**Revista Iberoamericana de la Educación**, Vol - 10 No. 2 , April - June 2026
e-ISSN: 2737-632x
Pgs 220-237

# Entorno Quantum-Safe: Impacto de la Computación Cuántica sobre la Información Históricamente Cifrada

Quantum-Safe Environment: Impact of Quantum Computing on Historically Encrypted Information

Ambiente Quantum-Safe: Impacto da Computação Quântica sobre a Informação Historicamente Cifrada

**Juan Rigoberto Castillo Serracín***
**Odessa Aranda***
**Francisco Farnum Castro***
**Javier Miguel Gómez Solís***

How to cite:
Castillo, J., Aranda, O., Farnum, F., Gómez, J. (2026) Entorno Quantum-Safe: Impacto de la Computación Cuántica sobre la Información Históricamente Cifrada. *Revista Iberoamericana De educación,* 10 (2).

http://www.revista-iberoamericana.org/index.php/es

* Universidad de Panamá, Panamá.
juan.castillos@up.ac.pa
https://orcid.org/0009-0006-5821-7028
** Universidad de Panamá, Panamá.
odessa.aranda@up.ac.pa
https://orcid.org/0000-0002-3698-1141
*** Universidad de Panamá, Panamá.
francisco.farnum@up.ac.pa
https://orcid.org/0000-0002-5879-2296

**** Universidad de Panamá, Panamá.
javier.gomez@up.ac.pa.
https://orcid.org/0009-0000-4583-5157

## Abstract

Cyberspace has become a domain of power and conflict that challenges traditional geopolitics. This study analyzes how digital dependence redefines sovereignty, borders, and power, aiming to develop a conceptual framework for understanding new conflict and cooperation paradigms in the 21st century. Using a qualitative methodology and documentary analysis of state doctrines, international reports, and academic literature, the results confirm the central hypothesis: cyberspace has fractured traditional paradigms. States are not adapting international law; instead, they prioritize building digital sovereignties through infrastructure control and data localization. Likewise, the normalization of gray-zone operations (cyber espionage, disinformation, attacks on technological infrastructure) is evident as legitimate foreign policy tools within a normative vacuum that fosters competition over cooperation. Finally, the concept of hybrid sovereignty is proposed as the new axis of state authority in the 21st century.

**Keywords:** Protection; Processing; Data; Cryptography; Post-quantum; Computing.

## Resumen

El ciberespacio se ha consolidado como un dominio de poder y conflicto que desafía la geopolítica tradicional. Este estudio analiza cómo la dependencia digital redefine soberanía, frontera y poder, con

el objetivo de desarrollar un marco conceptual para comprender los nuevos paradigmas de conflicto y cooperación en el siglo XXI. Mediante una metodología cualitativa y análisis documental de doctrinas estatales, informes internacionales y literatura académica, los resultados confirman la hipótesis central: el ciberespacio ha fracturado los paradigmas tradicionales. Los Estados no están adaptando el derecho internacional, sino que priorizan la construcción de soberanías digitales mediante el control de infraestructuras y la localización de datos. Asimismo, se evidencia la normalización de operaciones en la zona gris (ciberespionaje, desinformación, ataques a infraestructuras tecnológicas) como herramientas legítimas de política exterior, en un entorno de vacío normativo que fomenta la competencia por encima de la cooperación. Finalmente, se propone el concepto de soberanía híbrida como nuevo eje de autoridad estatal en el siglo XXI.

**Palabras clave:** Protección; Procesamiento; Datos; Criptografía; Post-cuántica; Computación

## Resumo

O ciberespaço consolidou-se como um domínio de poder e conflito que desafia a geopolítica tradicional. Este estudo analisa como a dependência digital redefine soberania, fronteira e poder, com o objetivo de desenvolver um quadro conceitual para compreender os novos paradigmas de conflito e cooperação no século XXI. Por meio de uma metodologia qualitativa e análise documental de doutrinas estatais, relatórios internacionais e literatura acadêmica, os resultados confirmam a hipótese central: o ciberespaço fraturou os paradigmas tradicionais. Os Estados não estão adaptando o direito internacional, mas sim priorizando a construção de soberanias digitais mediante o controle de infraestruturas e a localização de dados. Da mesma forma, evidencia-se a normalização de operações na zona cinzenta (ciberespionagem, desinformação, ataques a infraestruturas tecnológicas) como ferramentas legítimas de política externa, em um ambiente de vazio normativo que fomenta a competição acima da cooperação. Por fim, propõe-se o conceito de soberania híbrida como novo eixo de autoridade estatal no século XXI.

**Palavras-chave:** Proteção; Processamento; Dados; Criptografia; Pós-quântica; Computação.

## INTRODUCCIÓN

En la actualidad, el paradigma de la ciberseguridad global se fundamenta en la complejidad computacional de la Criptografía de Clave Pública (PKC), operando bajo estándares universales como RSA y la Criptografía de Curva Elíptica (ECC) (National Institute of Standards and Technology [NIST], 2013). La premisa de estos sistemas reside en la intractabilidad computacional que presentan problemas matemáticos como la factorización de grandes enteros. Esta complejidad asegura que, frente a los sistemas clásicos, los recursos necesarios para vulnerar una clave crezcan de manera exponencial (Rivest, Shamir & Adleman, 1978).

No obstante, en el contexto tecnológico del siglo XXI, este paradigma enfrenta una amenaza existencial: el advenimiento de la Computación Cuántica Criptográficamente Relevante (CRQC). La demostración teórica del Algoritmo de Shor (1994) establece que una máquina cuántica con suficientes qubits estables resuelve estos problemas en tiempo polinomial (clase BQP). Hitos recientes, como la demostración de teletransportación cuántica sobre infraestructuras de internet comercial, confirman que la coexistencia de redes clásicas y cuánticas es inminente, lo que reduce drásticamente el horizonte temporal de la seguridad clásica (Infobae, 2025; Bernstein, 2009).

Esta disrupción tecnológica exacerba una vulnerabilidad asimétrica que constituye una amenaza presente: el ataque “Cosechar Ahora, Descifrar Después” (Harvest Now, Decrypt Later - HNDL) (Gartner, 2024). Las entidades hostiles interceptan y almacenan flujos de datos cifrados en la actualidad con el objetivo de descifrarlos una vez que la tecnología cuántica alcance su madurez. Esta estrategia desafía cualquier garantía de confidencialidad a largo plazo y convierte a la Información Históricamente Cifrada o Datos en Reposo (DAR) en el vector de ataque más crítico (Parlamento Europeo, 2024).

En cuanto a los antecedentes investigativos, estudios previos como los de Aumasson (2023) y las evaluaciones de arquitectura de Intel Corporation (2022) abordan profusamente la robustez matemática de los estándares postcuánticos y su impacto sobre el procesador (CPU). Sin embargo, limitan sus métricas a la latencia computacional. El presente trabajo aporta a esta línea de investigación al desplazar el análisis desde el cálculo algorítmico hacia el impacto logístico sobre la infraestructura física. El problema central radica en la falsa premisa corporativa de que la transición constituye una simple actualización de software, ignorando que la

expansión volumétrica del cifrado postcuántico saturará las arquitecturas heredadas (legacy).

A partir de esta problemática se sostiene la hipótesis de que la migración hacia un entorno Quantum-Safe genera una inversión estructural del cuello de botella operativo, trasladando la limitación técnica desde la capacidad de procesamiento (CPU) hacia el ancho de banda de la red y el almacenamiento (I/O Bound).

Este problema no es solo de ingenieros. Afecta a cualquier persona u organización que guarde información sensible a largo plazo: hospitales públicos, juzgados, universidades, cooperativas, pequeñas empresas. Si la solución requiere hardware caro y rápidas conexiones, quienes no puedan costearlo quedarán excluidos de la seguridad digital del futuro. La transición cuántica podría profundizar la brecha entre grandes corporaciones y el resto de la sociedad.

En consecuencia, se prevé que las infraestructuras que no adopten proactivamente tecnologías de alta velocidad (como arreglos NVMe) enfrentarán una brecha de viabilidad operativa inasumible frente a la inminencia cuántica. Por todo ello, el objetivo general de esta investigación es modelar y cuantificar la carga computacional, el overhead de almacenamiento y el tiempo teórico requerido para el recifrado masivo de datos en reposo utilizando el algoritmo ML-KEM, operando bajo variables independientes como el volumen de datos y la granularidad de los archivos, frente a variables dependientes como el crecimiento físico del almacenamiento y la latencia temporal.

## MATERIALES Y MÉTODOS

El presente estudio se desarrolló bajo un enfoque cuantitativo de tipo descriptivo y predictivo. Para dar respuesta a la problemática planteada, se estructuró sobre un diseño no experimental y transversal, fundamentado específicamente en la simulación prospectiva y el modelado matemático. La adopción de esta aproximación metodológica se fundamenta en la viabilidad técnica y en la gestión de riesgos, dado que el objeto de estudio aborda el impacto de una tecnología en actual estandarización (ML-KEM). La ejecución empírica de pruebas de recifrado masivo sobre infraestructuras de producción en vivo fue descartada por resultar inasumible, ante el inminente riesgo de disrupción operativa y parálisis del servicio.

Dada la naturaleza predictiva del modelado, la población de estudio no estuvo constituida por sujetos humanos, sino por el universo

teórico de repositorios de Información Históricamente Cifrada (DAR). Como técnica de muestreo intencional para la simulación, se establecieron dos dimensiones representativas o escenarios de análisis: un Escenario Base de 10 TB (típico de una pequeña y mediana empresa o departamento universitario) y un Escenario de Estrés de 1 PB (representativo de infraestructuras críticas, Data Lakes o banca transaccional).

Los criterios de inclusión para la parametrización del modelo se limitaron estrictamente a documentación técnica primaria y normativas de organismos rectores vigentes, incluyendo los estándares FIPS 203 (ML-KEM) y FIPS 186-4 del NIST, así como directrices del ETSI.

Para la recolección de datos se aplicó la técnica de revisión documental técnica y normativa, orientada a la extracción de métricas de rendimiento y parametrización de hardware (benchmarking). El instrumento central consistió en una matriz paramétrica diseñada para tabular las tasas de expansión criptográfica y las velocidades teóricas máximas de transferencia (I/O) provistas en los estándares oficiales y reportes técnicos de la industria.

Bajo este modelo, se definieron como variables independientes el volumen de datos históricos, la granularidad de los archivos y el ancho de banda sostenido de la infraestructura. Las variables dependientes proyectadas fueron el crecimiento absoluto del almacenamiento físico y el tiempo de latencia de migración.

El procedimiento analítico se estructuró parametrizando en primer lugar el factor de expansión del cifrado $(\delta_{exp})$. Posteriormente, para proyectar la latencia temporal, se formuló y aplicó la ecuación de rendimiento matemático $(T_{mig})$ derivada del marco teórico, expresada como:

$$T_{mig} = \frac{V_{DAR} \times (1+\delta_{exp})}{\min(BW_{disk}, BW_{net})}$$

Donde:

***T mig*:** Tiempo total estimado para la migración.

***V DAR*:** Volumen original de datos a recifrar (ej.1 Terabyte)

***& exp: Coeficiente*** de expansión de cifrado (derivado de la Tabla de Referencia NIST)

***BW disk*:** Ancho de banda secuencial de escritura/lectura en disco (MB/s)

***BM net*:** Ancho de banda disponible de la red para la transferencia (MB/s)

Esta métrica, que confirma la limitación de entrada/salida (I/O Bound), se ejecutó iterativamente sobre cuatro topologías de

infraestructura física (WAN, HDD Legacy, SSD SATA y Arreglos NVMe).

Finalmente, desde el punto de vista de las consideraciones éticas, la investigación priorizó el principio de no maleficencia al optar por un entorno simulado, garantizando que ninguna infraestructura crítica real fuera sometida a estrés que pudiera comprometer servicios. En cuanto a las limitaciones, se advierte que el modelo matemático asume tasas de transferencia sostenidas en operación continua 24/7; en implementaciones físicas reales, variables como latencias intermitentes de red o fragmentación severa del disco podrían incrementar los tiempos base arrojados por este modelo.

## RESULTADOS

Para dimensionar la criticidad temporal de esta amenaza, resulta imperativo visualizar la interacción entre la vida útil de la información y el tiempo de migración tecnológica. Tal como ilustra la representación gráfica del Teorema de Mosca (Figura 1), existe un periodo crítico o Zona de Riesgo en el cual la confidencialidad de los datos se ve matemáticamente comprometida antes de que la organización logre completar su transición hacia algoritmos seguros. LA representación gráfica del Teorema de Mosca, expresa que el área sombreada, delimitada por la línea vertical roja, señala el periodo en el que la información cifrada históricamente se vuelve susceptible a ataques de descifrado retroactivo, debido a que la vida útil del secreto (Y) supera la llegada de la computación cuántica (Z).

**Figura 1.**

*El Teorema de Mosca (HNDL)*


**Fuente.** Elaboración propia, adaptado de Mosca (2018).

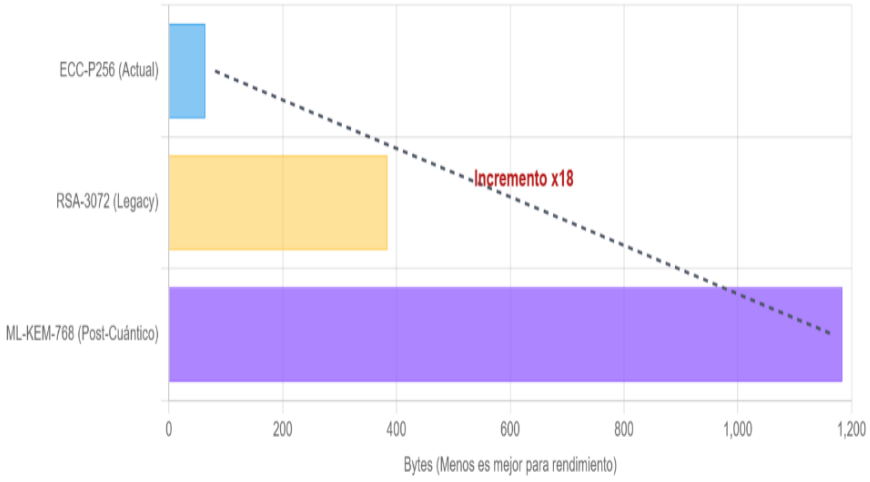
Para contrarrestar esta vulnerabilidad, el NIST ha estandarizado recientemente el algoritmo ML-KEM (basado en retículos matemáticos o *Module-Lattices*) como el mecanismo definitivo de encapsulamiento de claves postcuánticas (NIST, 2024). De acuerdo con las guías de resiliencia cuántica, la protección de los Datos en Reposo exige ejecutar un proceso de Recifrado Masivo (*Bulk Re-encryption*) hacia este nuevo estándar (European Telecommunications Standards Institute [ETSI], 2022).

Sin embargo, para comprender la magnitud del desafío logístico de esta transición, es necesario analizar el fenómeno de expansión del cifrado (*Ciphertext Expansion*). La robustez de los esquemas basados en retículos requiere estructuras de datos significativamente más grandes que las curvas elípticas. Tal como evidencia la Figura 2, existe una desproporción extrema en el tamaño de la clave pública entre el estándar actual (ECC) y el postcuántico, ilustrando el origen físico del *overhead* que amenaza con saturar los medios de almacenamiento.

La figura que se muestra a continuación expresa la comparación del tamaño de claves públicas entre estándares criptográficos actuales y postcuánticos. Se observa un incremento notable del volumen de datos (aprox. 18×) al pasar de curvas elípticas (ECC) a esquemas basados en retículos (ML-KEM), con impacto directo en la latencia de red y los requerimientos de almacenamiento.

**Figura 2.**

*La Expansión del Cifrado*




**Fuente.** Elaboración propia con base en datos de NIST FIPS 203 (2024).

La expansión de datos descrita provoca, a su vez, una ruptura en el paradigma de rendimiento tradicional. Mientras que en la criptografía clásica el factor limitante era la velocidad de cálculo del procesador algorítmico, el modelo postcuántico invierte esta relación.

La Figura 3 esquematiza este desplazamiento del cuello de botella operativo (*Throughput Shift*), donde la saturación técnica se traslada desde la Unidad Central de Procesamiento (CPU) hacia el subsistema de Entrada/Salida (I/O), convirtiendo al ancho de banda de almacenamiento y red en el componente crítico.

La inversión del cuello de botella operativo. En el enfoque postcuántico (derecha), el mayor volumen de datos satura la capacidad de escritura/entrada-salida (I/O), mientras que en el enfoque clásico (izquierda) la limitación principal recae en el procesamiento matemático.

**Figura 3**

*El Desplazamiento del Cuello de la Botella*


**Fuente.** Elaboración propia.

La aplicación del modelo matemático de simulación prospectiva arrojó proyecciones determinantes sobre el impacto logístico del algoritmo ML-KEM en infraestructuras heredadas.

A continuación, se presentan los hallazgos estructurados en torno a las dos variables dependientes del estudio: el crecimiento del volumen físico (obesidad de datos) y la latencia temporal de migración, culminando con la discusión teórica de sus implicaciones

operativas.

Al analizar la expansión volumétrica y la obesidad de datos postcuántica, el modelado de la variable de expansión del cifrado $(\delta_{exp})$ reveló un comportamiento asintótico altamente penalizador para ecosistemas de datos fragmentados. Al simular el escenario base de 10 Terabytes (TB), se evidenció que la proporción de la sobrecarga criptográfica es inversamente proporcional a la granularidad del archivo.

La cuantificación exacta de este fenómeno, que ilustra cómo los entornos transaccionales absorben el mayor margen de expansión (+200%), donde el diferencial de expansión demuestra que los micro-registros (1 KB) que sufren un impacto crítico en comparación con los archivos multimedia. Estos elementos se detallan a continuación en la Tabla 1.

**Tabla 1**

*Proyección de Expansión de Almacenamiento (Base: 10 TB)*

| **Tipo de Datos (Entorno)** | **Tamaño Promedio Archivo** | **Cantidad de Registros** | **Volumen Final (Post-Quantum)** | **% de Expansión (Overhead)** |
|---|---|---|---|---|
| Base de Datos Bancaria | 1 KB | 10,000 Millones | 30.0 TB | +200% |
| Registros Médicos / Logs | 10 KB | 1,000 Millones | 12.0 TB | +20% |
| Documentos de Oficina | 1 MB | 10 Millones | 10.02 TB | +.02% |
| Archivos Multimedia | 10 MB | 1 Millón | 10.002 TB | Despreciable |

**Fuente.** Elaboración propia.

Como se observa en la Tabla 1, en entornos de Big Data transaccional,caracterizados por micro-registros de 1 KB, la adición de la firma postcuántica basada en retículos triplica los requerimientos físicos, generando un crecimiento absoluto del +200% sobre la cuota original.

Para validar la escalabilidad de este fenómeno, el modelo se extrapoló al escenario de estrés de 1 Petabyte (PB), El diferencial de hardware evidencia la criticidad extrema en entornos bancarios

(archivos de 1 KB), requiriendo 2,000 TB adicionales, mientras que en entornos documentales el impacto es despreciable. cuyos resultados se detallan en la Tabla 2.

**Tabla 2**

*Impacto de la Expansión en Grandes Volúmenes (Base: 1 PB)*

| **Tipo de Datos (Entorno)** | **Tamaño Promedio Archivo** | **Volumen Base** | **Volumen Final (Post-Quantum)** | **Diferencial (Hardware Requerido)** |
|---|---|---|---|---|
| Banca / Transaccional | 1 KB | 1 PB | 3.0 PB | + 2,000 TB (Crítico) |
| Registros / Logs | 10 KB | 1 PB | 1.2 PB | + 200 TB |
| Docs / Multimedia | > 1 MB | 1 PB | ~1.0 PB | Despreciable |

**Fuente.** Elaboración propia.

La proyección sobre el escenario de estrés demuestra que el diferencial de hardware requerido deja de ser un problema lógico para convertirse en una limitante física.

Mientras que en ecosistemas documentales (archivos > 1 MB) el impacto es estadísticamente despreciable, la protección de bases de datos bancarias masivas exigiría la adquisición de múltiples Petabytes adicionales de almacenamiento de alta redundancia, transformando un proceso de aseguramiento de software en un proyecto crítico de gasto de capital (CAPEX).

Al analizar la latencia de Migración y la Brecha de Viabilidad Operativa en la segunda fase de la simulación se aplicó la ecuación de rendimiento temporal $(T_{mig})$ para evaluar el tiempo de inactividad operativo requerido durante el recifrado masivo a través de cuatro topologías de infraestructura.

Para el escenario de escala media (10 TB), la Tabla 3 y la Figura 4 ilustran que la adopción de arreglos *All-Flash* de nivel empresarial (NVMe) logra mitigar la expansión geométrica del algoritmo ML-

KEM.

Esta tecnología comprime el tiempo de recifrado a una ventana de mantenimiento nocturna manejable de aproximadamente 2.5 horas, neutralizando el riesgo de disrupción del servicio frente a los discos rígidos tradicionales (HDD). Se asume un overhead de expansión constante del 15% y operación continua (24/7).

**Tabla 3**

Tiempo Estimado para Recifrar 10 TB

| **Infraestructura** | **Velocidad (Sostenida)** | **Tiempo Estimado** | **Viabilidad Operativa** |
|---|---|---|---|
| WAN / Nube | 50 MB/s | 2.7 Días | Crítica (Ventana excesiva) |
| HDD Legacy | 100 MB/s | 1.3 Días | Riesgo Medio |
| SSD SATA | 500 MB/s | 0.3 Días (7h) | Manejable |
| NVMe Enterprise | 2,500 MB/s | 0.05 Días (~1.3 h) | Óptima (Ventana nocturna) |

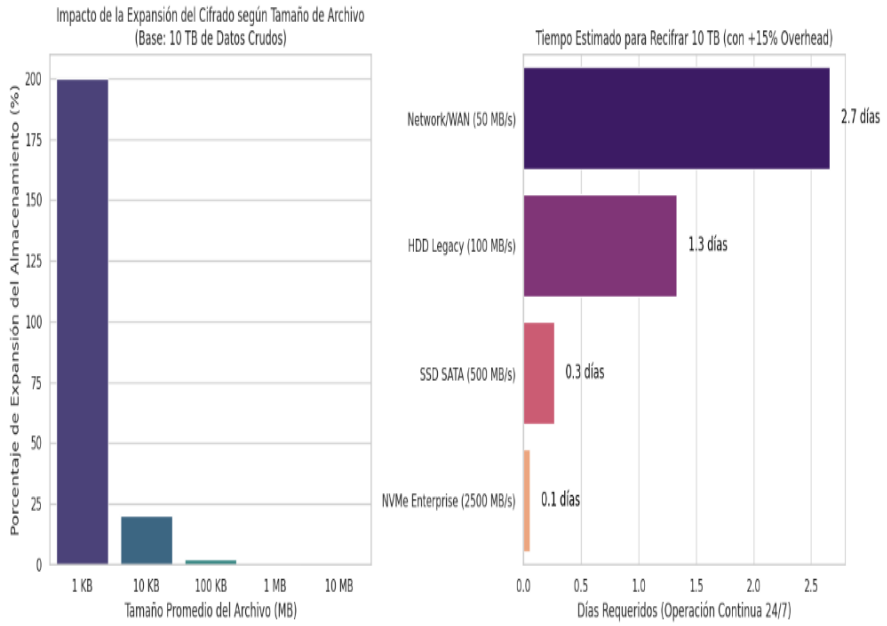
**Fuente.** Elaboración propia.

En la figura 4 se muestra un panel de análisis dual (Base 10 TB). A la izquierda se observa el impacto exponencial en la cuota de almacenamiento para registros de menor tamaño.

A la derecha se contrasta la mitigación del tiempo de migración al utilizar tecnologías de estado sólido (NVMe) frente a infraestructuras tradicionales.

**Figura 4**

*Panel de Análisis para Escenario Base (10 TB)*




**Fuente.** Elaboración propia.

No obstante, la paradoja de la escalabilidad se hace crítica al extrapolar estas métricas hacia un entorno macroscópico. Cuando la variable de expansión criptográfica impacta un repositorio de 1 Petabyte (1,000 TB), volumen representativo de infraestructuras críticas, banca o *Data Lakes* corporativos, el *overhead* deja de ser una simple penalización lógica para convertirse en un estrangulamiento físico absoluto.

El panel de análisis de la Figura 5 y los datos proyectados en la Tabla 4 evidencian que la infraestructura tradicional colapsa bajo el peso masivo de los datos postcuánticos. Intentar ejecutar un proceso de recifrado masivo a través de una red de área amplia (WAN) requeriría más de 260 días ininterrumpidos de transferencia.

Este lapso resulta matemáticamente inviable, logísticamente inasumible y expone a la organización a un riesgo extremo de corrupción de datos por fallos de sesión, confirmando así una severa brecha de viabilidad operativa que paralizaría la continuidad del negocio. En la misma se proyecta el tiempo de inactividad operativa considerando un volumen base macroscópico y un 15% de expansión criptográfica constante. Se evidencia el colapso operativo de las infraestructuras heredadas y redes WAN.

**Tabla 4**

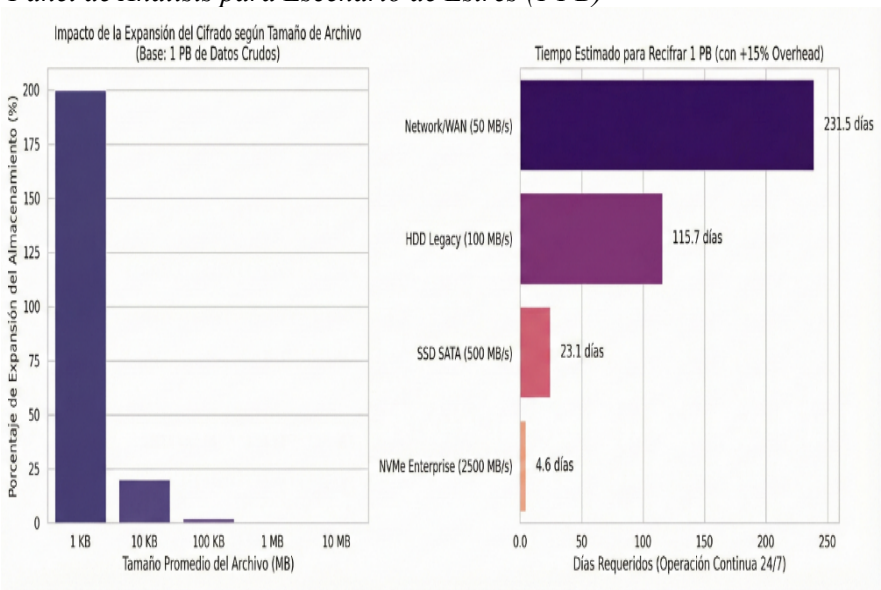
*Tiempo Estimado para Recifrar 1 PB (1,000 TB)*

| Infraestructura de Almacenamiento | Velocidad (Sostenida) | Tiempo Estimado de Migración | Viabilidad Operativa |
|---|---|---|---|
| WAN / Nube | 50 MB/s | 266 días | Inviable (Casi un año) |
| HDD Legacy | 100 MB/s | 133 días | Inviable (Riesgo de falla) |
| SSD SATA | 500 MB/s | 26.6 días | Crítica (Paralización mensual) |
| NVMe Enterprise | 2,500 MB/s | 5.3 días | Desafiante (Requiere segmentación) |

**Fuente.** Elaboración propia.

**Figura 5**

*Panel de Análisis para Escenario de Estrés (1 PB)*




**Fuente.** Elaboración propia.

El panel de análisis dual bajo escenario de estrés (Base 1 PB) en la figura 5, evidencia la brecha de viabilidad operativa, donde el recifrado de micro-registros transaccionales (izq.) detona una expansión crítica del almacenamiento, forzando tiempos de latencia (der.) que resultan inasumibles para la continuidad del negocio en redes WAN y discos heredados.

## DISCUSIÓN

De manera crítica, el modelo demuestra que incluso utilizando la tecnología de almacenamiento NVMe más avanzada, el proceso a macroescala exige más de cinco días continuos de latencia. Este lapso supera cualquier estándar de Acuerdo de Nivel de Servicio (SLA) para infraestructuras críticas, confirmando la existencia de una severa brecha de viabilidad operativa.

Los hallazgos expuestos permiten contrastar y expandir la literatura criptográfica actual. Mientras que estudios previos (Aumasson, 2023; Intel, 2022) se han enfocado en validar la eficiencia matemática de ML-KEM, demostrando su bajo impacto sobre la Unidad Central de Procesamiento (CPU), esta investigación fundamenta empíricamente una inversión estructural del cuello de botella.

La novedad científica de este trabajo radica en establecer que la seguridad postcuántica transforma el recifrado masivo de un proceso limitado por el cálculo algorítmico (Compute Bound) a un proceso estrangulado por la capacidad de lectura, escritura y transmisión de la infraestructura física (I/O Bound). A partir de esta premisa, emergen tres consideraciones que desafían los paradigmas corporativos vigentes:

-La Falacia de la Nube Pública para la Transición Cuántica: La tendencia global de centralizar la seguridad perimetral en la nube resulta inoperante para el recifrado retroactivo masivo de Datos en Reposo (DAR). Las latencias de red evidenciadas en las simulaciones WAN, exacerbadas por la expansión volumétrica de las firmas postcuánticas, exponen a las organizaciones a riesgos inasumibles de paralización y corrupción de datos por fallos de transferencia prolongados (ETSI, 2022).

Esta limitación física del ancho de banda sugiere una prospectiva tecnológica orientada hacia el renacimiento del procesamiento *On-Premise* de ultra alta velocidad y la adopción de arquitecturas de *Edge Computing*, las cuales permiten descentralizar la carga

criptográfica y mitigar la latencia al procesar la información clasificada directamente en el borde de la red (Amiriara et al., 2025).

-La Inviabilidad de la Estrategia Big Bang y el Imperativo Híbrido: Los tiempos de latencia proyectados en el escenario de estrés demuestran empíricamente que las grandes organizaciones no podrán ejecutar transiciones criptográficas totales en una sola ventana de mantenimiento de fin de semana. Intentar una migración abrupta expone a la infraestructura a un colapso operativo inaceptable.

Esto además, obligará a los arquitectos de sistemas a abandonar los enfoques de despliegue instantáneo y a diseñar modelos de recifrado segmentado en segundo plano (*Background Re-encryption*). En consecuencia, las infraestructuras deberán adoptar el principio de agilidad criptográfica y operar obligatoriamente bajo esquemas híbridos, entrelazando algoritmos clásicos y postcuánticos, durante periodos de transición prolongados, garantizando así la continuidad del negocio y la disponibilidad de los repositorios masivos (Agencia de Seguridad de Infraestructura y Ciberseguridad [CISA] et al., 2023; World Economic Forum, 2024).

-El Imperativo de la Auditoría de Vida Útil y la Minimización de Datos: Dado el alto costo logístico y el incremento radical en el gasto de capital (CAPEX) provocados por la obesidad de datos, se hace indispensable la implementación de políticas de depuración estrictas antes de iniciar cualquier migración.

Carece de sentido técnico y financiero someter información histórica cuya vida útil ha expirado a la pesada carga volumétrica de los algoritmos postcuánticos. Por ello, los marcos regulatorios establecen que la fase cero de la transición *Quantum-Safe* debe centrarse en el descubrimiento, la clasificación y la aplicación rigurosa de principios de minimización de datos; expurgar la información obsoleta no solo reduce la superficie de exposición ante ataques HNDL, sino que es la única estrategia de gobernanza viable para contener la saturación del almacenamiento físico que exige el estándar ML-KEM (Agencia de la Unión Europea para la Ciberseguridad [ENISA], 2022).

El modelo predictivo demuestra de forma consistente que la protección frente a la táctica ofensiva HNDL trasciende la dimensión lógica. La transición hacia un ecosistema Quantum-Safe se erige como un desafío fundamental de reingeniería de hardware, forzando a las organizaciones a rediseñar sus esquemas de bases de datos y a

modernizar su capa física antes de implementar el estándar ML-KEM.

## CONCLUSIONES

La inminencia de la Computación Cuántica Criptográficamente Relevante (CRQC) y el ataque *Harvest Now, Decrypt Later* (HNDL) han convertido una amenaza teórica en un riesgo sistémico tangible. Aunque el estándar ML-KEM del NIST ofrece una respuesta criptográfica definitiva, la industria ha subestimado gravemente la externalidad logística de esta solución: migrar hacia un entorno *quantum-safe* no es una simple actualización de software, sino una crisis inminente de reingeniería de infraestructura física.

El verdadero desafío no es la complejidad matemática, sino la "obesidad de datos" que genera ML-KEM. Con una expansión demostrada superior al +200% en almacenamiento para ecosistemas transaccionales, las arquitecturas heredadas resultan incompatibles. Esta sobrecarga invierte el cuello de botella operativo: el estrangulamiento se desplaza desde la CPU hacia el ancho de banda de red y la escritura en disco (I/O Bound). Como consecuencia, asegurar la información históricamente cifrada deja de ser un asunto rutinario de ciberseguridad para convertirse en un proyecto crítico de gasto de capital (CAPEX) orientado al almacenamiento masivo.

Las estrategias actuales de mitigación son inviables: recifrar un Petabyte por WAN tomaría más de 260 días, invalidando la nube pública como solución única. Se impone un recifrado nocturno por microlotes con NVMe on-premise, abandonar el cifrado transparente (TDE) por cifrado por campos específicos, y destruir datos obsoletos. Queda pendiente investigar el impacto energético y desarrollar protocolos de compresión para edge computing: la resiliencia futura dependerá tanto de algoritmos cuánticamente seguros como de nuestra capacidad física y sostenible para almacenarlos.

## REFERENCIAS

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (2022). *Post-Quantum Cryptography: Integration study.* Publications Office of the European Union. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Agencia de Seguridad de Infraestructura y Ciberseguridad [CISA], Agencia de Seguridad Nacional [NSA], & Instituto Nacional de

Estándares y Tecnología [NIST]. (2023). *Quantum-readiness: Migration to post-quantum cryptography*. Departamento de Seguridad Nacional de EE. UU. https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness_Migration-to-Post-Quantum-Cryptography_Fact-Sheet_508c.pdf

Amiriara, H., Mirmohseni, M., & Tafazolli, R. (2025). *PLS-assisted offloading for edge computing-enabled post-quantum security in resource-constrained devices*. arXiv. https://arxiv.org/abs/2504.09437

Aumasson, J.-P. (2023). *Post-Quantum Cryptography: Standards and Progress* [Presentación]. STHACK 2023. https://www.aumasson.jp/data/talks/qcpqc-sthack23.pdf

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. En D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 1-14). Springer. https://doi.org/10.1007/978-3-540-88702-7_1

European Telecommunications Standards Institute [ETSI]. (2022). *Quantum-safe cryptography (QSC)*. ETSI Technologies. https://www.etsi.org/technologies/quantum-safe-cryptography

Gartner. (2024). *Top strategic technology trends for 2025. Gartner Research. https://www.gartner.com/en/articles/top-technology-trends-2025*

Infobae. (2025, 23 de enero). *Revolución en las comunicaciones, la teletransportación cuántica se aproxima al mundo real*. Infobae. https://www.infobae.com/salud/ciencia/2025/01/23/revolucion-en-las-comunicaciones-la-teletransportacion-cuantica-se-aproxima-al-mundo-real/

Intel Corporation. (2022). *Accelerate Post-Quantum Cryptography with Intel Crypto Technologies*. Intel Industry Solution Builders. https://builders.intel.com/docs/networkbuilders/accelerate-post-quantum-cryptography-with-intel-crypto-technologies-1759835295.pdf

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

National Institute of Standards and Technology [NIST]. (2013). *Digital signature standard (DSS)* (FIPS PUB 186-4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-4

National Institute of Standards and Technology [NIST]. (2024**).** *Module-lattice-based key-encapsulation mechanism standard* (FIPS PUB 203). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

Parlamento Europeo. (2024). *Cryptographic security: A question for Europe's digital sovereignty* (Briefing EPRS_BRI(2024)766237). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126. https://doi.org/10.1145/359340.359342

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

World Economic Forum. (2024). *Quantum security for the financial sector: Informing global regulatory approaches*. https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf