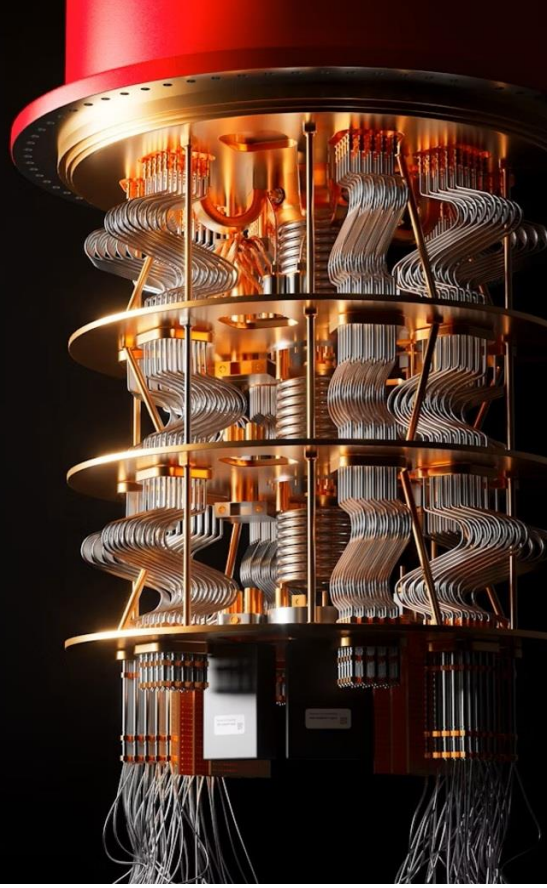
la amenaza de la Computación Cuántica al sistema bancario

riesgos, urgencias y soluciones



migración a infraestructura de seguridad poscuántica

ABAPPRA
ASOCIACIÓN DE BANCOS PÚBLICOS Y PRIVADOS DE LA REPÚBLICA ARGENTINA

UNIVERSIDAD NACIONAL DE ROSARIO
FACULTAD DE CIENCIAS ECONÓMICAS Y ESTADÍSTICA
UNR

UNIVERSIDADE SALVADOR
UNIFACS

Índice de contenidos

1 resumen

Si bien las innovaciones en Blockchain e inteligencia artificial han provocado profundas transformaciones en la actividad bancaria, la tecnología que promete generar los cambios más drásticos en la gestión, análisis y seguridad del universo financiero es **la computación cuántica.**

Ya se sabe, con certeza, que el increíble poder de cómputos que tendrá el procesador cuántico le permitirá quebrar la infraestructura de seguridad actual.

Pero **la amenaza no es solo a futuro**. **Es actual.** Un informe reciente del BIS (Banca de Basilea) advierte sobre la estrategia "cosechar ahora para desencriptar luego". La posibilidad cierta que, en unos años cuando se cuente con un procesador cuántico "relevante", se desencripte la información confidencial de transacciones y comunicaciones actuales **es un riesgo inaceptable en términos de la confianza, pilar central del sistema financiero**.

Este documento presenta un resumen ejecutivo analizando la urgencia de parte de los bancos de iniciar **la migración de su infraestructura de seguridad a PQC - Criptografía Poscuántica**.

2 amenaza

supremacía cuántica
amenaza futura
amenaza actual

“la computación cuántica, podría ser un "evento de nivel de extinción" (extinction-level event) para los sistemas criptográficos actuales si las industrias no actúan rápidamente”

Amit Sinha, DigiCert

2 amenaza

“supremacía” cuántica

John Preskill, físico de partículas que acuño el término “supremacía cuántica”

El término “supremacía” cuántica fue acuñado por el físico de partículas John Preskill, y hace referencia a la capacidad del computador cuántico de realizar cálculos increíblemente más complejos que las computadoras actuales, abriendo posibilidades sin precedentes para solucionar problemas que actualmente resultan irresolubles.

Las instituciones financieras enfrentan actualmente desafíos computacionales que incluyen la **optimización de carteras de inversión, complejos análisis de riesgos, la detección de fraudes en tiempo real y la modelación de escenarios económicos predictivos**.

La computación cuántica ofrecerá la posibilidad de abordar estas temáticas con una eficiencia y precisión sin precedentes, reduciendo significativamente el tiempo de análisis de la big data. La consecuencia lógica de esto será la necesidad por parte de los bancos de adaptarse a escenarios más cambiantes, donde la ventaja competitiva que brindan estas sofisticadas herramientas tecnológicas se tornará un factor excluyente.

Sin bien, la futura implementación de la computación cuántica en el sector bancario presentará oportunidades extraordinarias, **también tiene asociada riesgos considerables que deben ser rápidamente abordados**.

El riesgo potencial más acuciante está vinculado a su capacidad para quebrar los algoritmos de encriptación actuales. **Esto le permitirá volver obsoletos y vulnerables a casi la totalidad de los sistemas de seguridad que usamos.**

amenaza futura

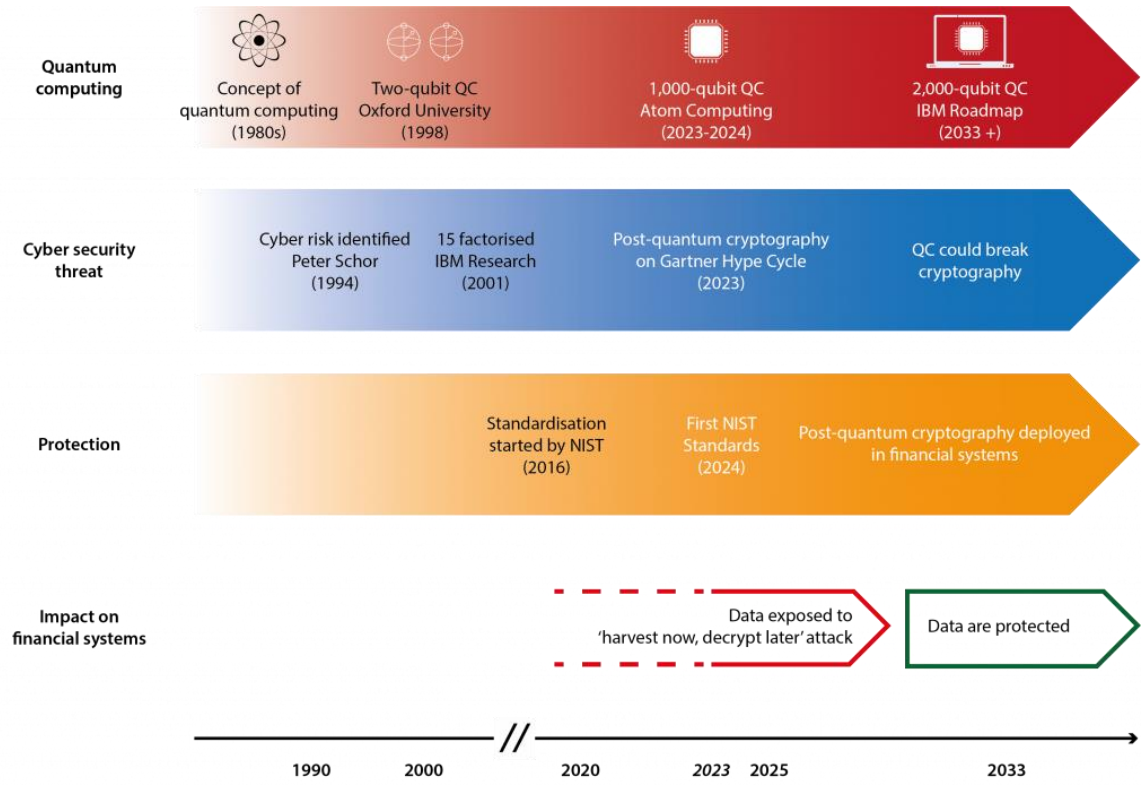
Se ha definido como **el “Q-Day” (Quantum Day)** al momento en que se cuente con un computador cuántico de relevancia criptográfica (CRQC), estable y con **capacidad de quebrar los algoritmos de encriptación utilizados en la actualidad**.

En 1995 Peter Shor, publicó lo que se conoce como “el algoritmo de Shor”, el desarrollo que permitirá al computador cuántico quebrar la encriptación actual, como la de los algoritmos RSA y de Curva Elíptica, utilizados en todo el mundo financiero y por las principales criptomonedas respectivamente.

¿cuándo se estima que ocurrirá el Q-Day?

La fecha aproximada es difícil de estimar. Autores optimistas la ubican en 2028 (en dos años) otros más moderados creen que entre el 2030 y 2035 (entre cuatro y nueve años), mientras que los más pesimistas la sitúan más allá del 2035.

La disparidad de las estimaciones es consecuencia de una enorme complejidad de factores que se deben considerar. Algunos de estos factores son: la diversidad de enfoques técnicos de implementación con los que se trabaja (superconductores, trampas de iones, fotones, spin, y otros), la estabilidad de los “estados cuánticos” que se consiguen (cuanto tiempo se mantienen estables) y la tasa de errores que el procesador genera.



Amenazas de la computación cuántica a los sistemas financieros. Extraído de "BIS Papers No 149 - Quantum computing and the financial system: opportunities and risks" (octubre 2024).

En la segunda línea (Cyber security threat) se puede observar un pronóstico tentativo de ocurrencia del "Q-Day" para alrededor del ***año 2030.***

amenaza actual

"La clave es estar en este viaje hoy y no esperar hasta el último minuto"

Rob Joyce, director de Ciberseguridad de la ***NSA – National Security Agency USA***

Independientemente del momento en que ocurra el Q-Day y se pueda quebrar la criptografía actual, organismos internacionales están advirtiendo sobre la necesidad de comenzar a migrar a infraestructura de seguridad poscuántica, lo antes posible.

Estos organismo ponen foco en la estrategia de HNDL – Cosechar ahora para desencriptar luego (por sus siglas en inglés).

¿En qué consiste un ataque HNDL?:

Confiamos en la confidencialidad de información de transacciones, comunicaciones y todo tipo de mensajes que intercambiamos por internet, ya que dicha información viaja encriptada y por canales seguros. Pero todos esos datos pueden estar siendo almacenados por actores maliciosos, para desencriptarlos cuando se cuente con un CRQC (computador cuántico relevante).

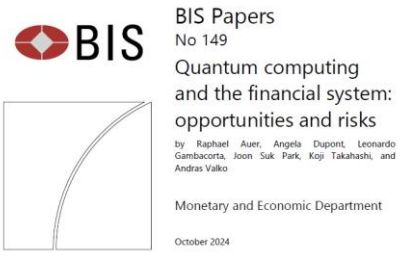
El uso de esta estrategia como forma de ciber-ataque en contra de bancos e instituciones financieras puede tener un efecto catastrófico. No solo habría que **considerar la cantidad de acciones legales de clientes contra sus bancos, por no preservar el secreto bancario**, sino también pensar en un **quiebre de la confianza en el sistema financiero** en gran escala. De allí la necesidad de **mitigar este riesgo con la mayor urgencia**.

Algunos de los organismos internacionales que se encuentran advirtiendo sobre la urgencia de comenzar la migración a infraestructura de seguridad poscuántica a causa de ataques vinculados a HNDL – cosechar ahora para desencriptar luego, son:

Organismo	Fecha	Documento
Federal Reserve USA	Setiembre 2025	"Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks
CISA, NSA y NIST (Conjunto)	Agosto 2023	QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY
World Bank	Diciembre 2024	PKI implementing high-trust electronic signatures
IMF – International Monetary Fund	2021	[IMF] QUANTUM COMPUTING'S POSSIBILITIES AND PERILS

Organismos internacionales relevantes que están advirtiendo sobre el ataque HNDL – cosechar ahora para desencriptar luego

En el sector bancario, el BIS – Banco para Pagos Internacionales, ha emitido varios trabajos advirtiendo a los bancos, ante los ataques de HNDL, sobre **la necesidad de iniciar urgentemente la migración a infraestructura de seguridad poscuántica (PQC)**:



BIS Papers 149 – "Quantum Computing and financial system: opportunities and risks" advierte la urgencia a los bancos de migrar a PQC

[BIS] PROJECT LEAP Quantum-proofing the financial system, June 2023:

"Cualquier dato que requiera protección criptográfica a largo plazo (es decir, todos los datos que deban mantenerse seguros y privados durante más de 10 años) requerirá protección post-cuántica lo antes posible, especialmente si se almacena fuera de las instalaciones (por ejemplo, en la nube).
Este riesgo cibernético tendría consecuencias perjudiciales para el sistema financiero. Es fundamental considerar este riesgo y las vulnerabilidades derivadas que podrían afectar la estabilidad financiera".

[BIS] Quantum computing and the financial system opportunities and risks, October 2024:

"Hasta que las soluciones de seguridad cuántica se implementen por completo, la vulnerabilidad de los datos altamente sensibles a los ataques HNDL sigue siendo una preocupación crítica. Esta amenaza inminente subraya la necesidad urgente de medidas preventivas para salvaguardar la autenticidad, la integridad y la confidencialidad de los datos".

[BIS] Quantum-readiness for the financial system - a roadmap, July 2025:

"Los ataques HNDL pueden provocar filtraciones de datos y la futura divulgación de información altamente confidencial".

3 criptografía

cuáles sistemas se volverán vulnerables
a la criptografía poscuántica

3 criptografía

cuáles sistemas se volverán vulnerables

La criptografía se define como *"el estudio de técnicas matemáticas para asegurar la información digital, sistemas, y cómputos distribuidos contra ataques de adversarios"*

J. Katz, Y. Lindell - Introduction to Modern Cryptography

La criptografía no busca formular un problema matemático imposible de resolver, sino uno que requiera de un poder de cómputo tan inmensamente grande que no tenga sentido, siquiera, analizar la posibilidad de intentar resolverlo. La disrupción de la computación cuántica en este punto es que va a contar con ese poder de cómputos tan significativo.

Las técnicas matemáticas que menciona la definición son implementadas por medio de algoritmos pensados para distintas finalidades. Por ejemplo: la técnica matemática de factorización en números primos es usada por el algoritmo RSA, y la técnica matemática de cálculo de curva elíptica es usada por el algoritmo ECC.

Esos algoritmos se agrupan en protocolos y estándares para funcionalidades específicas. Por ejemplo, el protocolo TLS/SSL que implementa RSA (o semejantes), permite comunicación segura por Internet. Así lo encontramos en HTTPS (páginas web seguras), e-mail, VPN seguras, Apps móviles, Web services, entre otros.

Sobre todo este andamiaje se montan los servicios bancarios actuales: gestión de cuentas, inversiones, adquisición de moneda extranjera, líneas de préstamos, tarjetas de crédito, débito, pagos contact-less, e-checks, evaluaciones y scoring crediticio, KYC, pasarelas de pago, autenticación de usuarios, finanzas embebidas y super Apps financieras, solo para mencionar algunos.

El algoritmo de Shor (ya probado en escala acotada en computador cuántico) y el algoritmo de Groove son los principales que permiten quebrar la criptografía basada en factorización en números primos, curva elíptica y otros.

De esta manera, **pueden hacer caer los servicios bancarios** que mencionados **como una casa de naipes,** y a **casi la totalidad de la infraestructura de seguridad de los sistemas bancarios actuales**

Modelo de la infraestructura de seguridad bancaria actual, que será vulnerable a los ataques de computación cuántica

PQC: criptografía poscuántica

En 2016, el **NIST - Instituto Nacional de Estándares y Tecnología de USA** anunció la realización de un concurso público para seleccionar **algoritmos criptográficos resistentes a la computación cuántica**.

Se presentaron más de 80 algoritmos de encriptación en un proceso colaborativo en el que participaron expertos de todo el mundo. En varias rondas competitivas, la comunidad científica probó los algoritmos propuestos.

En 05 de julio de 2022, **tras seis años de competencias y análisis**, el NIST realizó el anuncio de la selección de los **primeros 4 algoritmos de criptografía poscuántica**:

Algoritmo	Descripción	Propósito
CRYSTALS-Kyber	Entre sus ventajas están las claves de cifrado comparativamente pequeñas que dos partes pueden intercambiar fácilmente, así como su velocidad de operación.	Propósito general
CRYSTALS-Dilithium	Los algoritmos de firma digital se utilizan a menudo cuando necesitamos verificar identidades durante una transacción digital o firmar un documento de forma remota. NIST recomienda CRYSTALS-Dilithium como algoritmo principal.	Firma digital
FALCON	Se recomienda FALCON para aplicaciones que requieren firmas más pequeñas que las que puede proporcionar el Dilithium.	Firma digital
SPHINCS+	SPHINCS+, es algo más grande y lento que los otros dos, pero es valioso como respaldo por una razón principal: se basa en un enfoque matemático diferente al de las otras tres selecciones del NIST.	Firma digital

***Algoritmos poscuánticos seleccionados por NIST luego de 6 años de análisis* (Basado en comunicación oficial NIST 05/07/2022)**

FIPS 203

Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)

FIPS 204

Module-Lattice-Based Digital Signature Standard (ML-DSA)

FIPS 205

Stateless Hash-Based Digital Signature Standard (SLH-DSA)

En agosto de 2024, el NIST publicó los primeros 3 estándares de PQC - criptografía poscuántica (FIPS - Federal Information Processing Standards) basados en los algoritmos candidatos que fueron seleccionados a través del proceso de 6 años:

FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard

FIPS 204: Module-Lattice-Based Digital Signature Standard

FIPS 205: Stateless Hash-Based Digital Signature Standard

Estándar	Denominación	Descripción
FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard	especifica un mecanismo de encapsulación de claves (genera una clave secreta compartida por medio de un canal público) llamado ML-KEM. La seguridad de ML-KEM está relacionada con la dificultad computacional del problema de Aprendizaje del Módulo con Errores. Puede utilizarse para realizar tareas básicas en comunicaciones seguras, como cifrado y autenticación.
FIPS 204	Module-Lattice-Based Digital Signature Standard	especifica ML-DSA, un conjunto de algoritmos que pueden utilizarse para generar y verificar firmas digitales. Las firmas digitales se utilizan para detectar modificaciones no autorizadas de datos y autenticar la identidad del firmante
FIPS 205	Stateless Hash-Based Digital Signature Standard	especifica el algoritmo de firma digital basado en hash sin estado (SLH-DSA)

Estándares de criptografía poscuántica (PQC) aprobados por MIST hasta el momento

4 migración

consideraciones
proceso de migración

4 migración

consideraciones

¿cómo debería un banco encarar un plan de migración a PQC?

El BIS (banca de Basilea) emitió en julio 2025 el documento **"Quantum-readiness for the financial system - a roadmap"**, donde se presenta una hoja de ruta integral para que autoridades, bancos centrales, instituciones financieras y proveedores tecnológicos desarrollen estrategias de preparación para PQC.

Algunos aspectos destacados del documento son:

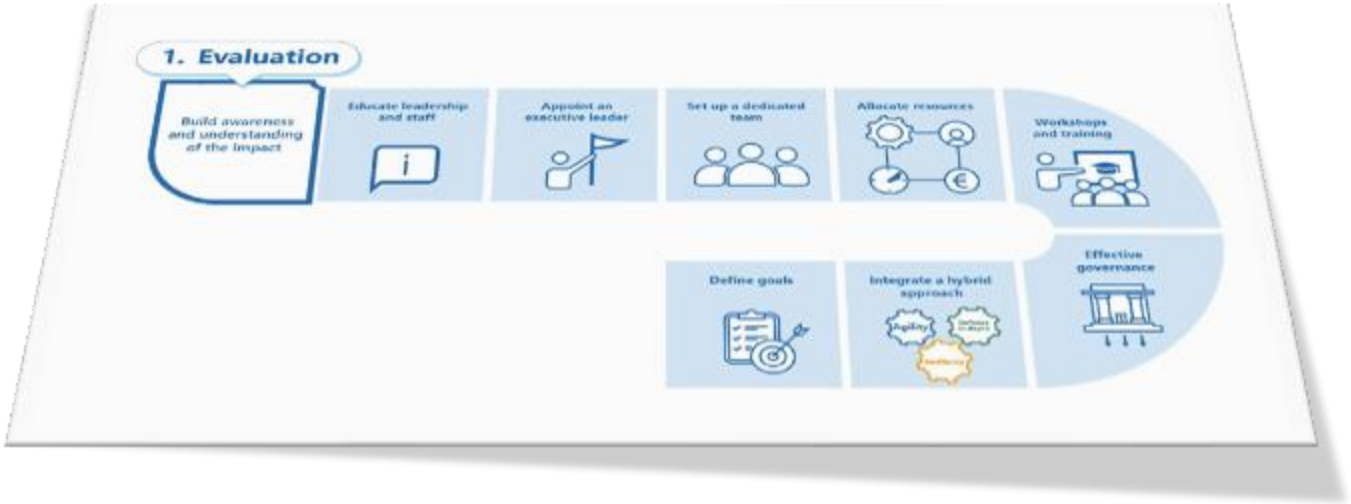
Interdisciplinaridad: "*Un enfoque bien coordinado garantiza que todas las facetas de la organización estén alineadas para abordar los múltiples riesgos y desafíos que plantea la computación cuántica, en lugar de considerarla una simple actualización técnica*". "*El equipo debe incluir representantes de los departamentos de tecnología, legal, recursos humanos, finanzas, operaciones y seguridad*"

Gobernanza: "*Como parte de los pasos preparatorios, se deben establecer estructuras de gobernanza para guiar la toma de decisiones y la coordinación durante todo el proceso de migración. El marco de gobernanza promoverá la coherencia entre las divisiones y garantizará el cumplimiento de los objetivos generales de seguridad y resiliencia de la institución*"

Relevamiento: "*Desarrollar un inventario criptográfico es un paso crucial para mapear el panorama criptográfico de la institución. Las herramientas de descubrimiento automatizado pueden identificar cómo y dónde se utiliza la criptografía en toda la infraestructura, incluyendo los sistemas locales y en la nube*"

PCQ Agility: "*Un ciclo de evaluación continua respalda el éxito a largo plazo. A medida que las tecnologías cuánticas evolucionan, las instituciones financieras deben revisar sus estrategias criptográficas, actualizar sus evaluaciones de riesgos y perfeccionar sus implementaciones. Este enfoque adaptativo promueve la agilidad institucional y ayuda a mantener la resiliencia ante las amenazas emergentes*"

De esta forma propone un plan de migración a PQC centrado en tres fases:



1. Sensibilización interna y evaluación del proceso

La fase inicial de sensibilización remarca la necesidad para la organización de iniciar un dialogo estratégico sobre la migración.

Actividades que se identifican en esta fase:

1. Educar a los líderes y al personal
2. Establecer quien será el líder ejecutivo
3. Seleccionar el equipo dedicado
4. Asignar recursos
5. Workshops y capacitación
6. Gobernanza efectiva
7. Decidir si se realiza una aproximación híbrida o no
8. Definición de objetivos

2. Planificación de la migración

Planificar la migración a la criptografía cuántica segura requiere una comprensión integral de cómo y dónde se utiliza la criptografía dentro de la institución. Actividades que se identifican en esta fase:

1. Identificación de sistemas críticos y datos sensibles
2. Migraciones prioritarias
3. Dependencias de activos y enganche con proveedores externos
4. Definir soluciones quantum-safe con sus respectivos casos de uso
5. Revisión de políticas de seguridad y procesos de evaluación de riesgo
6. Definición de líneas de tiempo e hitos
7. Lanzamiento de pilotos, testing de perfomance e interoperabilidad
8. Definición del presupuesto de largo plazo
9. Ajustar hojas de ruta
10. Seguimiento de progreso en estándares y guías prácticas
11. Cooperación para aseguramiento de interoperabilidad

3. Implementación

La migración a sistemas con seguridad cuántica es un proceso iterativo que evoluciona junto con la planificación continua. La implementación debe comenzar con los sistemas identificados como de alta prioridad o aquellos con soluciones de resistencia cuántica bien probadas. Actividades que se identifican en esta fase:

1. Desarrollo de herramientas automatizadas
2. Actualización de sistemas
3. Testing y validación continua
4. Implementación en producción
5. Preparación de mediciones
6. Evaluación continua de rendimiento
7. Cooperación continua con partes externas

proceso de migración

Otros organismos internacionales han sugerido guías y buenas prácticas para el momento de encarar un proceso de migración a PQC. En base a esos saberes, y experiencias la hoja de ruta que se detalla a continuación pone en consideración una secuencia de 10 actividades que entendemos ineludibles para el éxito del proceso de migración a PQC:

CAPACITACIÓN DE RRHH

La primera actividad sugerida en un proceso de migración a PQC es la de capacitación del personal de la institución bancaria.

Además del objetivo primario de la transferencia de conocimientos esenciales, se debe considerar el desarrollar competencias técnicas y de negocio que permitan comprender la **dinámica de nuevos estándares criptográficos, gestión de riesgos, métodos de resiliencia y planeamiento de la/s fases de transición de la migración**.

La capacitación no se debe concebir como una etapa cerrada, sino como un continuo (ver etapa PQC Agility). Es aconsejable complementar los contenidos teóricos que se brinden, con **talleres prácticos, simulaciones de incidentes cuánticos, detección de vulnerabilidades y planificación de tests de pruebas**. Es sugerido que la capacitación se enfoque en forma transversal a las diferentes áreas, ciberseguridad, TI, redes, riesgo operativo, auditoría, desarrollo de productos y cumplimiento regulatorio, entre otros. Es decir, **tanto personal técnico, como de negocio**.

Algunos de los contenidos mínimos a incluir son:

- ✓ tipos de algoritmos criptográficos actuales,
- ✓ servicios y productos bancarios en que se utilizan,
- ✓ capas de infraestructura de seguridad bancaria y sus vulnerabilidades,
- ✓ flujos de negocio afectados por ataques cuánticos,
- ✓ inventario de activos digitales,
- ✓ estándares de PQC, marco regulatorio y compliance,
- ✓ estrategias y diseño de plan de migración,
- ✓ técnicas de testeo,
- ✓ QA (quality assurance) de la migración,
- ✓ PQC Agile, entre otros.

EQUIPO DE TRABAJO

La migración a PQC-criptografía poscuántica no es sólo un proyecto tecnológico: implica cambios en seguridad, arquitectura, cumplimiento, procesos de negocio, diseño de productos bancarios, gestión de proveedores y gobernanza institucional. Por ello es clave para gestionarla, conformar un equipo de trabajo multidisciplinario.

Un factor importante para considerar es que del equipo que se integre para gestionar la migración original, se conformará posteriormente el de PQC Agility.

No existe una composición única de equipo para gestionar la migración a PQC. En tanto que cada institución bancaria tiene modelos de negocio, productos y servicios bancarios, planes estratégicos y operativos diferenciados. Incluso una cultura organizacional propia.

Sin perjuicio de esto, roles y responsabilidades a considerar como impostergables son:

- ✓ encargados de definición de lineamientos estratégicos, prioridades, presupuesto y tiempos para todo el programa cuántico del banco.
- ✓ equipo ejecutor, coordinador y seguimiento del proceso
- ✓ encargados de diseño técnico de la arquitectura y seguridad PQC (arquitectos de soluciones, infraestructura y redes, datos, Q-PKI, certificados)
- ✓ desarrollo y adecuación de aplicaciones (back-end, front-end, despliegues, integraciones: APIs, Web-services…)
- ✓ responsables de infraestructura crítica y hardware (HSM, ATMs, tarjetas, TLS, y otros dispositivos)
- ✓ equipo a cargo de gestión de riesgo, cumplimiento, auditoria y gobierno
- ✓ gestión y aseguramiento de servicios de proveedores y otros servicios externos
- ✓ QA, Testing e Interoperabilidad
- ✓ PQC Agility, como continuación del proceso de migración

INVENTARIO DE ACTIVOS DIGITALES

La comunicación A-7724 de BCRA establece la obligación para entidades financieras de "*mantener un inventario detallado de sus activos de información*" y por otra parte establece, en referencia a esos activos que se deberán considerar "*Vulnerabilidades y necesidades de actualización y reemplazo*".

Es por esto por lo que esta etapa del proceso de migración a QPC, no es ajena a las entidades bancarias.

Sin embargo, es importante destacar que se deberá relevar detalladamente los estándares y algoritmos criptográficos vinculados a cada uno de estos activos digitales, con la finalidad de poder evaluar en la etapa siguiente el grado de vulnerabilidad expuesto ante ataques cuánticos.

INVENTARIO DE VULNERABILIDADES

Una vez que se haya realizado el relevamiento completo de los activos digitales es fundamental identificar el grado de vulnerabilidad de estos.

Es recomendable previamente clasificarlos en base a su sensibilidad (ej. públicos, confidenciales, restringidos, …)

Para identificar vulnerabilidades es necesario analizar todo el espectro de la infraestructura IT, propia, e incluso de terceros proveedores de servicios.

El documento de BIS, realiza la siguiente enunciación de capas de infraestructura, que se entiende no restrictiva, sino enunciativa:

CAPA	SISTEMAS / PROCESOS
Hardware	Hardware criptográfico
	Servicios de red
Firmware	Sistemas embebidos
Sistema Operativo	Kernel (núcleo)
	Dispositivos del sistema
Aplicaciones	Aplicaciones de software
	Navegadores web
	Emails
Redes	Protocolos
	Certificados

CAPA	SISTEMAS / PROCESOS
Datos	Bases de datos
	Sistemas de back-up
Seguridad	Gestores de acceso e identidad
	Autenticación y gestión de claves
	Gestores de eventos y seguridad
Desarrollo	Herramientas de desarrollo
	Revisores de código y testing
Gobernanza y Compliance	Políticas
	Auditorías y evaluación

ELECCIÓN DE MODELO

Cuando mencionamos PQC – Post-Quantum Cryptography nos estamos refiriendo a implementaciones de criptografía que soportan ataques cuánticos. Esto puede realizarse por medio de algoritmos que corren en un computador tradicional, pero que se ha comprobado que resisten ataques cuánticos (ej. los que mencionamos que fueron aprobados por NIST), o por algoritmos que solo pueden correr en un computador cuántico (ej. BB84 basado en la no clonación de estados cuánticos).

A su vez, la implementación puede realizarse también por medio de los denominados "modelos híbridos", donde las claves que se utilizan son generadas con algoritmos PQC, pero una vez generadas se implementan en algoritmos tradicionales. Estas soluciones se las conoce como "distribución de claves" QKD (Quantum Key Distribution). Existe una discusión acerca de si estos "modelos híbridos" son suficientemente robustos para ser considerados para su utilización, especialmente en sistemas de camino crítico como los del sector financiero.
Todas estas variantes, deberán ser analizadas, y evaluadas en términos de costo-beneficio, robustez, factibilidad de implementación, antes de pasar a la actividad siguiente de desarrollo de la estrategia de migración.

ESTRATEGIA DE MIGRACIÓN

Existen multiplicidad de factores que se deben considerar al desarrollarse la estrategia de migración a PQC. Algunos de los más importantes, son:

- ✓Participación activa y transversal de todas las áreas de la institución, a fin de lograr que se sientan involucrados en el proceso
- ✓Vinculado con el punto anterior, es vital lograr una clara y concisa comunicación de la estrategia y sus objetivos globales y particulares
- ✓Definir roles y alcances de los terceros involucrados, especialmente de los proveedores de IT y de servicios. Delinear en este último caso los SLA – Acuerdos de Nivel de Servicios
- ✓Decidir si la migración se realizará en forma incremental, en función de prioridades de sistemas críticos, en bloques, en coordinación con partners, u otras estrategias.
- ✓ Parámetros de QA (aseguramiento de calidad) y robustez exigidos a los sets de testing que se implementarán

PLAN DE MIGRACIÓN

Una vez definida la estrategia de migración se debe elaborar el plan, definiendo las migraciones específicas para cada activo de información / sistema, programando los tiempos en ambientes de desarrollo, testing y producción, los aislamientos (isolation) de servicios / sistemas y sus reemplazos.

Entre los factores más relevantes del plan de migración, se deberán considerar:

- ✓ **Alcance**: Entregables o informes a presentar. Criterios de aceptación / reformulación
- ✓ **Líneas de tiempo**: Actividades, sus duraciones, secuencias y solapamientos (Gantt). Hitos. Estimación de desvíos / retrasos
- ✓ **Financiero**: Costo total del proyecto. Desglose por actividades y prioridades. Posibles desvíos y tolerancia
- ✓ **QA**: Estándares de Calidad adoptados o parámetros generados. Proceso de aseguramiento de metas
- ✓ **Gestión de riesgos**: Identificación. Matriz de impacto. Planes de respuesta, resiliencia. Contingencias
- ✓ **Gestión con partners / proveedores**: cumplimientos a solicitar. SLA – Acuerdos de nivel de servicios.

En este último punto jugará un rol decisivo analizar la factibilidad, alcance e impacto de sustituir a partners / proveedores de servicios que no cumplimenten el aseguramiento de calidad y mitigación del riesgo que se les demande.

Se deberá considerar para esta evaluación, puntos de vulnerabilidad ante ataques cuánticos en la totalidad del linaje de datos que gestionen (trazabilidad completa), y todas las actividades de los procesos que brinden en sus aplicaciones / servicios, a la entidad bancaria.

EJECUCIÓN

Además de las tareas básicas de implementar los algoritmos PQC adoptados, se deberá poner foco especial en la coordinación de secuencialidad de actividades planeadas en base a: pasajes de aplicaciones entre ambientes de desarrollo, de testing, y de producción, cohabitación de soluciones híbridas (con criptografía tradicional - con criptografía PQC), ejecución de fases distribuidas según prioridades de activos de información, sucursales, sistemas críticos.

Un punto relevante en esta etapa será el de la generación, distribución y comunicación (según el caso) de nuevas claves criptográficas generadas con algoritmos PQC.

CONTROL

Antes del traspaso a ambiente de producción, se debe ejecutar y evaluar el set de pruebas individuales y de integración planificadas. La selección y el alcance de las pruebas tiene que considerar los distintos sistemas, toda la trazabilidad de datos y de procesos, la superficie de ataque, generación y distribución de claves y certificados, entre otros.

La evaluación que se realice de las pruebas ejecutadas debe contemplar, medición de eficiencia en términos computacionales, planes de desvíos y gestión de fallas, alcance de parámetros de aseguramiento de calidad.

PQC Agility

La Computación Cuántica, en términos de funcionamiento, conlleva la disrupción más grande que se haya generado en la historia de la computación. El principio de superposición en que se basa el procesador cuántico es lo que le permite alcanzar una potencialidad inimaginable. Pero simultáneamente, fuerza la reescritura de las aplicaciones con las que contamos actualmente que fueron desarrolladas para computadoras tradicionales. Esto obliga a generar nuevos algoritmos y desarrollos de software absolutamente innovadores.

Considerando la potencialidad casi ilimitada de su poder de cómputo, y la necesidad de creación de nuevas generaciones de algoritmos, es presumible que la QC despliegue una vertiginosa dinámica de cambio, incluso más acelerada de la que observamos actualmente.

Esto fuerza a las instituciones bancarias a planificar estrategias de rápida adaptabilidad, en términos de infraestructura de seguridad IT tales como PQC Agility.

Al respecto, el BIS (Basilea) define:

PQC Agility

"La agilidad cuántica se refiere a la capacidad de los sistemas criptográficos para adaptarse y realizar una transición fluida a algoritmos resistentes a la computación cuántica en respuesta a las amenazas emergentes que plantea la computación cuántica…

La agilidad cuántica permite a las organizaciones mantenerse adaptables en un panorama tecnológico en constante cambio."

BIS – Bank for International Settlements
Fully Scalable Settlement Engine (FuSSE)
Abril 2024

5 conclusiones

conclusiones

5 conclusiones

conclusiones

- ✓ La increíble capacidad de cómputos con que contaran los procesadores cuánticos (CRQC) les permitirá vulnerar la arquitectura de seguridad de los sistemas actuales. Este fenómeno que conocemos como "Amenaza de la Superioridad Cuántica", pondrá en jaque a casi la totalidad de los sistemas y a la comunicación actual, En términos de sustitución de identidades y confidencial puede ser un evento catastrófico para los sistemas que no se adecúen.
- ✓ La amenaza no solo es a futuro. Los ataques HNDL - *recolectar ahora para desencriptar luego*-, se están iniciando actualmente y significan a futuro la vulneración del secreto bancario, pilar esencial de la confianza en el sistema financiero.
- ✓ Es impostergable para los bancos iniciar sus procesos de migración a sistemas de criptografía poscuántica (PQC). Como primer paso, conformando sus equipos de migración para interiorizarse en los nuevos algoritmos criptográficos estandarizados (especialmente por NIST).
- ✓ Las estrategias y planes de migración que se desarrollen no podrán obviar el inventario de los Activos de Información, identificación de sus vulnerabilidades, gestión de riesgos y prioridades de migración, transitoriedad de soluciones híbridas y un énfasis destacado en la planificación y ejecución de robustas pruebas de testeo que aseguren la resistencia a ataques cuánticos.
- ✓ Ante la complejidad de las arquitecturas de software y comunicaciones actuales, será un factor prioritario asegurarse de la migración PQC exitosa de los sistemas, aplicaciones, servicios y comunicaciones contratados a terceros. De otra forma, la vulnerabilidad de sistemas de terceros será la puerta de entrada de ataques a los sistemas de la institución bancaria. El abordaje de una migración conjunta y colaborativa con los proveedores de servicios será esencial para la institución bancaria.
- ✓ Considerando la vertiginosa dinámica que se prevé de los sistemas cuánticos, es fundamental que no se considere al plan de migración PQC como un proyecto aislado y de ejecución única. Por el contrario, debería ser el puntapié inicial de un plan de PQC Agility que esté constantemente monitoreando y mitigando las variantes y nuevas amenazas cuánticas que se generen a futuro.

6 contacto

desarrollo
autores

6 contacto

desarrollo

El presente documento es un desarrollo realizado por UNR – Universidad Nacional de Rosario, Argentina en conjunto con UNIFACS, Universidade Salvador, Brasil, para ABAPPRA – Asociación de Bancos Públicos y Privados de la República Argentina.

Se ha implementado en el marco del Convenio de Cooperación que ABAPPRA posee con UNR, desde el año 2020.

autores

Daniel Díaz – UNR

Daniel es profesor de posgrado en la "Especialización en Gestión Estratégica de la Tecnología Informática (GETI)" y de grado en la asignatura "Tecnología de la Información (TI)" en UNR – Universidad Nacional de Rosario.
Se ha desempeñado como asesor de:

- ✓ Banco Central de la República Argentina (BCRA)
- ✓ Banco Central de Chile
- ✓ Banco Central del Uruguay
- ✓ Comisión Bancaria y Valores de México
- ✓ Secretaría del Tesoro Nacional de Brasil

Fue galardonado a nivel internacional por XBRL International Inc. y Oracle Corporation.
Posee una distinción de la Cámara de Diputados de la Nación de Argentina, por su labor en investigación.
Es capacitador de ABAPPRA en temas de tecnología como Blockchain, Tokenización, IA y Computación Cuántica.

Daniel Díaz <ddiaz@fcecon.unr.edu.ar>

@daniel-diaz-unr

Paulo Caetano da Silva – UNIFACS, Brasil

Paulo es profesor de la Maestría en Sistemas de computación y en MBA de UNIFACS - Universidade Salvador, Bahía, Brasil. Es funcionario del Banco Central de Brasil, desde 1994. Actualmente se desempeña en la implementación de Compliance y Controles Internos en BACEN (Banco Central do Brasil).
Fue miembro del Comité de Certificaciones del estándar tecnológico-financiero internacional XBRL
Posee una maestría en Redes de Computación, doctorado en Ciencia de Computación (Univ Pernambuco- Brasil) y Pos-doctorado en Sistemas de Información Financiera (Rutgers University – New Jersey USA).
Es autor de 3 libros y fue asesor de la Secretaría del Tesoro Nacional de Brasil en la implementación del sistema SICONFI. Dirige trabajos de investigación y de iniciación científica sobre temas de computación cuántica, y ha sido conferencista internacional invitado en múltiples eventos para exponer sobre ese tema.

Paulo Caetano da Silva <caetano.paulo@animaeducacao.com.br>

@ paulo-caetano-da-silva-a90675155

revisión y control - Enfoque Estratégico Bancario

Marcelo Mazzón – ABAPPRA

Marcelo es Lic. en Economía (UBA) y Lic. en Sistemas de las Organizaciones (UBA)
Se desempeña desde enero 2021 como **Director Ejecutivo de ABAPPRA** – Asociación de Bancos Públicos y Privados de la República Argentina.
Desde ese cargo ha impulsado la agenda de tecnologías innovadoras tales como Blockchain, Inteligencia Artificial y Computación Cuántica dentro del sector bancario de Argentina

ABAPPRA <info@abappra.org.ar>

@ marcelo-mazzon-989559282

7 referencias

libros y trabajos
publicaciones de organismos

7 referencias

libros y trabajos

Agarwal, D., & Ganguly, S. (2023). *Productizing quantum computing*. Springer

Anandan, E. (Ed.). (2022). *Frontiers in quantum computing: New research*. Nova Science Publishers.

Banafa, A. (2023). *Introduction to quantum computing*. River Publishers

Bernhardt, C. (2019). *Quantum computing for everyone*. The MIT Press.

Corbett Moran, C. (2019). *Mastering quantum computing with IBM QX: Explore the world of quantum computing using the Quantum Composer and Qiskit*. Packt Publishing.

Easttom, C., II. (2021). *Quantum computing fundamentals*. Addison-Wesley Professional.

Easttom, C. (2024). *Hardware for quantum computing*. Springer.

Gribbin, J. (2023). *Computing with quantum cats: The history, theory, and application of a revolutionary science*. Rowman & Littlefield.

Jacquier, A., Kondratyev, O., Lipton, A., & de Prado, M. L. (2022). *Quantum machine learning and optimisation in finance: On the road to quantum advantage*. Packt Publishing Ltd.

Kaku, M. (2023). *Quantum supremacy: How the quantum computer revolution will change everything*. Doubleday.

Kaye, P., Laflamme, R., & Mosca, M. (2007). *An introduction to quantum computing*. Oxford University Press.

Loredo, R. (2020). *Learn quantum computing with Python and IBM quantum experience*. Packt Publishing.

Mykhailova, M. (2025). *Quantum programming in depth with Q# and Qiskit*. Manning Publications.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press.

Orrell, D. (2020). *Quantum economics and finance: An applied mathematics introduction*. Panda Ohana Publishing.

Preskill, J. (2012). *Quantum computing and the entanglement frontier*. arXiv. https://arxiv.org/abs/1203.5813

Rieffel, E. G., & Polak, W. H. (2011). *Quantum computing: A gentle introduction*. The MIT Press.

Shor, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Silva, V. (2024). *Quantum computing by practice: Programming quantum computers in the cloud using Qiskit, Cirq, and Python*. Springer

Sutor, R. S. (2024). *Dancing with qubits: How quantum computing works and how it can change the world (2nd ed.)*. Packt Publishing.

Terán Pérez, D. M. (2024). *Introducción a la computación cuántica para ingenieros*. Marcombo.

Van Der Post, H. (2024). *Quantum finance: Harnessing Q# to revolutionize financial modeling*. Reactive Publishing.

Vos, J. (2022). *Quantum computing in action*. Manning Publications.

Wilde, M. M. (2013). Quantum information theory. Cambridge University Press

Yanofsky, N. S., & Mannucci, M. A. (2008). *Quantum computing for computer scientists*. Cambridge University Press.

Ying, M. (2016). *Foundations of quantum programming*. Morgan Kaufmann.

Zygelman, B. (2024). *A first introduction to quantum computing and information*. Springer

publicaciones de organismos

Bank for International Settlements (BIS)

BIS – Bank for International Settlements - Project Leap: quantum-proofing the financial system , June 2023
https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

BIS – Bank for International Settlements - Fully Scalable Settlement Engine (FuSSE) - A strategic framework for quantum-cryptography in FuSSE, April 2024
https://www.bis.org/publ/bisih_fusse.pdf

BIS – Bank for International Settlements - BIS Papers No 149 - Quantum computing and the financial system: opportunities and risks - Raphael Auer, Angela Dupont, Leonardo Gambacorta, Joon Suk Park, Koji Takahashi, Andras Valko (Monetary and Economic Department), October 2024
https://www.bis.org/publ/bppdf/bispap149.htm

BIS – Bank for International Settlements - BIS Papers No 158 - Quantum-readiness for the financial system: a roadmap - Raphael Auer, Donna Dodson, Angela Dupont, Maryam Haghighi, Nicolas Margaine, Danica Marsden, Sarah McCarthy Andras Valko (Monetary and Economic Department), July 2025
https://www.bis.org/publ/bppdf/bispap158.htm

Federal Reserve Board, Washington, D.C.

Federal Reserve Board, Washington, D.C. – "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks - Jillian Mascelli and Megan Rodden, September 2025
https://www.federalreserve.gov/econres/feds/harvest-now-decrypt-later-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm

National Institute of Standards and Technology (NIST)

U.S. Department of Commerce's National Institute of Standards and Technology (NIST) - Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, August 13, 2024
https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

U.S. Department of Commerce's National Institute of Standards and Technology (NIST) - FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 13, 2024
https://csrc.nist.gov/pubs/fips/203/final

U.S. Department of Commerce's National Institute of Standards and Technology (NIST) - FIPS 204 Module-Lattice-Based Digital Signature Standard, August 13, 2024
https://csrc.nist.gov/pubs/fips/204/final

U.S. Department of Commerce's National Institute of Standards and Technology (NIST) - FIPS 205 Stateless Hash-Based Digital Signature Standard, August 13, 2024
https://csrc.nist.gov/pubs/fips/205/final

U.S. Department of Commerce's National Institute of Standards and Technology (NIST) - NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, July 5, 2022
https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

World Economic Forum (WEF – Foro de Davos)

WEF – World Economic Forum - Quantum Security for the Financial Sector: Informing Global Regulatory Approaches, January 2024
https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/

WEF – World Economic Forum - Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders, July 2025
https://www.weforum.org/publications/quantum-technologies-key-strategies-and-opportunities-for-financial-services-leaders/

SEC – Securities and Exchange Commission USA

SEC – Securities and Exchange Commission USA Post-Quantum Financial Infrastructure Framework (PQFIF) A Roadmap for the Quantum-Safe Transition of Global Financial Infrastructure, September 2025
https://www.sec.gov/files/cft-written-input-daniel-bruno-corvelo-costa-090325.pdf

CISA – Cybersecurity & Infrastructure Security Agency
NSA – National Security Agency
NIST – National Institute of Standards and Technology

CISA, NSA y NIST – QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY, August 2023
https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography