo para que la clave resultante sea confiable. Institutos de estandarización como el NIST han concentrado buena parte de su investigación en construir detectores de fotón único capaces de operar a temperaturas cercanas al cero absoluto, minimizando el ruido y mejorando la precisión del registro.

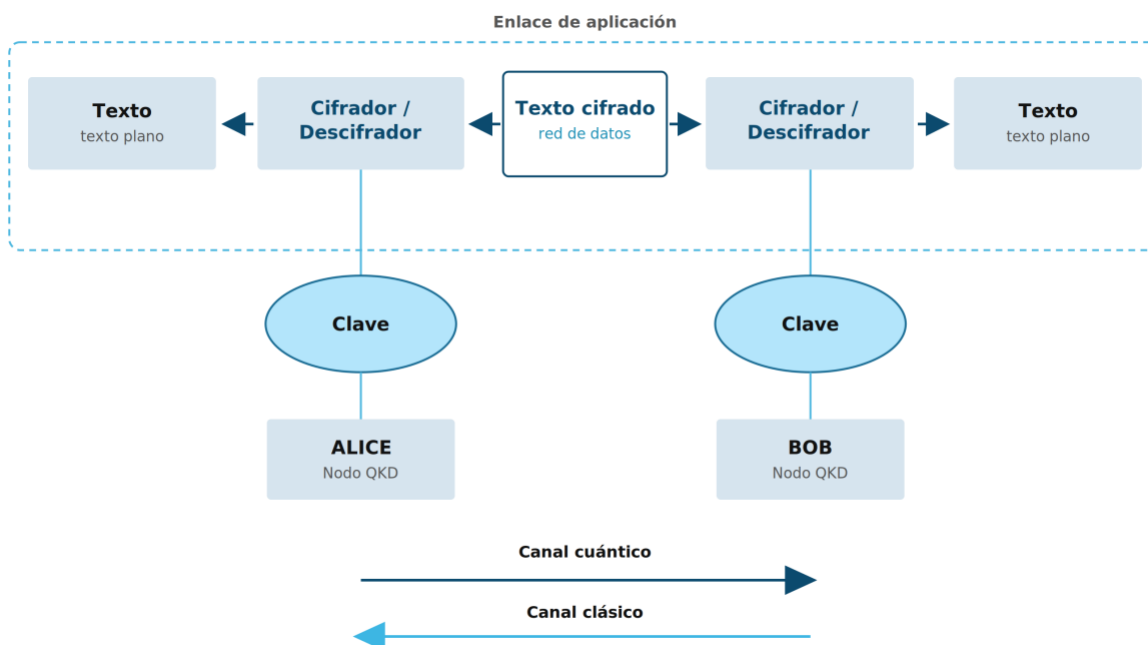


Figura 2. Cómo funciona la distribución cuántica de claves (QKD): el intercambio entre Alice y Bob, el rol del fotón, el teorema de no clonación como mecanismo de detección de intrusos y la generación de la clave segura.

Estas imperfecciones abren, además, una vía de ataque específica. Dado que las tolerancias de fabricación generan pequeñas variaciones en la ventana de detección de cada instrumento, un atacante puede interceptar un fotón, medirlo y reenviar al receptor un “estado falso” calibrado para explotar esas variaciones, evitando ser detectado. Cerrar por completo esta clase de vulnerabilidades exige protocolos más sofisticados, denominados “independientes del dispositivo”, cuya seguridad no depende de las propiedades físicas particulares del hardware que los ejecuta, sino de las correlaciones observadas en los resultados (Durr-E-Shahwar et al., 2024).

4.3 Generación cuántica de números aleatorios (QRNG)

Un segundo protocolo relevante es la generación cuántica de números aleatorios (QRNG), que responde a una debilidad poco visible de la seguridad digital: buena parte de las claves de cifrado se construyen a partir de números que se presumen aleatorios, en una operación que se repite cientos de miles de millones de veces al día, pero que rara vez es aleatoria en un sentido absoluto.

Un lanzamiento de moneda, por ejemplo, puede parecer impredecible, aunque en teoría su resultado podría anticiparse si se conociera con exactitud su trayectoria física; del mismo modo, los generadores de números aleatorios por software suelen partir de un valor inicial que, aunque difícil de deducir, no es enteramente impredecible.

La física cuántica ofrece, en cambio, una fuente de aleatoriedad genuina: el instante exacto en que decae un átomo radiactivo, o el recorrido de un fotón a través de un sistema de lentes y componentes ópticos, son fenómenos que ningún modelo físico permite anticipar. Investigadores del NIST han construido generadores que traducen ese comportamiento en secuencias confiables de ceros y unos, hoy utilizadas para alimentar mecanismos públicos de aleatoriedad empleados en aplicaciones de cómputo seguro distribuidas entre múltiples partes.

4.4 Verificación cuántica de posición (QPV) y autenticación

Un tercer desarrollo, aún experimental, es la verificación cuántica de posición, que busca resolver un problema distinto: no proteger el contenido de un mensaje, sino confirmar que quien lo envía o recibe se encuentra efectivamente en la ubicación que declara, exigiendo al receptor manipular qubits de una manera que solo resulta posible desde esa posición física.

Un caso ilustrativo ayuda a dimensionar el problema: si una diplomática necesita enviar un mensaje confidencial hacia su país de origen, querrá tener la certeza de que el servidor con el que se está comunicando se encuentra efectivamente en el territorio que dice representar, y no en una ubicación suplantada. Investigadores del Joint Center for Quantum Information and Computer Science estudian actualmente cómo llevar este tipo de verificación a aplicaciones reales, aunque el protocolo todavía no ha sido desplegado fuera de un entorno experimental.

QPV, sin embargo, solo verifica dónde está un interlocutor, no quién es; para una autenticación completa de identidad, la literatura propone combinar este mecanismo con certificados digitales convencionales, de modo que la criptografía cuántica complementa, en lugar de sustituir, a la infraestructura de clave pública existente.

4.5 Cifrado homomórfico y protocolo cuántico ciego

Un cuarto desarrollo en el campo de la criptografía responde a un problema diferente del de la comunicación: la protección del dato durante su procesamiento. La situación típica es la de una organización que necesita procesar grandes volúmenes de información sensible en infraestructura externa, ya sea por capacidad de cómputo o por economías de escala en la nube. El cifrado protege esos datos en tránsito y en reposo, pero la mayoría de los sistemas actuales exige descifrarlos en el momento del cómputo, generando una ventana de exposición que afecta tanto a la confidencialidad como a la integridad de la información. Es en ese intervalo donde reside una vulnerabilidad estructural que el modelo de nube convencional no ha resuelto.

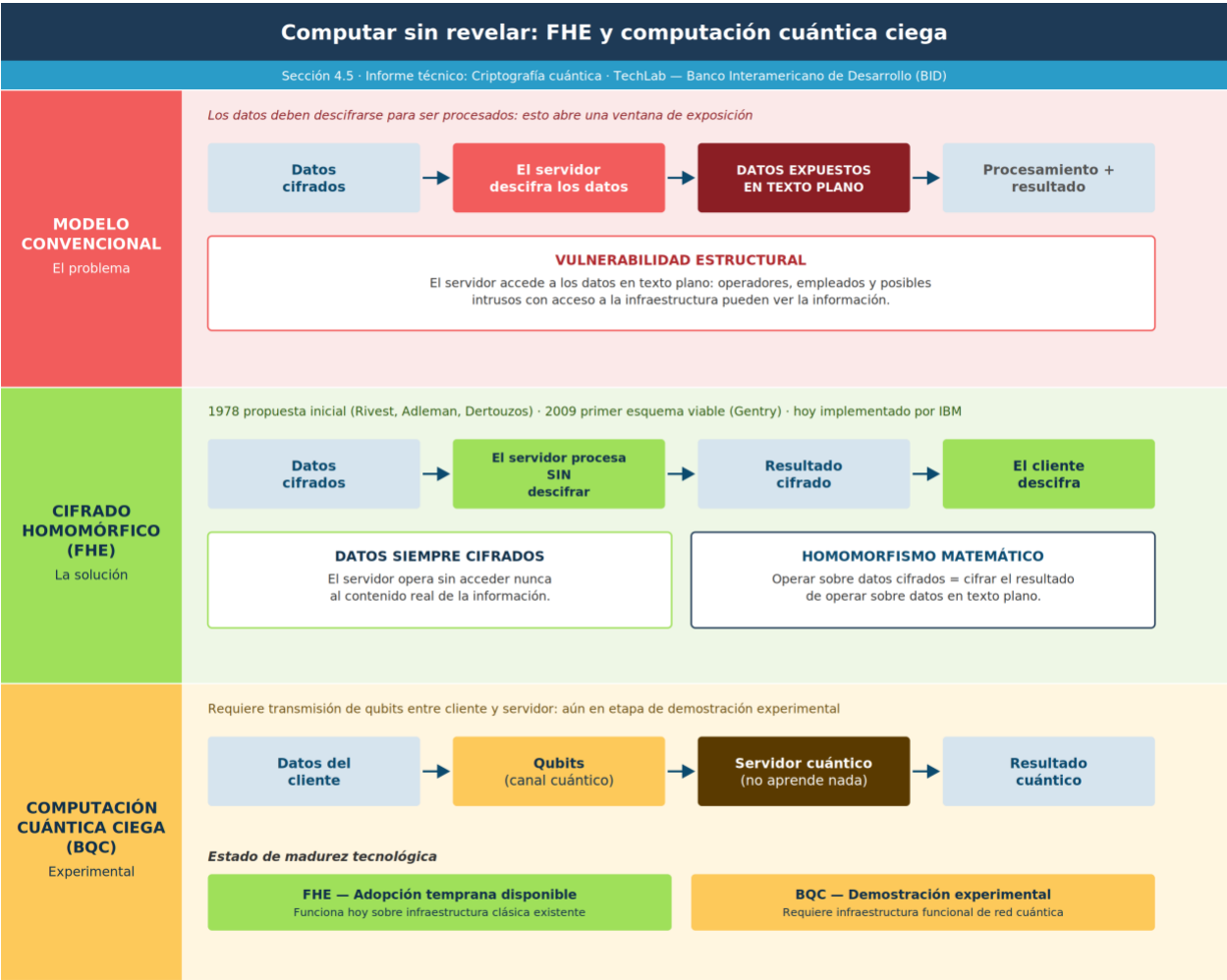
La respuesta más madura a ese desafío es el cifrado totalmente homomórfico (FHE, por sus siglas en inglés): un esquema que permite realizar operaciones matemáticas directamente sobre datos

cifrados, sin descifrarlos en ningún momento y sin que quien ejecuta el cómputo acceda al contenido de la información. El resultado que devuelve el servidor externo es, a su vez, un dato cifrado que solo el titular de la clave puede interpretar. La lógica que lo hace posible descansa en el concepto de homomorfismo matemático: si una función F transforma elementos de un conjunto en otro preservando su estructura algebraica, entonces operar sobre los datos transformados produce el mismo resultado que operar primero y transformar después. En términos concretos: sumar dos números cifrados homomórficamente produce el mismo resultado cifrado que sumar los números en claro y luego cifrarlos. Esa propiedad permite que un tercero opere sobre información que nunca conoció.

La idea fue formulada por primera vez en 1978 por Ronald Rivest, Leonard Adleman y Michael Dertouzos, los mismos Rivest y Adleman que un año antes publicaron el algoritmo RSA, pero su viabilidad permaneció sin demostrar durante tres décadas. Fue Craig Gentry quien, en 2009, estableció los fundamentos matemáticos para construir un esquema FHE simultáneamente seguro y computacionalmente realizable. El FHE es actualmente una tecnología real: empresas como IBM la han incorporado en arquitecturas de zero trust, donde los datos permanecen cifrados a lo largo de todo el ciclo de procesamiento, incluidas operaciones en entornos de nube no confiables. Su principal limitación sigue siendo el costo computacional dado que las operaciones homomórficas son órdenes de magnitud más intensivas en recursos que su equivalente sobre datos en claro, lo que restringe su adopción a casos de uso donde la protección del dato justifica ese overhead.

En ese punto aparece la intersección con la computación cuántica, aunque debe señalarse con precisión: no existe hoy evidencia consolidada de que los computadores cuánticos disponibles o de mediano plazo ofrezcan una ventaja práctica clara para acelerar los algoritmos que sustentan el FHE. Algunos investigadores exploran si ciertas operaciones matemáticas sobre retículas, la base de los esquemas FHE modernos, podrían beneficiarse de algoritmos cuánticos, pero esa línea sigue siendo materia de investigación abierta. Lo que sí está demostrado es la dirección inversa: dado que el FHE se fundamenta en problemas como el aprendizaje con errores (Learning With Errors), considerados resistentes a ataques de computadoras cuánticas, esta tecnología forma parte de la familia de soluciones post-cuánticas y no requiere ser reemplazada frente a la amenaza que el cómputo cuántico representa para el cifrado clásico.

Paralelo al FHE y conceptualmente emparentado, el campo cuántico ha desarrollado el protocolo de computación cuántica ciega (BQC), en el que un cliente delega el procesamiento a un servidor cuántico sin que este aprenda nada sobre la tarea ni sobre los datos que maneja. A diferencia del FHE, que opera sobre datos clásicos en infraestructura convencional, el BQC requiere la transmisión de qubits entre las partes y está directamente ligado al desarrollo de redes cuánticas funcionales. Ambos protocolos comparten el mismo objetivo, computar sobre lo que no se puede ver, pero desde arquitecturas y estados de madurez radicalmente distintos: el FHE es una tecnología en fase de adopción temprana, mientras que el BQC es un protocolo en fase de demostración experimental.



Fuente: TechLab — Banco Interamericano de Desarrollo (BID) · Informe técnico: Criptografía cuántica

Figura 3. Cifrado totalmente homomórfico (FHE) y computación cuántica ciega (BQC): dos protocolos para operar sobre datos sin exponerlos, comparados según su arquitectura y grado de madurez.

4.6 Estado de madurez tecnológica actual

Ordenados según su grado de madurez, los protocolos descritos en este capítulo ocupan posiciones distintas: la QKD es el más avanzado, con implementaciones piloto documentadas desde 2004; la QRNG se encuentra en una etapa de adopción más consolidada, integrada ya en mecanismos públicos de aleatoriedad; mientras que la QPV y la computación cuántica ciega permanecen, todavía, en fases predominantemente experimentales o de investigación académica. La literatura especializada describe a la criptografía cuántica, en su conjunto, como una tecnología “en desarrollo” que debe superar obstáculos identificados de forma sistemática como desplazamientos involuntarios de polarización, distancias de transmisión acotadas y limitaciones en la tasa de generación de claves a medida que aumenta la distancia recorrida antes de alcanzar una adopción comparable a la de la criptografía clásica (Durr-E-Shahwar et al., 2024).

Sobre el ritmo general de avance de la computación cuántica resulta ilustrativa la perspectiva de Aram Harrow, investigador del MIT con 25 años de trayectoria en el campo y co-desarrollador en 2008 del algoritmo HHL, una de las primeras demostraciones de ventaja exponencial de las computadoras cuánticas sobre las clásicas. Harrow reconoce haber sido, en sus propias palabras, “demasiado pesimista” al estimar sistemáticamente horizontes de diez a quince años, y sostiene ahora que conviene prepararse para la aparición, en un plazo más corto, de computadoras cuánticas de miles de qubits capaces de realizar tareas imposibles para las computadoras actuales, lo que él considera el verdadero punto de partida de la computación cuántica útil (El País, 2026).



La amenaza cuántica

5. La amenaza cuántica a la seguridad digital existente

5.1 Por qué las computadoras cuánticas vulneran el cifrado RSA y de clave pública

La razón por la cual una computadora cuántica suficientemente potente pondría en riesgo el cifrado RSA y, en general, la criptografía de clave pública se encuentra en la forma en que procesa la información. Una computadora clásica con dos bits solo puede representar, en un instante dado, uno de cuatro valores posibles; una computadora cuántica con dos qubits puede representar los cuatro simultáneamente, y ese número de estados se duplica con cada qubit adicional. Esa propiedad no convierte, por sí sola, a una computadora cuántica en una herramienta universalmente más veloz: leer una superposición exige medirla, y toda medición reduce el resultado a un único valor elegido esencialmente al azar, destruyendo el resto de la información contenida en los demás estados (Veritasium, 2023).

Aprovechar esa ventaja exige, entonces, algoritmos capaces de manipular la superposición de forma que, al medirla, se obtenga precisamente la información buscada, y hasta ahora solo se ha identificado un número reducido de problemas donde esto es posible. La factorización de números grandes es uno de ellos. El Recuadro 5.1 ilustra esta lógica con un ejemplo simplificado de cómputo paralelo.

Recuadro 5.1 — Por qué más qubits multiplican la potencia de cómputo

Con dos bits clásicos es posible representar únicamente uno de cuatro valores en un momento dado (00, 01, 10 u 11), interpretables como los números 0, 1, 2 y 3. Para calcular, por ejemplo, el resultado de elevar el número 7 a cada uno de esos valores, una computadora clásica debe repetir la operación cuatro veces, una por cada estado.

Con dos qubits, en cambio, el sistema puede representar los cuatro valores simultáneamente, de modo que una única operación cuántica produce, en superposición, los cuatro resultados a la vez: 7 elevado a 0, 1, 2 y 3, es decir, 1, 7, 49 y 343. Cada qubit adicional duplica el número de estados representables: veinte qubits ya alcanzan para más de un millón de estados simultáneos, y trescientos bastarían, en teoría, para representar más estados que partículas existen en el universo observable.

El límite es que esa información solo puede extraerse mediante algoritmos diseñados específicamente para aprovecharla; de lo contrario, medir la superposición solo arroja un resultado al azar, y el resto de la información se pierde.

5.2 El algoritmo de Shor: la mecánica de la amenaza

En 1994, Peter Shor y Don Coppersmith mostraron cómo aprovechar esa ventaja mediante la transformada cuántica de Fourier, una operación capaz de extraer la frecuencia de una señal periódica. Su idea central consiste en transformar el problema de factorizar un número n (producto de dos primos p y q) en el de encontrar el periodo de una secuencia: se elige un número g sin factores comunes con n , se eleva a potencias sucesivas y se registra el resto de dividir cada resultado por n ; esos restos se repiten con una periodicidad r que, una vez hallada mediante la transformada de Fourier, permite, si r resulta par, construir dos nuevos números que comparten factores con n , los cuales el algoritmo de Euclides permite identificar rápidamente como p y q (Veritasium, 2023).

Ejecutar este procedimiento en computadoras clásicas no ofrece ninguna ventaja de velocidad; lo que una computadora cuántica acelera de forma decisiva es, específicamente, el paso de encontrar ese periodo r . El Recuadro 5.2 reproduce, de forma simplificada, la lógica aritmética detrás de este procedimiento.

Recuadro 5.2 — Cómo factoriza Shor un número: un ejemplo con $n = 77$

Tomemos un número n , producto de dos primos desconocidos, y fijemos $n = 77$ solo para ilustrar el método (en un caso real, los primos tendrían cientos de dígitos). Se elige un número g menor que n y sin factores comunes con él, por ejemplo, $g = 8$, y se calculan sus potencias sucesivas, dividiendo cada resultado por n y registrando únicamente el resto: 8^1 deja resto 8; 8^2 deja resto 64; 8^3 deja resto 50; y así sucesivamente, hasta que 8^{10} deja un resto de exactamente 1.

Ese exponente, 10, es el “periodo” r que el algoritmo de Shor permite hallar de forma eficiente mediante la transformada cuántica de Fourier. Como r es par, puede usarse para construir dos nuevos números: $8^5 + 1 = 32.769$ y $8^5 - 1 = 32.767$, que muy probablemente comparten factores con n .

Aplicando el algoritmo de Euclides (dividir el número mayor por el menor y repetir el proceso con el resto hasta llegar a cero) se obtiene que el máximo común divisor entre 32.769 y 77 es 11, uno de los dos factores primos de 77; dividiendo 77 por 11 se obtiene el segundo, 7. Sobre una computadora clásica, encontrar el periodo r no ofrece ninguna ventaja de velocidad; es precisamente ese paso el que una computadora cuántica resuelve de forma exponencialmente más rápida, y es allí donde reside la amenaza al cifrado RSA.

Las estimaciones de qubits físicos necesarios para ejecutar el algoritmo sobre claves RSA reales han caído de forma sostenida: de mil millones en 2012 a 230 millones en 2017, y a 20 millones en 2019, lo que ilustra cuán rápido se achica la distancia entre la teoría y una amenaza operativa.

5.3 “Almacenar ahora, descifrar después”: la amenaza que ya está activa

La amenaza cuántica a la criptografía de clave pública no es, sin embargo, un riesgo enteramente futuro. Bajo la lógica conocida como “store now, decrypt later”, actores estatales y no estatales interceptan y almacenan hoy grandes volúmenes de información cifrada sin poder leerla en el presente, pero apostando a poder hacerlo en cuanto exista una computadora cuántica suficientemente potente. La estrategia resulta racional porque buena parte de esa información conservará valor dentro de una década.

La lista de objetivos típicos de esta práctica incluye tanto a actores públicos como privados: bancos centrales, agencias de inteligencia, empresas farmacéuticas y operadores de infraestructura crítica manejan información cuya sensibilidad no caduca en el corto plazo, lo que los convierte en blancos naturales del SNDL incluso en ausencia, todavía, de una computadora cuántica capaz de explotarlo.

La Agencia de Seguridad Nacional de Estados Unidos ha señalado públicamente que una computadora cuántica suficientemente grande, si llegara a construirse, sería capaz de comprometer todos los algoritmos de clave pública hoy ampliamente desplegados, lo que convierte al SNDL en una amenaza activa incluso mientras el hardware necesario para explotarla todavía no existe (Veritasium, 2023).

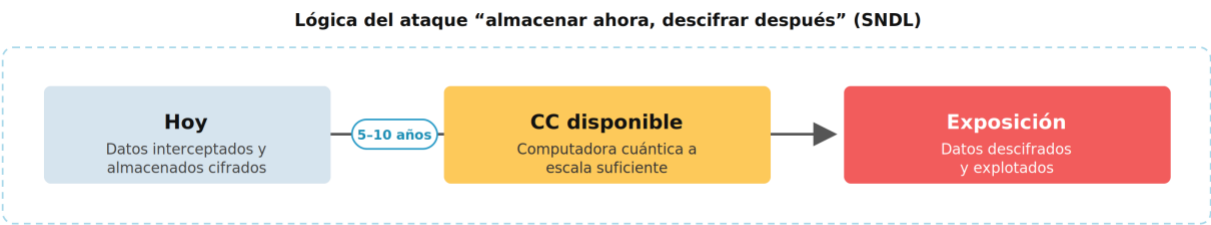


Figura 4. El flujo del ataque “store now, decrypt later” (SNDL): interceptar y almacenar hoy datos cifrados para descifrarlos una vez que exista una computadora cuántica suficientemente potente.

Datos cuya sensibilidad persiste diez años o más: objetivos típicos del SNDL.

Categoría	Activos con sensibilidad persistente	Horizonte típico
Defensa y seguridad	Bases militares e instalaciones de defensa; agentes de inteligencia y comunicaciones clasificadas	Posiciones operativas vigentes durante décadas
Infraestructura crítica	Redes eléctricas, plantas nucleares y de agua; protocolos de emergencia e instalaciones clave	Infraestructura activa entre 20 y 50 años

Sector financiero	Estrategias y reservas de deuda soberana; contratos y posiciones de fondos soberanos	Vigente durante toda la duración del contrato
Datos personales	Información genética y biométrica; historial médico completo	Los datos biométricos y el ADN son permanentes e irrevocables
Propiedad intelectual	Fórmulas farmacéuticas y secretos comerciales; investigación científica no publicada, I+D estratégica	Patentes vigentes entre 15 y 20 años

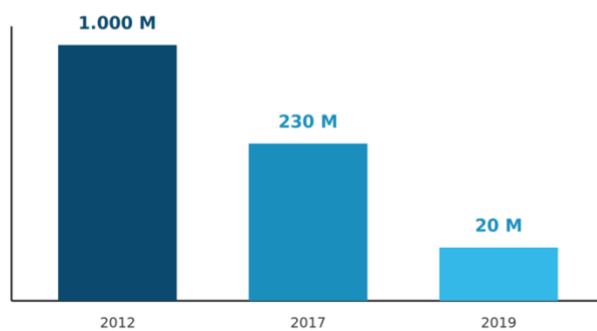
5.4 Horizonte temporal: ¿cuándo es real el riesgo?

Establecer con precisión cuándo se materializará ese riesgo resulta difícil, en parte porque las propias estimaciones han cambiado con rapidez. Las proyecciones disponibles ubican la aparición de una computadora cuántica capaz de romper el cifrado RSA en un horizonte de entre cinco y veinte años, según la fuente y el año en que se realizó la estimación, y la tendencia observada sugiere que ese horizonte tiende a acortarse antes que a extenderse.

La comparación entre la capacidad de cómputo cuántico disponible y la requerida para ejecutar el algoritmo de Shor sobre claves reales ilustra la naturaleza de este horizonte: al observar el estado actual de los procesadores cuánticos comercialmente disponibles, la distancia respecto de los millones de qubits necesarios sigue siendo amplia, pero la trayectoria de crecimiento ha sido consistentemente exponencial. Esa misma dinámica explica por qué investigadores que durante años sostuvieron horizontes de diez a quince años, como Harrow, han revisado sus propias proyecciones hacia plazos más cortos.



Qubits físicos estimados necesarios para romper RSA



Nota: las alturas de las barras son ilustrativas, no están a escala. Fuente: elaboración propia a partir de estimaciones citadas en la literatura sobre el algoritmo de Shor y del NIST (2016-2022).

Figura 5. Línea de tiempo de la amenaza cuántica: hitos regulatorios y tecnológicos (NIST 2016-2022), caída en la estimación de qubits necesarios para romper RSA (2012-2019) y ventana crítica del SNDL.

CAPÍTULO

6

Aplicaciones sectoriales

6. Aplicaciones sectoriales

Los capítulos anteriores establecieron por qué la criptografía de clave pública es vulnerable a la computación cuántica, cómo opera esa amenaza y qué alternativas existen para responder a ella. Este capítulo traslada esa discusión a los sectores donde la migración hacia esquemas resistentes resulta más urgente, identificados ya en el resumen ejecutivo de este reporte: el financiero, el gubernamental, el de salud, el de infraestructura crítica y el de comercio exterior.

6.1 Sector financiero y banca central

El sistema financiero es, probablemente, el sector cuya dependencia de la criptografía de clave pública resulta más directa: las transferencias bancarias, los sistemas de pago electrónico, la banca en línea y las plataformas de intercambio de valores dependen, en última instancia, de que las claves públicas utilizadas para autenticar transacciones no puedan falsificarse ni descifrarse.

La lógica del “store now, decrypt later” descrita en el capítulo 5 resulta, en este sector, particularmente relevante: los datos de clientes y los registros de transacciones interceptados hoy conservarían buena parte de su valor, así como su potencial de daño reputacional y patrimonial, incluso si se descifran varios años después de haber sido capturados. Los bancos centrales, en su rol de supervisores del sistema financiero, enfrentan además la tarea adicional de coordinar cronogramas de migración entre múltiples entidades reguladas, un desafío de agilidad criptográfica a escala sectorial que excede la capacidad de cualquier institución individual.

6.2 Gobierno y administración pública

Las comunicaciones oficiales entre agencias de gobierno, los sistemas de identidad digital y los registros administrativos comparten con el sector financiero una misma exposición estructural: dependen de la criptografía de clave pública para garantizar que solo los destinatarios autorizados puedan leer un mensaje o validar una identidad. La diferencia, en este caso, es la naturaleza de la información en juego: buena parte de las comunicaciones diplomáticas y de inteligencia gubernamental conserva su sensibilidad durante períodos mucho más largos que una transacción financiera, lo que las convierte en uno de los objetivos más citados de la práctica de interceptar y almacenar información hoy para descifrarla en el futuro.

La verificación cuántica de posición y los certificados digitales anticipan, en este sentido, una de las aplicaciones más directas de la criptografía cuántica en el ámbito gubernamental: confirmar que una comunicación oficial proviene efectivamente del servidor y la jurisdicción que declara.

6.3 Salud

Las historias clínicas y los registros médicos electrónicos presentan una combinación particular de sensibilidad y persistencia: a diferencia de una contraseña, que puede modificarse una vez

comprometida, un diagnóstico médico o un historial genético no pierden su carácter sensible con el paso del tiempo, lo que los vuelve especialmente vulnerables a la lógica del “store now, decrypt later”.

La creciente digitalización de los sistemas de salud a partir de historias clínicas electrónicas, telemedicina, intercambio de datos entre proveedores y aseguradoras, entre otros, multiplica, además, los puntos en los que la información viaja cifrada por redes que eventualmente deberán migrar a esquemas post-cuánticos, sin que la evidencia disponible permita precisar plazos ni estados actuales de adopción en el sector salud de América Latina y el Caribe.

6.4 Infraestructura crítica y energía

Las redes eléctricas, los sistemas de distribución de agua y las redes de telecomunicaciones dependen cada vez más de sistemas de control remoto y de comunicaciones cifradas entre sensores, centros de operación y proveedores, lo que traslada a la operación física de estos servicios buena parte de los riesgos de seguridad digital planteados en este reporte.

A diferencia de un registro financiero o clínico, cuya vulneración compromete la confidencialidad de la información, un ataque exitoso sobre las comunicaciones cifradas de una red eléctrica o de agua podría comprometer, además, la continuidad operativa del servicio, lo que añade una dimensión de seguridad física a la discusión sobre agilidad criptográfica. La literatura consultada no ofrece precisiones adicionales sobre el estado de la infraestructura crítica de la región frente a esta amenaza: se trata, en consecuencia, de un área donde el diagnóstico sectorial resulta particularmente necesario.

6.5 Cadenas de suministro y comercio exterior

Las cadenas de suministro globales dependen de sistemas de trazabilidad, documentación aduanera y comunicación entre múltiples actores que hoy se apoyan en firmas digitales y canales cifrados para garantizar la autenticidad de la documentación comercial y evitar fraudes.

La naturaleza distribuida de estas cadenas, que involucran actores de distinta capacidad tecnológica y jurisdicciones regulatorias diversas, hace que la migración hacia esquemas post-cuánticos requiera, en este sector, un grado de coordinación multilateral considerable. El comercio exterior de América Latina y el Caribe, altamente dependiente de mercados y cadenas logísticas internacionales, se encuentra por tanto expuesto a los cronogramas de migración que definan sus principales socios comerciales, un factor adicional que refuerza la conveniencia de una participación temprana de la región en los procesos de estandarización.

En Estados Unidos, por ejemplo, la Agencia de Seguridad Nacional (NSA) estableció, a través de la Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), un cronograma progresivo para incorporar algoritmos resistentes a la computación cuántica: prevé que determinados sistemas, como los equipos tradicionales de redes, adopten exclusivamente estos algoritmos hacia 2030,

mientras que la transición general de los sistemas de seguridad nacional deberá completarse en 2035 (National Security Agency, 2022).

Estos calendarios anticipan cambios en los requisitos tecnológicos, de interoperabilidad y de seguridad que pueden extenderse más allá de las fronteras norteamericanas y afectar a empresas e instituciones de la región. En ese contexto, una participación temprana de América Latina y el Caribe en los procesos de estandarización y una planificación anticipada de la migración resultan fundamentales para reducir costos, evitar nuevas dependencias tecnológicas y preservar la integración con los mercados internacionales.

Sector	Qué protege hoy la criptografía de clave pública	Por qué importa el SNDL
Financiero y banca central	Transferencias, banca en línea y autenticación de pagos	Los datos de clientes y transacciones conservan valor durante años
Gobierno y administración pública	Identidad digital y comunicaciones oficiales	Comunicaciones diplomáticas y de inteligencia con sensibilidad prolongada
Salud	Historias clínicas electrónicas y telemedicina	La sensibilidad de un diagnóstico o historial genético no caduca
Infraestructura crítica y energía	Comunicación entre sensores, redes y centros de control	Compromete la continuidad operativa, no solo la confidencialidad
Cadenas de suministro y comercio exterior	Firmas digitales en documentación aduanera	Requiere coordinación multilateral entre actores y jurisdicciones

Síntesis elaborada a partir de la lógica de exposición descrita en los capítulos 2, 5 y 7 de este reporte; no sustituye un diagnóstico sectorial específico para América Latina y el Caribe.

Figura 6. Exposición sectorial a la amenaza cuántica: síntesis cualitativa a partir del marco conceptual desarrollado en los capítulos 2 a 6.



Recomendaciones

7. Recomendaciones

El análisis desarrollado en los capítulos anteriores deja un diagnóstico claro: la amenaza que la computación cuántica plantea a la infraestructura criptográfica actual no es especulativa ni lejana, y en su modalidad de "almacenar ahora, descifrar después", ya está activa. La pregunta que corresponde responder a continuación es cómo actuar.

Este capítulo propone un marco estructurado para responderla, organizado en cuatro ejes: una herramienta para calibrar la urgencia de la acción, recomendaciones prácticas para gobiernos e instituciones de la región, el rol que los organismos multilaterales pueden desempeñar en el acompañamiento de la transición, y la visión institucional del BID.

7.1 El teorema de Mosca

Antes de formular recomendaciones específicas, conviene establecer el marco analítico que permite responder a una pregunta que muchas organizaciones postergan: ¿cuándo, exactamente, es necesario actuar? El teorema de Mosca, formulado por el investigador en computación cuántica Michele Mosca, ofrece una respuesta a través de una desigualdad simple pero con implicancias operativas de primer orden.

El teorema propone definir tres variables: X , el número de años que los datos a proteger deben permanecer confidenciales; Y , el número de años que tomará migrar los sistemas a esquemas criptográficos resistentes al cómputo cuántico; y Z , el número de años que restan hasta que exista una computadora cuántica criptográficamente relevante a escala. La conclusión central es que una organización enfrenta riesgo presente siempre que $X + Y > Z$, incluso si la computadora cuántica todavía no existe. El motivo es estructural: si la migración demanda más tiempo del que queda hasta que la amenaza se materialice, cualquier dato que deba permanecer seguro más allá de ese punto ya está expuesto a través de los ataques SNDL.

Aplicado a un gobierno de América Latina y el Caribe que gestiona datos de infraestructura con vigencia de veinte años ($X = 20$), cuyos sistemas complejos requieren entre cinco y siete años de migración ($Y = 6$), y donde estimaciones conservadoras ubican una computadora cuántica relevante en un horizonte de diez a quince años ($Z = 12$): la suma arroja 26 contra 12. El riesgo es presente, antes de que la computadora cuántica exista.

La utilidad del teorema no depende de la certeza sobre Z , y eso es precisamente su mayor fortaleza: aun con la incertidumbre que caracteriza las proyecciones sobre el cómputo cuántico, la suma de X e Y es frecuentemente suficientemente grande como para generar riesgo presente independientemente de qué estimación de Z resulte correcta. En esas condiciones, la respuesta adecuada no es esperar certeza sobre Z , sino reducir X e Y a través de una migración planificada. Para la región, el teorema tiene además una implicación directa de priorización: los sectores que gestionan datos de larga vida, defensa, salud, justicia, infraestructura financiera, encabezan la

agenda no porque la amenaza sea necesariamente más inminente en su caso, sino porque su X es mayor, lo que adelanta el umbral a partir del cual la desigualdad se viola.

7.2 Recomendaciones para gobiernos e instituciones de la región

Las recomendaciones que siguen están ordenadas por lógica operativa: las primeras sientan las bases institucionales sin las cuales las restantes no pueden ejecutarse; las siguientes definen las prioridades técnicas de la migración; y las últimas abordan las condiciones habilitantes de largo plazo. Todas parten de un reconocimiento común: la transición hacia la criptografía post-cuántica no es un proyecto tecnológico acotado, sino una transformación de infraestructura con dimensiones de gobernanza, recursos humanos, cadena de proveedores y cooperación regional.

- Definir responsabilidades y gobernanza institucional. Ninguna transición criptográfica de escala es posible sin un marco institucional que la sostenga. Esto implica, como condición mínima, designar un responsable con autoridad suficiente para impulsar decisiones transversales, establecer una hoja de ruta con hitos verificables y contar con patrocinio ejecutivo que garantice continuidad más allá de los ciclos políticos. En los contextos donde esa capacidad no existe o es incipiente, la prioridad es construirla antes de avanzar en la dimensión técnica: una migración sin gobernanza clara tiende a fragmentarse en iniciativas aisladas que no producen protección sistémica.
- Levantar y mantener un inventario criptográfico. No es posible migrar lo que no se conoce. El primer paso operativo de cualquier transición es un proceso de descubrimiento que mapee dónde se usa criptografía de clave pública, con qué algoritmos, en qué sistemas y qué tipo de información protege. Ese inventario no es un ejercicio puntual sino un activo dinámico: los sistemas cambian, los proveedores actualizan sus componentes y la superficie criptográfica de una institución evoluciona. Invertir en herramientas y procesos que mantengan ese inventario actualizado es una condición estructural de la transición, no una etapa que se completa y se cierra.
- Priorizar por longevidad del dato y exposición al SNDL. La migración no puede ni debe ocurrir simultáneamente en toda la infraestructura. El criterio de priorización más sólido combina dos dimensiones: la sensibilidad y vida útil del dato protegido, y la exposición real a los ataques de "almacenar ahora, descifrar después". Los sistemas que protegen información cuya confidencialidad debe sostenerse durante décadas, y que ya están siendo potencialmente interceptados y almacenados por actores con capacidad de largo plazo, deben encabezar la hoja de ruta. En la práctica, esto suele incluir comunicaciones diplomáticas, registros de infraestructura crítica, datos biométricos de ciudadanos y sistemas financieros con pasivos de largo plazo.
- Adoptar la agilidad criptográfica como principio de diseño. La incertidumbre sobre la velocidad del desarrollo cuántico y la posibilidad de que futuros avances afecten incluso a los algoritmos post-cuánticos hoy considerados sólidos hacen que la resiliencia de largo plazo no dependa únicamente de los algoritmos elegidos, sino de la capacidad para reemplazarlos

sin reingeniería completa. Diseñar sistemas con agilidad criptográfica, es decir, con la capacidad de intercambiar el algoritmo subyacente de manera modular, convierte a la transición en un proceso gestionable en lugar de un evento disruptivo. Este principio aplica tanto a nuevos sistemas como a aquellos en proceso de renovación: incorporar agilidad criptográfica en la etapa de diseño tiene un costo marginal muy inferior al de retroajustarla una vez que los sistemas están operativos.

- Migrar hacia los estándares ya finalizados y seguir los calendarios de referencia. La publicación de los estándares NIST en agosto de 2024 (FIPS 203, FIPS 204 y FIPS 205), junto con la incorporación del HQC en 2025, elimina una de las principales justificaciones para la demora: la incertidumbre sobre cuáles algoritmos adoptar. Los gobiernos e instituciones de la región deben establecer planes de migración alineados con los calendarios que los principales socios internacionales han comenzado a fijar, que apuntan a completar la transición de los sistemas más críticos entre 2030 y 2035. Esperar a que esos calendarios sean mandatorios equivale, en muchos casos, a violar la desigualdad de Mosca para datos que ya están siendo almacenados.
- Involucrar a proveedores y establecer requisitos en compras públicas. Una proporción significativa de la infraestructura criptográfica de los gobiernos no es desarrollada internamente sino adquirida a proveedores de software, hardware y servicios en la nube. La migración post-cuántica requiere, por tanto, trasladar las exigencias al ecosistema de proveedores: incorporar requisitos de compatibilidad con los estándares NIST en los pliegos de licitación, exigir hojas de ruta de transición a los proveedores actuales y preferir soluciones con agilidad criptográfica incorporada en los procesos de compra. Las instituciones con capacidad de articular estas exigencias tienen, adicionalmente, la posibilidad de generar efecto de arrastre sobre el mercado regional de tecnología.
- Desarrollar capacidades y promover la cooperación regional. La transición post-cuántica requiere perfiles técnicos que hoy son escasos en la región: especialistas en criptografía aplicada, en auditoría de inventarios criptográficos y en integración de algoritmos post-cuánticos en arquitecturas de sistemas existentes. Desarrollar esas capacidades no puede depender exclusivamente de la formación interna de cada institución: la cooperación regional, el intercambio de metodologías y la construcción de programas conjuntos de formación son mecanismos más eficientes para generar masa crítica. Los mecanismos de cooperación sur-sur y las plataformas de intercambio técnico entre países de la región tienen un rol específico e irremplazable en este proceso.
- Coordinar entre sectores. La infraestructura criptográfica de un país no pertenece a un único actor institucional: bancos centrales, telecomunicaciones, salud, defensa y sistemas de identidad comparten protocolos, proveedores y, en muchos casos, infraestructura. Una migración sectorial no coordinada puede crear puntos de quiebre en las interfaces entre sistemas que ya migraron y sistemas que todavía no lo han hecho. La coordinación intersectorial, con instancias formales de articulación y criterios comunes de priorización, es una condición de integridad de la transición a escala nacional.

7.3 Actores multilaterales y posición institucional del BID

La transición hacia la criptografía post-cuántica plantea desafíos que ningún país de la región puede abordar de manera completamente autónoma: escasez de capacidades técnicas especializadas, asimetría de recursos entre economías grandes y pequeñas, fragmentación regulatoria y dependencia de proveedores globales de tecnología. En ese contexto, los organismos multilaterales tienen un rol habilitante que va más allá del financiamiento y que abarca la producción de bienes públicos regionales: estándares, metodologías, marcos regulatorios y plataformas de intercambio de conocimiento.

En el plano global, las agencias del sistema de Naciones Unidas ofrecen espacios de articulación normativa y técnica de particular relevancia. La Unión Internacional de Telecomunicaciones (UIT) ha incorporado la preparación post-cuántica en su agenda de estándares para infraestructura digital, y sus marcos de evaluación de madurez pueden servir como punto de partida para diagnósticos nacionales en la región. La UNESCO, desde su mandato en ética de tecnologías emergentes, aporta el marco conceptual para abordar las dimensiones de gobernanza y equidad de acceso. La Organización para la Cooperación y el Desarrollo Económicos (OCDE), por su parte, ha publicado lineamientos sobre innovación responsable en tecnologías de seguridad relevantes para el diseño de marcos regulatorios nacionales.

En el ámbito regional, la CARICOM enfrenta una situación que merece atención diferenciada. Sus economías miembros, en su mayoría pequeños estados insulares, combinan alta dependencia de infraestructura digital para servicios públicos y turismo con capacidades técnicas y presupuestarias limitadas para gestionar una transición criptográfica compleja. El riesgo de que la brecha post-cuántica se profundice entre las economías más grandes de la región y los estados del Caribe es real, y requiere mecanismos específicos de cooperación técnica y financiera, incluyendo plataformas compartidas de inventario y migración que reduzcan los costos unitarios de la transición para estos países.

El Banco Mundial puede movilizar recursos para la etapa de inversión más intensiva, con instrumentos de asistencia técnica especialmente relevantes para el diseño de marcos regulatorios y la construcción de capacidades en los países de menor desarrollo relativo. El Fondo Monetario Internacional (FMI) tiene un canal de influencia específico en el sector financiero: la incorporación del riesgo post-cuántico en los Programas de Evaluación del Sector Financiero (PESF) y en los marcos de supervisión prudencial puede acelerar la acción de bancos centrales e instituciones financieras con mayor eficacia que cualquier recomendación técnica aislada. La Organización de los Estados Americanos, a través del Comité Interamericano contra el Terrorismo (CICTE) y su programa de ciberseguridad, dispone de canales de articulación con las agencias de seguridad y los equipos de respuesta a incidentes (CSIRT) de los países miembros que pueden servir para institucionalizar la dimensión post-cuántica dentro de las agendas nacionales.

7.3.1 Tecnología corporativa en el BID

El BID ocupa en este proceso una posición singular: es simultáneamente una institución que debe gestionar su propia transición criptográfica y un actor con capacidad de acompañar a los países miembros en la suya. Esas dos dimensiones se refuerzan mutuamente: la credibilidad del Banco como acompañante de la transición en la región depende, en parte, de su capacidad para recorrer ese camino de manera rigurosa en su propia infraestructura.

La mayor oportunidad para avanzar hacia esquemas resistentes al cómputo cuántico está en la gestión de dos factores: los datos cuya confidencialidad debe sostenerse más de una década, expuestos por tanto a los ataques SNDL, y los sistemas con ciclos de renovación planificados, donde incorporar agilidad criptográfica cuesta una pequeña parte de lo que costaría una reingeniería posterior.

En el equipo de ciberseguridad del departamento de Tecnología y Transformación Digital (TTD) del BID se está aplicando esta aproximación. Ya se ha iniciado la fase de descubrimiento e inventario criptográfico de los sistemas corporativos para identificar dónde se usa criptografía de clave pública, con qué algoritmos y qué información protege. El proceso exige cumplir tres condiciones: patrocinio ejecutivo con gobernanza clara y un responsable designado; visibilidad a través de un inventario actualizado de sistemas criptográficos; y estándares de referencia claros, actualmente los publicados por el NIST en 2024, alineados con los calendarios de los principales socios internacionales, que apuntan a completar la migración de los sistemas críticos entre 2030 y 2035.

El primer paso concreto es el inventario, priorizando por longevidad del dato: no todo debe migrar a la vez, pero es necesario saber qué migrar primero. El papel del Banco empieza por predicar con el ejemplo, recorrer el camino y compartir metodología y lecciones aprendidas con las instituciones de la región a través de iniciativas conjuntas como este informe.



Conclusión

8. Conclusión

Este reporte partió de una premisa simple, pero con implicancias profundas: la criptografía de clave pública, que durante más de cuatro décadas sostuvo la confianza digital global, enfrenta en la computación cuántica una amenaza estructural con un horizonte de materialización cada vez más próximo. Esa amenaza no es hipotética ni exclusivamente futura: bajo la lógica del “store now, decrypt later”, la exposición de información sensible ya está, en los hechos, en marcha, incluso antes de que exista una computadora cuántica capaz de explotarla plenamente.

Frente a esa amenaza, el reporte abordó el concepto de la criptografía cuántica, que utiliza principios de la física como superposición, entrelazamiento y el teorema de no clonación para proteger la información y detectar cualquier intento de interceptación. A su vez, se introduce la noción de criptografía post-cuántica, que reemplaza los problemas matemáticos vulnerables por otros, como los basados en retículas, que ni las computadoras clásicas ni las cuánticas logran resolver de forma eficiente. De las dos, la segunda ofrece hoy la ruta de adopción más viable a corto y mediano plazo, precisamente porque no exige la infraestructura física especializada que sí requiere la primera.

La selección, en 2022, de los primeros cuatro algoritmos del estándar post-cuántico del NIST marcó el inicio formal de una migración que, sin embargo, está lejos de completarse: como se discutió a lo largo del reporte, sustituir un algoritmo de cifrado exige identificar dónde se usa la criptografía de clave pública a lo largo de sistemas financieros, gubernamentales, de salud, de infraestructura crítica y de comercio exterior, y coordinar esa transición con una multiplicidad de actores que no siempre comparten cronogramas ni capacidades.

América Latina y el Caribe aún no desempeñan un papel protagónico en el desarrollo de hardware cuántico ni en la definición de los nuevos estándares, una brecha que podría profundizar su dependencia externa en decisiones clave para la seguridad de su información más sensible. Pero esa misma etapa temprana del proceso global, en la que los marcos de gobernanza, las estrategias de migración y las prácticas de agilidad criptográfica todavía se están definiendo, representa una oportunidad concreta de incidencia, siempre que la región actúe con la urgencia que el horizonte de riesgo, estimado entre cinco y veinte años, exige.

Esta transición involucra mucho más que ecuaciones y protocolos: compromete la protección de datos que, una vez expuestos, no pueden protegerse retroactivamente; interpela el equilibrio entre las capacidades de vigilancia estatal y los derechos de privacidad; y plantea preguntas de equidad sobre quién tiene la capacidad institucional de migrar a tiempo y quién no. Atender estas dimensiones será tan determinante para el resultado final de esta transición como la solidez de los algoritmos que la sostienen.



Referencias

9. Referencias

- Chen, Y.-A. et al. (2021). Una red integrada de comunicación cuántica tierra-espacio a lo largo de 4.600 kilómetros. Nature, 589, 214–219. <https://www.nature.com/articles/s41586-020-03093-8><https://www.nature.com/articles/s41586-020-03093-8>
- Gidney, C. (2025). How to factor 2048-bit RSA integers in less than a week using less than a million noisy qubits. arXiv. <https://doi.org/10.48550/arXiv.2505.15917>
<https://doi.org/10.48550/arXiv.2505.15917>
- IBM. (s.f.). ¿Qué es el cifrado homomórfico? IBM Think. <https://www.ibm.com/es-es/think/topics/homomorphic-encryption><https://www.ibm.com/es-es/think/topics/homomorphic-encryption>
- El País. (2026, 5 de junio). Aram Harrow, investigador cuántico: "No quedan 10 años para estos ordenadores, llegarán antes". El País Tecnología. <https://elpais.com/tecnologia/2026-06-05/aram-harrow-investigador-cuantico-no-quedan-10-anos-para-estos-ordenadores-llegaran-antes.html>
<https://elpais.com/tecnologia/2026-06-05/aram-harrow-investigador-cuantico-no-quedan-10-anos-para-estos-ordenadores-llegaran-antes.html>
- Mosca, M., & Piani, M. (2015). Quantum threat timeline. Cryptology ePrint Archive, Paper 2015/1075. <https://eprint.iacr.org/2015/1075><https://eprint.iacr.org/2015/1075>
- National Institute of Standards and Technology (NIST). (2025) What is quantum cryptography? NIST Cybersecurity. <https://www.nist.gov/cybersecurity-and-privacy/what-quantum-cryptography>
<https://www.nist.gov/cybersecurity-and-privacy/what-quantum-cryptography>
- National Security Agency. (2022, September). Commercial National Security Algorithm Suite 2.0. U.S. Department of Defense. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF
- Veritasium. (2023). How quantum computers break the internet... starting now [video]. YouTube. <https://www.youtube.com/watch?v=-UrdExQW0cs>
<https://www.youtube.com/watch?v=-UrdExQW0cs>
- WeLiveSecurity by ESET. (2019, September 4). Homomorphic encryption: the closest encryption paradigm. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2019/09/04/criptografia-homomorfica-paradigma-cifrado-cercano/>
<https://www.welivesecurity.com/la-es/2019/09/04/criptografia-homomorfica-paradigma-cifrado-cercano/>