Universidad Siglo 21

Trabajo final de grado. Trabajo de investigación en tecnologías informáticas.

Carrera: Licenciatura en informática

Análisis Comparativo de RSA-2048 y CRYSTALS-Kyber: Eficiencia, Robustez Criptográfica y Desafíos para la Adopción Post-Cuántica.

Autor: Bazán Pedro Uriel

Legajo: VINF011655

Tutor: Virgolini, Pablo Alejandro

Fecha: 29 de junio del 2025

Índice

Índice tablas

Resumen

Esta investigación evaluó la viabilidad técnica, operativa y de seguridad de reemplazar el algoritmo criptográfico RSA-2048 por el estándar post-cuántico CRYSTALS-Kyber, ante la amenaza que representa la computación cuántica. La metodología combinó un análisis experimental de rendimiento, una revisión documental de la robustez criptográfica y entrevistas a expertos argentinos para identificar los desafíos de adopción. Las pruebas de rendimiento indicaron que CRYSTALS-Kyber (ML-KEM-512) es significativamente más rápido en la generación de claves y decapsulamiento, mientras que RSA-2048 lo es para el cifrado de mensajes pequeños; se constató también el mayor tamaño de los artefactos criptográficos de Kyber. En cuanto a la seguridad, se confirmó la vulnerabilidad teórica de RSA frente al algoritmo de Shor y la robustez de Kyber; no obstante, se destacaron riesgos asociados a su implementación práctica, como los ataques de canal lateral. Por último, se identificaron importantes desafíos organizacionales y técnicos, como la necesidad de un inventario criptográfico, los costos de migración y la escasez de personal capacitado. Se concluye que, si bien CRYSTALS-Kyber es un sucesor técnicamente viable, su adopción representa un desafío complejo que exige una planificación estratégica integral y una considerable inversión en recursos para las organizaciones en Argentina.

Palabras clave: Criptografía Post-Cuántica, CRYSTALS-Kyber, RSA, Seguridad de la Información, Computación Cuántica, Migración Criptográfica.

Abstract

This research evaluated the technical, operational, and security feasibility of replacing the RSA-2048 cryptographic algorithm with the post-quantum standard CRYSTALS-Kyber, given the threat posed by quantum computing. The methodology combined an experimental performance analysis, a documentary review of cryptographic robustness, and interviews with Argentine experts to identify adoption challenges. Performance tests indicated that CRYSTALS-Kyber (ML-KEM-512) is significantly faster in key generation and decapsulation, whereas RSA-2048 is faster for encrypting small messages; the larger size of Kyber's cryptographic artifacts was also confirmed. Regarding security, RSA's theoretical vulnerability to Shor's algorithm and Kyber's robustness were confirmed; however, risks associated with its practical implementation, such as side-channel attacks, were highlighted. Finally, significant organizational and technical challenges were identified, such as the need for a cryptographic inventory, migration costs, and a shortage of trained personnel. It is concluded that while CRYSTALS-Kyber is a technically viable successor, its adoption represents a complex challenge that demands comprehensive strategic planning and considerable resource investment for organizations in Argentina.

Keywords: Post-Quantum Cryptography, CRYSTALS-Kyber, RSA, Information Security, Quantum Computing, Cryptographic Migration.

Introducción

La criptografía puede definirse como el arte y la ciencia de proteger la información, ocultando su contenido para que solo las personas autorizadas puedan acceder a él. Su historia se remonta a las civilizaciones antiguas, con métodos como el cifrado de sustitución empleado por griegos y romanos. Este campo se ha caracterizado desde entonces por un ciclo constante de desarrollo: la creación de un nuevo método de cifrado es inevitablemente seguida por el esfuerzo de romperlo, lo que a su vez impulsa la invención de técnicas aún más seguras (Singh, 1999).

La seguridad de las comunicaciones digitales modernas se ha fundamentado durante décadas en la criptografía de clave pública, cuyo pilar principal ha sido el algoritmo RSA (Rivest, Shamir, & Adleman, 1978). Esto no fue una mejora incremental, sino una verdadera revolución. Antes de su existencia, la criptografía se basaba exclusivamente en métodos simétricos, que requerían que ambas partes compartieran una clave secreta de antemano a través de un canal seguro. Esta limitación hacía impracticable la comunicación segura a gran escala en redes abiertas como internet.

El algoritmo RSA resolvió este problema fundamental al introducir un par de claves: una pública para cifrar y una privada para descifrar. Esta innovación habilitó la 'economía de la confianza' digital, sentando las bases para el comercio electrónico, las transacciones bancarias online, las redes privadas virtuales (VPN) y, fundamentalmente, el protocolo TLS que asegura gran parte de la web (el 'candado' en el navegador) (Rivest, Shamir, & Adleman, 1978).

La robustez que permitió esta revolución reside en la dificultad computacional de un problema matemático específico: la factorización de números enteros muy grandes.

Para las computadoras clásicas, que procesan información mediante bits con un valor definido de 0 o 1, esta tarea es intratable para claves de uso común, como las de 2048 bits (Pomerance, 1996).

Para poner esta dificultad en perspectiva, el algoritmo clásico más avanzado para este fin es el General Number Field Sieve (GNFS), un método altamente especializado que representa el 'estándar de oro' en la factorización clásica. A pesar de su eficiencia relativa, su tiempo de ejecución sigue siendo subexponencial, lo que significa que, aunque es más rápido que métodos más simples, aún requeriría miles de años para romper una clave RSA-2048, garantizando así la seguridad en el paradigma computacional actual (Pomerance, 1996).

Junto a RSA, el otro pilar de la criptografía de clave pública moderna es la Criptografía de Curva Elíptica (ECC). A diferencia de RSA, que basa su seguridad en la dificultad de la factorización, ECC se fundamenta en la intratabilidad de un problema matemático diferente: el problema del logaritmo discreto sobre curvas elípticas (Koblitz, 1987).

La principal razón de la amplia adopción de ECC es su eficiencia. Para un nivel de seguridad equivalente, ECC requiere claves significativamente más cortas que RSA. Por ejemplo, una clave ECC de 256 bits ofrece una seguridad comparable a una clave RSA de 3072 bits. Esta eficiencia en tamaño y las operaciones computacionales más rápidas que permite han hecho de ECC la opción predilecta para entornos con recursos limitados, como los dispositivos móviles, las tarjetas inteligentes y, de manera crucial, para la generación de firmas digitales que aseguran las transacciones en la mayoría de las criptomonedas. (Koblitz, 1987)

Sin embargo, este paradigma de seguridad se enfrenta a una amenaza fundamental con la llegada de la computación cuántica. A diferencia de un bit clásico, la unidad de información cuántica, el qubit, aprovecha el principio de superposición para existir en una combinación de los estados 0 y 1 simultáneamente (García-Ripoll, 2019). Esta capacidad es lo que permite a un sistema de n qubits explorar un espacio de 2n estados a la vez, otorgándole un poder de procesamiento paralelo que crece de forma exponencial y que es inalcanzable para cualquier computadora clásica.

Este masivo paralelismo cuántico, por sí solo, no es suficiente para obtener una solución. Se necesita de otras dos propiedades cuánticas clave. Una es el entrelazamiento, que crea una conexión profunda e inseparable entre qubits, de modo que el estado de uno afecta instantáneamente al otro sin importar la distancia, una propiedad que Einstein describió como 'acción fantasmal a distancia'. La otra es la interferencia cuántica, que permite manipular las probabilidades de los estados para que los caminos computacionales que llevan a respuestas incorrectas se cancelen entre sí, mientras que aquellos que conducen a la solución correcta se refuerzan mutuamente (García-Ripoll, 2019).

Es precisamente la combinación de estas propiedades lo que otorga a ciertos algoritmos cuánticos una ventaja decisiva. El ejemplo más relevante para la criptografía es el algoritmo de Shor, desarrollado en 1994 (Shor, 1994). Este algoritmo está específicamente diseñado para encontrar los factores primos de números grandes en tiempo polinomial, una tarea que logra al encontrar eficientemente el período de una función modular. La herramienta cuántica clave para este paso es la Transformada Cuántica de Fourier (QFT), que transforma un problema de complejidad subexponencial en uno polinomial, una mejora drástica en eficiencia que recuerda a las predicciones

originales de Gordon Moore sobre el crecimiento exponencial de la capacidad de cómputo (Moore, 1965).

La QFT es el análogo cuántico de la Transformada de Fourier clásica, una herramienta fundamental en el procesamiento de señales para, por ejemplo, descomponer un sonido complejo en las notas musicales que lo componen. De manera similar, la QFT opera sobre las amplitudes de un estado cuántico para revelar su periodicidad. Su verdadera ventaja reside en la velocidad: gracias al paralelismo cuántico, la QFT es exponencialmente más rápida que su contraparte clásica, y es este salto en eficiencia el que constituye el núcleo de la potencia del algoritmo de Shor (Martín-Delgado, 2020). Al aplicar la QFT, el algoritmo transforma el problema de tal manera que la información del período se vuelve fácilmente extraíble, permitiendo así calcular los factores primos y volver a RSA teóricamente vulnerable.

Aunque el algoritmo de Shor existe, construir una computadora cuántica tolerante a fallos capaz de ejecutarlo contra claves como RSA-2048 es un desafío tecnológico inmenso. Estimaciones detalladas indican que se requerirían del orden de decenas de millones de qubits físicos para producir los miles de qubits lógicos necesarios (Gidney & Ekerå, 2021). La distinción entre ambos es crucial: un qubit físico es la implementación real (un ión, un circuito superconductor), que es inherentemente 'ruidoso' y propenso a errores. Para superar esta fragilidad, se utiliza la corrección de errores cuánticos, agrupando muchos qubits físicos para codificar la información de un único y estable qubit lógico.

A pesar de que las estimaciones más optimistas sugieren que podrían pasar una o dos décadas antes de que exista una computadora cuántica con la capacidad de amenazar

a RSA-2048 (Sevilla & Riedel, 2020), el riesgo inherente de un colapso criptográfico es de una magnitud tal que ha impulsado una respuesta proactiva y global. La comunidad de ciberseguridad ha optado por una postura de anticipación, reconociendo que la migración de toda la infraestructura digital es un proceso que también llevará muchos años y no se puede esperar a que la amenaza se materialice.

Es en este contexto de preparación anticipada que la comunidad criptográfica, liderada por organismos como el NIST, ha trabajado en la Criptografía Post-Cuántica (PQC). El objetivo de la PQC es estandarizar nuevos algoritmos de cifrado basados en problemas matemáticos que se consideren difíciles de resolver tanto para computadoras clásicas como cuánticas (Chen et al., 2016).

El proceso de estandarización iniciado por el NIST en 2016 no fue una simple selección interna, sino una competencia global y transparente. Durante más de seis años, docenas de algoritmos candidatos, propuestos por equipos de criptógrafos de todo el mundo, fueron sometidos a un intenso escrutinio público. En sucesivas rondas de evaluación, la comunidad internacional de seguridad informática intentó activamente 'romper' estos algoritmos, analizando su seguridad, eficiencia y facilidad de implementación.

La selección de CRYSTALS-Kyber como uno de los primeros estándares fue, por tanto, el resultado de haber sobrevivido a este riguroso proceso evolutivo. Este enfoque de competencia abierta le otorga una considerable confianza a los algoritmos finalistas, ya que han sido puestos a prueba por una vasta comunidad de expertos antes de ser aprobados (Alagic et al., 2022).

La criptografía basada en retículos, a la que pertenece CRYSTALS-Kyber, se ha convertido en una de las familias más prometedoras para la era post-cuántica. Un retículo, en este contexto, puede entenderse conceptualmente como una cuadrícula infinita de puntos en un espacio multidimensional. La seguridad de estos criptosistemas se fundamenta en la presunta dificultad de resolver ciertos problemas dentro de esta cuadrícula, como el 'Problema del Vector Más Corto' (Shortest Vector Problem, SVP), que consiste en encontrar el punto del retículo más cercano al origen (Bos et al., 2018).

Lo que hace a los problemas de retículos tan atractivos para la PQC es que, hasta la fecha, se cree que son computacionalmente difíciles de resolver incluso para las computadoras cuánticas. A diferencia del problema de la factorización, que es vulnerable al algoritmo de Shor, no se conoce un algoritmo cuántico que ofrezca una ventaja exponencial para resolver problemas como el SVP en sus casos más difíciles. Esta aparente resistencia a los ataques cuánticos es la razón por la cual una gran parte de los algoritmos finalistas del proceso del NIST, incluyendo Kyber, se basan en esta familia de problemas matemáticos (Alagic et al., 2022).

Para asegurar la resiliencia a largo plazo y no depender de la seguridad de un único tipo de problema matemático, el NIST optó por estandarizar un portafolio diversificado de algoritmos. Además de la criptografía basada en retículos, a la que pertenece CRYSTALS-Kyber, se seleccionaron algoritmos de otras familias. Un ejemplo notable es la criptografía basada en hashes, como el esquema de firma digital SPHINCS+, que fundamenta su seguridad en propiedades muy bien entendidas de las funciones hash, ofreciendo así un enfoque de seguridad alternativo (Alagic et al., 2022).

Centrándonos en el algoritmo principal de este estudio, la seguridad de CRYSTALS-Kyber se fundamenta específicamente en el problema de Aprendizaje con Errores en Módulos (Module-LWE). Este es una variante del problema más fundamental de Aprendizaje con Errores (LWE), que puede entenderse como el desafío de resolver un sistema de ecuaciones lineales donde las respuestas han sido alteradas con pequeños 'ruidos' o errores aleatorios (Bos et al., 2018).

La seguridad de los esquemas basados en LWE reside en la creencia de que este problema es computacionalmente intratable para las computadoras cuánticas. A diferencia de la factorización, no se conoce un algoritmo cuántico que pueda resolver eficientemente el problema LWE, lo que lo convierte en una base sólida para la criptografía post-cuántica (Bos et al., 2018; Alagic et al.).

Module-LWE utiliza este mismo principio de dureza, pero lo aplica sobre estructuras algebraicas más complejas, específicamente polinomios. Este cambio estructural es clave para la eficiencia del criptosistema.

El uso de estas estructuras polinómicas permite crear esquemas criptográficos con claves más pequeñas y operaciones más rápidas en comparación con los basados en LWE simple. Esta fue una razón fundamental para su elección en el diseño de CRYSTALS-Kyber, logrando un mejor equilibrio entre seguridad y rendimiento (Bos et al., 2018).

La amenaza cuántica no es un problema hipotético ni futuro; es una vulnerabilidad que ya se está explotando de forma silenciosa. La estrategia de ataque conocida como 'cosechar ahora, descifrar después' (harvest now, decrypt later), que consiste en capturar y almacenar volúmenes masivos de datos cifrados con la tecnología actual, ya está siendo empleada por diversos actores (ENISA, 2023). La apuesta es simple, esperar a que una

computadora cuántica funcional esté disponible para romper el cifrado RSA y acceder a todos esos secretos retrospectivamente. Esto convierte la criptografía que usamos hoy en una bomba de tiempo que amenaza la confidencialidad a largo plazo de secretos gubernamentales, propiedad intelectual, datos financieros y registros de salud.

El tipo de datos en riesgo es particularmente sensible. Se trata de secretos de estado con clasificaciones de seguridad de 50 años, datos genéticos o de salud que son inmutables para toda la vida de una persona, y propiedad intelectual o secretos comerciales cuyo valor reside en su confidencialidad a largo plazo. La certeza de un futuro descifrado devalúa la seguridad de cualquier información que necesite permanecer secreta más allá de la próxima década.

El colapso de la criptografía de clave pública, pilar de la confianza digital, tendría consecuencias sistémicas que irían mucho más allá del robo de datos. La validez de una firma digital, por ejemplo, es lo que garantiza la autenticidad de un contrato, la seguridad de las actualizaciones de software o la identidad en una transacción. Si la criptografía que la sustenta se rompe, esta confianza se desvanece, socavando las bases de la interacción en el mundo moderno (ENISA, 2023). Lo mismo ocurre con la Criptografía de Curva Elíptica (ECC), otro estándar fundamental que, si bien es más eficiente que RSA, también es vulnerable al algoritmo de Shor. Por ello, tecnologías emergentes como blockchain y las criptomonedas, cuya propiedad se asegura mediante firmas digitales basadas en ECC, se volverían completamente indefensas, permitiendo el robo de activos digitales a una escala masiva (Office of Management and Budget & Office of the National Cyber Director, 2024). La llegada de la computación cuántica no representa, por tanto, un paso más en el ciclo evolutivo de la criptografía, sino una ruptura fundamental que amenaza con invalidar todas las defensas desarrolladas en el último medio siglo.

El núcleo de la problemática actual reside en una peligrosa carrera contra el tiempo. Por un lado, tenemos el avance incierto pero constante hacia una computadora cuántica criptográficamente relevante, un hito a menudo denominado por la comunidad de seguridad como el 'Día Q' (Q-Day). Las proyecciones sugieren una probabilidad significativa de que esto ocurra en las próximas una o dos décadas (Sevilla & Riedel, 2020). Por otro lado, la migración de toda la infraestructura digital mundial a nuevos estándares post-cuánticos es un proceso de una complejidad y duración inmensas, que se estima podría llevar más de una década para ser completado de forma segura (Office of Management and Budget & Office of the National Cyber Director, 2024).

Es importante señalar que esta no es la primera gran migración criptográfica que ha enfrentado la industria tecnológica. Transiciones anteriores, como el paso del estándar de cifrado DES a AES a finales de los 90, o la paulatina migración de claves RSA de 1024 bits a 2048 bits a medida que aumentaba la capacidad de cómputo clásica, también fueron procesos complejos que se extendieron durante años y requirieron una coordinación significativa. Sin embargo, lo que diferencia a la transición a PQC es su naturaleza disruptiva y no incremental: no se trata de alargar una clave, sino de reemplazar los fundamentos matemáticos de toda nuestra infraestructura de seguridad, y hacerlo de manera proactiva antes de que la amenaza se materialice por completo.

La naturaleza de la migración propuesto no radica solo en cambiar bibliotecas de software. Un desafío mayúsculo se encuentra en el hardware especializado, como los Módulos de Seguridad de Hardware (HSMs) que protegen las claves maestras en bancos y centros de datos. Estos dispositivos físicos a menudo tienen ciclos de vida de muchos años y no pueden ser actualizados con un simple parche, requiriendo su reemplazo físico a un costo considerable. Además, la cadena de suministro de software presenta otra capa

de dificultad: una aplicación moderna no es monolítica, sino que depende de docenas de componentes y librerías de terceros. Una sola dependencia desactualizada en un componente menor podría dejar una puerta trasera vulnerable en todo un sistema, haciendo que el proceso de auditoría e inventario criptográfico sea una tarea hercúlea para cualquier organización grande (Office of Management and Budget & Office of the National Cyber Director, 2024).

Esta brecha temporal entre la aparición de la capacidad de ataque y la finalización de la defensa crea un período de máxima vulnerabilidad. En este escenario de alta incertidumbre y consecuencias potencialmente catastróficas, las organizaciones (incluyendo las de Argentina) enfrentan la tarea monumental de planificar y ejecutar su propia migración. Sin embargo, la elección de un sucesor para RSA como CRYSTALS-Kyber no es una decisión trivial. Requiere un profundo entendimiento de la viabilidad técnica, la robustez real, la eficiencia operativa y los desafíos prácticos de su adopción.

Precisamente esta necesidad de una evaluación integral es la que motiva esta investigación, que busca responder a la pregunta central: ¿Cuál es la viabilidad de la migración de RSA-2048 a CRYSTALS-Kyber en el contexto argentino, considerando no solo el análisis técnico sino también las percepciones y desafíos prácticos del sector?

Para abordar esta cuestión principal, se plantearon las siguientes preguntas específicas, organizadas en tres ejes temáticos:

- Eficiencia: ¿Cuál es la diferencia de rendimiento operativo y tamaño entre RSA-2048 y CRYSTALS-Kyber, y cómo se alinea esta diferencia con las percepciones de los profesionales sobre el impacto en sistemas del mundo real?

- Seguridad: ¿Cuáles son las fortalezas y vulnerabilidades teóricas de cada algoritmo y cómo se relacionan estas con el nivel de confianza y los riesgos de implementación percibidos por los especialistas en seguridad?
- Implementación: ¿Cuáles son las principales barreras técnicas y organizacionales para la adopción de la criptografía post-cuántica en Argentina, según la evidencia documental y la experiencia de los profesionales del sector?

El objetivo general de este trabajo es determinar la viabilidad de la migración del estándar criptográfico RSA-2048 a CRYSTALS-Kyber en el contexto argentino, integrando el análisis técnico de rendimiento y robustez con las percepciones y experiencias de profesionales del sector. Para alcanzar esta meta, se definieron los siguientes objetivos específicos:

- Contrastar el rendimiento operativo y el tamaño de los artefactos de RSA-2048 y CRYSTALS-Kyber, medidos experimentalmente, con las percepciones de los profesionales sobre el impacto de esta eficiencia en aplicaciones del mundo real.
- Analizar la robustez teórica de RSA-2048 y CRYSTALS-Kyber frente a amenazas conocidas y vincularla con las perspectivas de los especialistas sobre el nivel de confianza y los riesgos prácticos de implementación.
- Identificar y categorizar los desafíos técnicos y operativos para la adopción de la criptografía post-cuántica, interpretando las barreras percibidas por los profesionales en el contexto argentino.
- Proponer un conjunto de pautas estratégicas, derivadas del análisis integrado de los hallazgos, para facilitar la migración en las organizaciones.

Métodos

Diseño

La presente investigación se abordó desde un diseño predominantemente cualitativo, sostenido por un componente cuantitativo de carácter exploratorio y complementario. Esta elección metodológica permitió una exploración profunda de un fenómeno complejo y emergente como es la transición a la criptografía post-cuántica.

El núcleo cualitativo del estudio se centró en dos áreas principales. Primero, se realizó un análisis exhaustivo de fuentes secundarias, que incluyó literatura científica, estándares técnicos como los del NIST, e informes de organismos de ciberseguridad como ENISA.

En segunda instancia, se recolectaron datos cualitativos primarios mediante entrevistas semi-estructuradas a expertos y un cuestionario a profesionales junior para explorar las percepciones y experiencias en el contexto argentino.

De manera complementaria, se implementó un experimento cuantitativo de alcance acotado. Su propósito fue obtener métricas de rendimiento empíricas y objetivas (velocidad y tamaño) para los algoritmos RSA-2048 y CRYSTALS-Kyber en un entorno controlado. Estos datos no buscan ser generalizables a todos los escenarios posibles, sino servir como un punto de partida concreto para la discusión sobre la eficiencia técnica.

La combinación de estos componentes, aunque de peso mayormente cualitativo, permitió la triangulación de la información. De esta forma, se pudieron contrastar los datos teóricos de la revisión documental con las perspectivas prácticas de los profesionales y los hallazgos de rendimiento del experimento, fortaleciendo así la validez de las conclusiones del estudio.

En cuanto a su alcance general, el estudio fue comparativo, al contrastar los dos algoritmos; descriptivo, al detallar sus características y los desafíos asociados; y exploratorio, al indagar sobre las perspectivas en un campo nuevo. Por su finalidad de generar conocimiento directamente utilizable para la toma de decisiones, la investigación se enmarca como aplicada.

Participantes

Para la recolección de datos cualitativos se trabajó con dos grupos de participantes diferenciados. La selección para ambos se realizó mediante un muestreo no probabilístico, adaptado a los fines exploratorios y de profundización de este estudio.

El primer grupo se compuso por dos expertos con roles directivos. Para ellos se utilizó un muestreo intencional o por criterio, buscando deliberadamente individuos cuya experiencia en la toma de decisiones estratégicas, gestión de riesgos y planificación a largo plazo pudiera aportar una perspectiva única sobre la viabilidad operativa de la migración PQC.

Este grupo de expertos estuvo conformado por el responsable del área de tecnología de una importante entidad del sector financiero regional y el director de tecnologías de información de una universidad nacional, lo que permitió contrastar dos contextos organizacionales distintos.

El segundo grupo consistió en diecisiete analistas, licenciados y/o estudiantes avanzados de informática. Para este grupo se empleó un muestreo por conveniencia, con el objetivo de evaluar el nivel de conciencia y la preparación académica de la base de profesionales que implementará estas nuevas tecnologías en el futuro.

Es fundamental reconocer las limitaciones de esta muestra. Debido al reducido número de participantes y a los métodos de selección no probabilísticos, los hallazgos cualitativos no son estadísticamente representativos ni generalizables. Su valor es puramente exploratorio y sirve para identificar temas clave y contrastar perspectivas.

Se implementaron procedimientos de consentimiento informado adaptados a cada grupo de participantes, garantizando siempre los principios éticos de voluntariedad y confidencialidad.

Para el grupo de expertos directivos, se obtuvo su consentimiento informado por escrito antes de realizar cada entrevista. En dicho documento se detalló el propósito del estudio, la naturaleza voluntaria de su participación y las medidas para asegurar la estricta confidencialidad y el anonimato de sus respuestas en la publicación de los resultados. El modelo de este formulario se puede consultar en el Anexo II.

Para el grupo de analistas y licenciados, que respondieron a un cuestionario online, la participación fue completamente voluntaria y anónima. Al inicio del formulario se presentó una descripción clara de la investigación y sus objetivos. De acuerdo con las prácticas estándar para encuestas anónimas de bajo riesgo, el acto de completar y enviar voluntariamente el cuestionario fue considerado como consentimiento implícito para participar. Este método se eligió para preservar el anonimato total de los encuestados, ya que solicitar un convenio por escrito habría requerido recoger datos identificatorios. La adaptación de la encuesta realizada se encuentra en Anexo III

Instrumentos

Para la recolección de los datos requeridos en esta investigación se empleó un conjunto de materiales e instrumentos específicos, adaptados a la naturaleza de cada objetivo y tipo de dato.

En las pruebas de rendimiento cuantitativas, el material principal fue una computadora de escritorio con un procesador AMD Ryzen 5 5600x y 24 GB de RAM, operando bajo Windows 11. Como instrumentos de software se utilizó Python versión 3.12, junto a la biblioteca cryptography versión 44.0.3 para las operaciones con RSA-2048 y la biblioteca de código abierto liboqs versión 0.12.0 (vía un wrapper de Python) para CRYSTALS-Kyber. La medición precisa de los tiempos de ejecución se realizó con el módulo timeit.

La recolección de datos secundarios se fundamentó en la revisión documental sistemática. Se utilizaron como instrumentos de búsqueda diversas bases de datos académicas y repositorios científicos, como IEEE Xplore, ACM Digital Library y Google Scholar. Se aplicaron criterios de búsqueda específicos (ej. 'CRYSTALS-Kyber security', 'RSA quantum threat') para seleccionar los materiales analizados, que incluyeron artículos de investigación, actas de conferencias especializadas e informes técnicos de organismos como el NIST y ENISA.

Para obtener los datos cualitativos de los expertos directivos, el instrumento principal fue una guía de entrevista semi-estructurada. Esta fue diseñada para explorar en profundidad temas como la percepción del riesgo y las estrategias de migración (ver Anexo I). Las sesiones se apoyaron en un dispositivo de grabación de audio, previo consentimiento.

Finalmente, para el grupo de profesionales junior y estudiantes, el instrumento fue un cuestionario online (realizado con Google Forms) con preguntas abiertas. El cuestionario se adaptó de la guía de entrevista principal, con el objetivo de evaluar el nivel de conocimiento y la percepción del tema en este segundo grupo de participantes.

Análisis de datos

El análisis de los datos recolectados se realizó mediante técnicas específicas para cada tipo de información, con el objetivo de integrar los hallazgos para responder a los objetivos del estudio. Como paso previo, se definieron conceptual y operacionalmente los constructos centrales de la investigación.

La eficiencia computacional se entendió como el uso óptimo de recursos de un algoritmo en relación con su seguridad (Alagic et al., 2022; Chen et al., 2016). Operacionalmente, se midieron los tiempos de ejecución y el tamaño de los artefactos criptográficos, es decir, los componentes generados por el algoritmo como las claves públicas, las claves secretas y los criptogramas.

La robustez criptográfica se definió como la capacidad de un sistema para resistir ataques, fundamentándose en la dificultad de sus problemas matemáticos subyacentes (National Institute of Standards and Technology, 2024; Alagic et al., 2022). Su evaluación se operacionalizó mediante la revisión de la base teórica de cada algoritmo y su resistencia a amenazas conocidas.

Finalmente, los desafíos de adopción se conceptualizaron como las barreras técnicas y organizacionales para la migración (ENISA, 2023; Office of Management and Budget & Office of the National Cyber Director, 2024). Estos se operacionalizaron a

través de su identificación en la literatura y en las entrevistas, donde destacó la necesidad de un inventario criptográfico, entendido como el proceso sistemático de descubrir, catalogar y gestionar todos los algoritmos criptográficos en uso dentro de una organización.

El análisis de los datos cuantitativos de rendimiento se realizó mediante estadística descriptiva. Se calcularon indicadores como la media y la desviación estándar para comparar objetivamente la eficiencia de ambos algoritmos.

Para los datos cualitativos, tanto de las entrevistas como de los cuestionarios, se empleó un análisis temático. Este proceso implicó la codificación sistemática de las respuestas para identificar y agrupar patrones y temas recurrentes.

La fase final del análisis consistió en la integración y triangulación de todos los hallazgos. Se contrastaron los resultados cuantitativos con los cualitativos para fortalecer la validez de las conclusiones del estudio.

Resultados

En respuesta al primer objetivo, el análisis experimental sobre la eficiencia computacional reveló diferencias notables en el rendimiento de los algoritmos. La disparidad más significativa se observó en la generación de pares de claves, donde ML-KEM-512 demostró una eficiencia órdenes de magnitud superior a la de RSA-2048. La consistencia en los tiempos de ejecución, evidenciada por una baja desviación estándar en ambos casos, subraya la fiabilidad de esta comparación, cuyos datos se detallan en la Tabla 1.

Tabla 1. *Tiempos de Generación de Pares de Claves para RSA-2048 y ML-KEM-512*

Algoritmo	Mínimo (s)	Máximo (s)	Media (s)	Desv. Estándar (s)
RSA-2048	3.479×10−2	3.616×10−2	3.579×10−2	5.146×10−4
ML-KEM-512	1.929×10−4	2.120×10−4	2.002×10−4	6.310×10−6

Fuente: Elaboración propia.

El panorama para las operaciones de aseguramiento de la confidencialidad fue más matizado. Para el cifrado de mensajes pequeños, RSA-2048 mantuvo una clara ventaja en velocidad. Inversamente, en la operación de recuperación del secreto, el decapsulamiento con ML-KEM-512 fue notablemente más eficiente que el descifrado con RSA. La Tabla 2 y la Tabla 3 exponen los datos descriptivos que sustentan este hallazgo de rendimiento contrapuesto.

Tabla 2. *Tiempos de Cifrado (RSA) y Encapsulamiento de Clave (ML-KEM) en segundos*

Algoritmo	Operación	Mínimo (s)	Máximo (s)	Media (s)	Desv. Estándar (s)
RSA-2048	Cifrado	2.198×10−5	2.479×10−5	2.299×10−5	8.888×10−7
ML-KEM-512	Encapsulado	2.168×10−4	2.341×10−4	2.243×10−4	6.428×10−6

Fuente: Elaboración propia.

Tabla 3. *Tiempos de Descifrado (RSA) y Decapsulamiento de Clave (ML-KEM)*

Algoritmo	Operación	Mínimo (s)	Máximo (s)	Media (s)	Desv Estándar (s)
RSA-2048	Descifrado	4.745×10−4	4.909×10−4	4.818×10−4	6.453×10−6
ML-KEM-512	Decapsulado	1.807×10−4	1.919×10−4	1.862×10−4	3.744×10−6

Fuente: Elaboración propia.

Un resultado cuantitativo adicional y de gran relevancia fue el considerable aumento en el tamaño de los artefactos criptográficos para ML-KEM-512. Se constató que tanto las claves públicas como los criptogramas resultantes son aproximadamente tres veces más grandes que sus equivalentes en RSA-2048 para un nivel de seguridad comparable, como se detalla en la Tabla 4.

Tabla 4. *Comparación de Tamaños de Claves y Datos Criptográficos en bytes*

Algoritmo	Tipo de Dato	Tamaño (bytes)
RSA-2048	Clave Pública	294
RSA-2048	Clave Privada	1216
RSA-2048	Texto Cifrado	256
ML-KEM-512	Clave Pública	800
ML-KEM-512	Clave Secreta	1632
ML-KEM-512	Criptograma (KEM)	768
ML-KEM-512	Secreto Compartido	32

Fuente: Elaboración propia.

Para abordar el segundo objetivo, el análisis de la literatura sobre la robustez criptográfica reveló un perfil de seguridad diferenciado para cada algoritmo. Se constató que la seguridad de RSA-2048 se fundamenta en la dificultad de la factorización de enteros, y que esta base matemática es teóricamente vulnerable al algoritmo de Shor en un entorno cuántico. Para CRYSTALS-Kyber, se encontró que su seguridad se basa en la presunta dificultad del problema Module-LWE, el cual es considerado resistente a ataques cuánticos conocidos. Adicionalmente, se identificó que su seguridad práctica está supeditada a la calidad de sus implementaciones, siendo los ataques de canal lateral y por inyección de fallos las amenazas más relevantes que la literatura señala a considerar.

Al consultar a los especialistas sobre su percepción de esta robustez, expresaron un alto nivel de confianza en la seguridad teórica de Kyber debido a su estandarización por el NIST. Sin embargo, compartieron la preocupación sobre los riesgos de implementación, señalando que la confianza del sector dependerá no solo de la fortaleza del algoritmo, sino de la disponibilidad de implementaciones auditadas y de la capacidad de los equipos técnicos para gestionarlas de forma segura.

En relación con el tercer objetivo, la investigación identificó un conjunto de desafíos significativos para la adopción de la criptografía post-cuántica. El análisis documental reveló la existencia de retos técnicos, como el impacto del mayor tamaño de los artefactos en los protocolos de red y la complejidad de la integración con sistemas heredados. A nivel operativo y organizacional, se identificaron retos como la necesidad de un inventario criptográfico exhaustivo, los altos costos de migración y la planificación estratégica a largo plazo.

Los datos primarios cualitativos complementaron y jerarquizaron estos hallazgos. Las entrevistas con los dos expertos directivos confirmaron que los principales obstáculos percibidos son la falta de personal capacitado, los costos asociados y la ausencia de un marco regulatorio que impulse la transición. Por su parte, el sondeo realizado a diecisiete analistas y licenciados en informática reveló un patrón claro en la percepción de los desafíos, donde los obstáculos de naturaleza organizacional y de recursos humanos fueron mencionados con una frecuencia notablemente mayor que los puramente técnicos, tal como se sintetiza en la Tabla 5.

Tabla 5. *Frecuencia de Desafíos de Adopción Percibidos por Profesionales Junior y Estudiantes*

Categoría del Desafío	Desafío Específico	Frecuencia de Mención (Nº de participantes)
Organizacional y Humano	Falta de Personal Capacitado / Brecha de Conocimiento	16
Económico	Altos Costos de Migración e Inversión	14
Organizacional y Humano	Falta de Conciencia o Prioridad Gerencial	12
Técnico	Integración con Sistemas Heredados (legacy)	11
Técnico	Impacto en el Rendimiento de Red y Sistemas	8
Político / Estratégico	Ausencia de un Marco Regulatorio o Impulso Estatal	7

Fuente: Elaboración propia.

Finalmente, aunque el cuarto objetivo específico sobre proponer pautas se desarrolla en la Discusión, los resultados de las entrevistas y la encuesta aportaron los insumos clave para ellas. Se encontró un consenso claro entre todos los participantes (tanto expertos directivos como profesionales junior) en que la transición exitosa en Argentina requiere un enfoque colaborativo. Señalaron que el Gobierno debe establecer las normas, las Universidades deben formar a los profesionales, y las Empresas deben ejecutar la implementación, indicando que ningún sector puede liderar el cambio de forma aislada.

Discusión

El análisis de los resultados obtenidos permite una interpretación profunda sobre la viabilidad de la transición desde RSA-2048 hacia CRYSTALS-Kyber. La discusión que sigue pone en diálogo los hallazgos experimentales, la evidencia documental y las perspectivas de los profesionales consultados, con el fin de contextualizar las implicaciones técnicas y organizacionales de este cambio criptográfico para el escenario argentino.

En lo que respecta al primer objetivo, la eficiencia computacional, los resultados mostraron un panorama de contrapartidas que merece un análisis detallado. La notable superioridad de Kyber en la generación de claves, por ejemplo, no es solo una métrica de rendimiento, sino que tiene implicaciones estratégicas. Sugiere que la adopción de Kyber podría habilitar nuevas arquitecturas de seguridad en entornos dinámicos, como protocolos con claves de sesión efímeras (Perfect Forward Secrecy) o la generación masiva de identidades en el ecosistema de IoT, escenarios donde la latencia de RSA ha sido históricamente un factor limitante.

Por otro lado, en cifrado de mensajes pequeños, RSA-2048 se mostró superior en velocidad. Este hallazgo, a menudo pasado por alto en discusiones de alto nivel, es crucial para organizaciones con un alto volumen de transacciones mínimas, como en ciertos sistemas de pago o autenticación. La discusión con los expertos directivos confirmó que, aunque este impacto podría ser marginal en muchos casos, es un factor que debe ser evaluado en pruebas de concepto específicas antes de una migración a gran escala, para evitar la introducción de nuevos cuellos de botella en el rendimiento de aplicaciones críticas.

Esta dicotomía en el rendimiento es más que una curiosidad técnica; revela que la elección del algoritmo PQC podría no ser uniforme dentro de una misma organización. Por ejemplo, un servidor web que establece miles de conexiones TLS por segundo se beneficiaría enormemente de la rápida generación de claves de Kyber para las sesiones efímeras. Sin embargo, un sistema de microservicios que intercambia constantemente pequeños mensajes cifrados de estado o comandos podría, en teoría, verse ligeramente afectado por la latencia del encapsulamiento de Kyber. Este análisis subraya que la migración no será un simple 'reemplazar todo', sino que podría requerir una estrategia diferenciada según el caso de uso específico dentro de la arquitectura de la empresa.

Además, el mayor tamaño de los artefactos criptográficos de Kyber es uno de los desafíos técnicos más tangibles. Este hallazgo, consistente con los informes del NIST (Alagic et al., 2022) y de ENISA (2023), y señalado por los expertos entrevistados, representa uno de los primeros 'costos' reales de la migración. El impacto va más allá del simple almacenamiento, afectando directamente a protocolos de red como TLS e IKEv2, donde podría generar fragmentación de paquetes y mayor latencia. Esto subraya que la migración implicará costos no solo en software, sino potencialmente en la optimización de la infraestructura de red para manejar este nuevo volumen de datos, un punto técnico que requerirá adaptaciones significativas a los estándares (IETF PQC Working Group, s.f.; Stebila & Mosca, 2016).

En cuanto al segundo objetivo, la robustez criptográfica, se confirmó la obsolescencia teórica de RSA-2048 frente al algoritmo de Shor (Shor, 1994). La seguridad de CRYSTALS-Kyber, respaldada por su estandarización por el NIST (NIST, 2024, FIPS 203), se basa en la dureza del problema Module-LWE. No obstante, la discusión con los expertos y la revisión de la literatura (ENISA, 2023; Bos et al., 2018)

permitieron profundizar y matizar esta afirmación: la fortaleza teórica es insuficiente por sí sola. La seguridad real dependerá críticamente de la calidad de las implementaciones para mitigar amenazas como los ataques de canal lateral. Como expresó uno de los directivos consultados, "la matemática de Kyber puede ser perfecta, pero si la implementación deja una puerta abierta, es como tener una caja fuerte de titanio con la llave debajo del felpudo". Esta perspectiva subraya que la inversión en auditorías de seguridad será tan importante como la propia migración del algoritmo.

Esta transición de la seguridad, desde la dureza de un problema matemático a la calidad de una implementación de software, cambia fundamentalmente la naturaleza del riesgo. La superficie de ataque ya no se limita al criptoanálisis teórico, sino que se expande para incluir errores de programación sutiles, una gestión de memoria deficiente o fallas en la generación de números aleatorios que pueden ser explotadas. Una implementación incorrecta de CRYSTALS-Kyber podría, paradójicamente, resultar en un sistema menos seguro en la práctica que un sistema RSA maduro y bien comprendido. Este hecho pone una presión enorme sobre los equipos de desarrollo y seguridad, y se vincula directamente con la brecha de conocimiento identificada en este estudio: sin una comprensión profunda de los nuevos vectores de ataque, el riesgo de introducir vulnerabilidades durante la migración es extremadamente alto.

Esta desconexión entre la visión estratégica y la conciencia de la base técnica no es un problema menor; es una vulnerabilidad organizacional activa. En la práctica, podría manifestarse de múltiples formas: equipos de desarrollo que, al no comprender la criticidad, implementen las nuevas bibliotecas PQC como un simple reemplazo, sin prestar atención a los nuevos vectores de ataque como los de canal lateral; gerencias de proyecto que subestimen los recursos y tiempos necesarios para la migración, llevando a

planificaciones irreales; o una falta general de apoyo operativo a las iniciativas de seguridad, que serían vistas como un 'gasto' en lugar de una inversión estratégica. Esta brecha, por tanto, puede sabotear la transición desde adentro antes de que cualquier amenaza externa se materialice.

Abordando el tercer objetivo, los desafíos de adopción identificados en la literatura, como la necesidad de un inventario criptográfico (ENISA, 2023) o la integración con sistemas heredados (Chen et al., 2016), fueron fuertemente corroborados por las perspectivas locales. Sin embargo, las entrevistas permitieron jerarquizar estos desafíos para el contexto argentino. Mientras que los informes internacionales a menudo ponen un gran énfasis en la complejidad técnica, los expertos directivos y los profesionales junior locales coincidieron de manera abrumadora en que las barreras más significativas son el impacto de los altos costos en una economía volátil y, de manera aún más enfática, la falta de personal capacitado. Este hallazgo es crucial, ya que desplaza el foco del debate desde un problema puramente tecnológico (¿es Kyber seguro y rápido?) a uno de estrategia, inversión y desarrollo de talento a nivel nacional (¿tenemos la capacidad y los recursos para implementarlo?).

Es crucial analizar estos desafíos organizacionales a la luz del contexto socioeconómico particular de Argentina. La barrera de los 'altos costos', por ejemplo, se magnifica en un entorno de alta volatilidad económica. Si bien las políticas de importación se han flexibilizado recientemente, las empresas locales aún enfrentan el desafío de adquirir hardware especializado y licencias de software dolarizadas, lo que representa una inversión significativamente mayor en moneda local. De manera similar, la 'escasez de personal capacitado' no se debe a una falta de talento, sino que se ve agravada por la alta demanda global que compite por los profesionales argentinos,

dificultando la retención de perfiles altamente especializados en áreas de vanguardia como PQC.

Un hallazgo particularmente revelador de este estudio, surgido al contrastar los dos grupos de participantes, fue la divergencia en la percepción del riesgo. Mientras los expertos directivos mostraron una clara conciencia de la urgencia impulsada por la amenaza del 'cosechar ahora, descifrar después', el sondeo a los profesionales junior reveló una baja percepción sobre la inminencia de la amenaza. Esta brecha entre la visión estratégica y la conciencia de la base técnica es un desafío organizacional significativo en sí mismo. Podría traducirse en una falta de apoyo operativo a las iniciativas de migración, en la subestimación de los recursos necesarios por parte de los equipos de desarrollo, o en la introducción de vulnerabilidades por una implementación que no comprende la criticidad de la tarea. Las causas de esta divergencia pueden ser múltiples: desde una comunicación interna deficiente sobre los riesgos estratégicos, hasta una sobrecarga de trabajo en los equipos técnicos que les impide enfocarse en amenazas a largo plazo, o una falta de exposición al tema en los planes de estudio universitarios, como también reveló este estudio. Identificar y cerrar esta brecha es, por tanto, un prerrequisito para cualquier plan de migración exitoso.

A partir de este análisis, y en respuesta al cuarto objetivo, se pueden formular las siguientes pautas estratégicas. Primero, es fundamental fomentar una cultura de 'agilidad criptográfica'. Esto no es solo una buena práctica, sino una necesidad para la supervivencia digital. Implica que las organizaciones deben invertir en arquitecturas modulares que no queden 'atadas' a un solo algoritmo, facilitando futuras migraciones con menor costo y disrupción, una recomendación consistente con los informes de ENISA (2023) No adoptar este enfoque desde ahora implica acumular una 'deuda criptográfica'

significativa. Cada nuevo sistema o aplicación desarrollado sin agilidad criptográfica en mente se convertirá en un problema costoso y complejo de solucionar en el futuro, multiplicando el costo y el riesgo de la migración cuando esta ya no sea opcional, sino una emergencia.

En la práctica, los pasos a seguir varían según el tamaño de la organización. Una pyme que utiliza servicios en la nube, por ejemplo, debería comenzar por exigir a sus proveedores que demuestren tener una hoja de ruta PQC. Una gran empresa, en cambio, debe iniciar una auditoría interna para identificar sus propias aplicaciones críticas con dependencias criptográficas 'duras' y planificar su refactorización.

Una segunda recomendación crucial es priorizar la capacitación a todo nivel. La brecha de conocimiento identificada en este estudio es un obstáculo mayor. Es esencial que las universidades actualicen sus currículas para incluir PQC de forma obligatoria y que las empresas creen planes de formación continua. Un ejemplo de acción concreta para una empresa podría ser la creación de un pequeño 'equipo PQC' piloto, encargado de realizar cursos de formación y presentar informes internos sobre los estándares del NIST, iniciando así la difusión del conocimiento.

Para llevar esto a la práctica, los roles deben ser diferenciados. Una universidad, por ejemplo, podría no solo actualizar las materias de grado, sino también crear cursos de extensión o diplomaturas en PQC dirigidas específicamente a profesionales que ya están en el mercado y necesitan reconvertirse. Dentro de una empresa, la capacitación debe ser segmentada: mientras que los equipos técnicos necesitan una formación profunda en las nuevas bibliotecas y vectores de ataque, los equipos de gestión y legales deben recibir formación sobre el impacto en los riesgos, los contratos y la continuidad del negocio.

En tercer lugar, se sugiere un enfoque de implementación gradual y basado en riesgos. La adopción de modelos híbridos, que combinan criptografía clásica y PQC durante la transición, fue señalada por los expertos como una estrategia pragmática. Esto permite mitigar riesgos, asegurar la interoperabilidad con socios que aún no han migrado y validar las nuevas implementaciones en entornos controlados (por ejemplo, en sistemas internos de bajo riesgo) antes de un despliegue completo en sistemas de cara al cliente.

Este enfoque gradual puede adaptarse al perfil de cada organización. Una empresa de desarrollo de software con alta tolerancia a la experimentación podría comenzar implementando un modelo híbrido en sus sistemas de comunicación interna, como un chat o una intranet, para ganar experiencia en un entorno de bajo impacto. Por el contrario, una entidad financiera, con una aversión al riesgo mucho mayor, podría aplicar este enfoque primero en un sistema de back-office no crítico, como la gestión de reportes internos, permitiéndole validar la tecnología y los procesos antes de considerar siquiera un despliegue en sistemas transaccionales.

Finalmente, la colaboración interinstitucional es indispensable. Se requiere un rol activo del gobierno argentino en la creación de una hoja de ruta nacional, siguiendo el ejemplo de la directiva de la Casa Blanca (Office of Management and Budget & Office of the National Cyber Director, 2024). Esta hoja de ruta debe coordinar los esfuerzos de la academia, los proveedores de tecnología y las industrias críticas para crear un ecosistema de apoyo.

Sin embargo, las organizaciones no deben esperar pasivamente por esta directiva gubernamental. A nivel práctico y proactivo, una empresa puede comenzar a impulsar la conversación participando en las cámaras y foros de su sector industrial para crear un

grupo de trabajo sobre PQC. Una universidad, por su parte, podría liderar la creación de un consorcio con empresas locales para proyectos de investigación aplicada y pruebas de concepto conjuntas. Estas iniciativas 'desde la base' son cruciales para generar el impulso y el conocimiento que luego facilitarán la implementación de una estrategia nacional.

La principal fortaleza y contribución de esta investigación radica en su enfoque integral y contextualizado para Argentina. En primer lugar, este estudio aporta datos empíricos originales sobre el rendimiento de CRYSTALS-Kyber frente a RSA-2048 en una configuración de hardware y software específica y replicable. Si bien la literatura internacional ofrece benchmarks, estos resultados locales sirven como un punto de partida tangible para que las organizaciones argentinas puedan estimar el impacto de la migración en sus propias infraestructuras, en lugar de depender exclusivamente de métricas obtenidas en contextos tecnológicos diferentes.

En segundo lugar, una contribución única de este trabajo es la triangulación de perspectivas cualitativas. Al no limitarse a la visión de los expertos directivos, sino complementarla con el sondeo a profesionales junior y estudiantes avanzados, la investigación pudo sacar a la luz un hallazgo no documentado previamente en este contexto: la brecha en la percepción del riesgo. Este descubrimiento es, en sí mismo, un aporte significativo, ya que identifica un obstáculo humano y cultural que es tan o más importante que los desafíos puramente técnicos.

Finalmente, el estudio no se queda en el diagnóstico, sino que avanza hacia la propuesta de pautas estratégicas adaptadas. La combinación del análisis técnico con las realidades organizacionales y socioeconómicas de Argentina permite ofrecer recomendaciones que son más que una simple traducción de guías internacionales. Al

contextualizar los desafíos, este trabajo ofrece un panorama multifacético de la viabilidad de la migración que no se había explorado previamente, sirviendo como un recurso fundamentado para la toma de decisiones en la región.

A pesar de estos hallazgos, es importante reconocer las limitaciones inherentes a este estudio. El experimento de rendimiento se realizó en un único entorno de hardware y software. Si bien esto garantiza la consistencia comparativa de los datos obtenidos, sus resultados no pueden generalizarse directamente a todas las arquitecturas posibles. El rendimiento de los algoritmos PQC puede variar significativamente en servidores de alta gama, plataformas en la nube o, especialmente, en sistemas con diferentes conjuntos de instrucciones de procesador, lo que requiere que cada organización realice sus propias pruebas de concepto.

Además, la muestra de participantes cualitativos fue pequeña y seleccionada de forma no probabilística. Aunque permitió obtener perspectivas profundas y ricas en matices de actores clave en los sectores financiero y académico, y contrastarlas con las de profesionales junior, sus opiniones no son estadísticamente representativas del conjunto de todas las organizaciones en Argentina. Su valor, por tanto, es puramente exploratorio y sirve para identificar temas y preocupaciones que merecen una investigación más amplia.

Finalmente, este estudio se centró en la comparación de RSA-2048 con una de las variantes de CRYSTALS-Kyber. El panorama de la PQC es vasto e incluye otros mecanismos de encapsulamiento de clave y, de manera crucial, esquemas de firma digital como CRYSTALS-Dilithium o SPHINCS+, que enfrentarán sus propios desafíos de implementación y rendimiento, los cuales no fueron abordados en esta investigación.

Estas mismas limitaciones abren nuevas y valiosas líneas de investigación futura. Sería crucial ampliar las pruebas de rendimiento a plataformas de bajo consumo energético, como las utilizadas en dispositivos IoT, donde el impacto del tamaño y la eficiencia es aún más crítico. Un análisis del consumo energético de estos algoritmos sería, de por sí, un aporte muy relevante.

Asimismo, se necesitan con urgencia estudios cualitativos con muestras más amplias y diversas para obtener una visión más granular de los desafíos por sector industrial en Argentina (ej. salud, gobierno, energía). Esto permitiría desarrollar pautas de migración mucho más específicas y efectivas para cada tipo de organización.

Finalmente, la realización de estudios de caso longitudinales sobre implementaciones piloto en empresas locales sería invaluable. Documentar los costos reales, los tiempos de implementación, las barreras culturales y las lecciones aprendidas a lo largo de varios años ofrecería una guía práctica sin precedentes para el resto del ecosistema empresarial argentino.

En conclusión, y en respuesta directa a la pregunta central de esta investigación, se determina que la sustitución de RSA-2048 por CRYSTALS-Kyber es técnicamente viable. El nuevo estándar ofrece una robustez teórica sólida frente a la amenaza cuántica y presenta ventajas de rendimiento en operaciones clave como la generación de claves, lo que lo posiciona como un sucesor adecuado desde una perspectiva puramente algorítmica.

Sin embargo, esta viabilidad técnica no garantiza una transición exitosa. La verdadera barrera para la adopción de Kyber en Argentina, como ha revelado este estudio, no es de naturaleza criptográfica, sino operativa y organizacional. La viabilidad de la migración está severamente condicionada por los altos costos, la escasez de profesionales

capacitados y, de manera crítica, una brecha en la percepción del riesgo entre los niveles directivos y la base técnica que deberá implementar los cambios.

El éxito de esta transición dependerá menos de la superioridad algorítmica de Kyber y más de la capacidad de las organizaciones para invertir en su capital humano y en una planificación estratégica a largo plazo. En última instancia, la seguridad de la infraestructura digital de Argentina en la era post-cuántica no se decidirá con la llegada del primer computador cuántico, sino con las acciones, y omisiones, que se inicien hoy.

Referencias

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., ... Stiehler, E. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (NIST Internal Report 8413)*. Gaithersburg, MD: National Institute of Standards and Technology. doi:10.6028/NIST.IR.8413

Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032

Chen, L., Chen, L.-K., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography (NISTIR 8105)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

ENISA (European Union Agency for Cybersecurity). (2023). *Post-Quantum Cryptography: Current state and quantum mitigation*. Recuperado de https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

García-Ripoll, J. J. (2019). *Introducción a la computación cuántica*. Madrid, España: Consejo Superior de Investigaciones Científicas (CSIC).

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. doi:10.22331/q-2021-04-15-433

IETF PQC Working Group. (s.f.). *Post-Quantum Cryptography Use Cases*. Recuperado de https://www.ietf.org/archive/id/draft-vaira-pquip-pqc-use-cases-00.html

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209

Martín-Delgado, M. A. (2020). El algoritmo de Shor. *Revista Española de Física*, *34*(2), 48-54.

Microsoft Security Response Center. (2023). *Microsoft Digital Defense Report 2023*. Microsoft. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Moore, G. E. (1965). Cramming more components onto integrated circuits. Electronics, 38(8), 114–117. https://ieeexplore.ieee.org/document/7165076.

National Institute of Standards and Technology. (2024). *Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS Publication 203)*. Gaithersburg, MD: U.S. Department of Commerce. doi:10.6028/NIST.FIPS.203

Office of Management and Budget & Office of the National Cyber Director. (2024). *Report on the Migration to Post-Quantum Cryptography*. Executive Office of the President of the United States. Recuperado de https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

Pomerance, C. (1996). A Tale of Two Sieves. *Notices of the AMS*, *43*(12), 1473-1485.

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.

Sevilla, J., & Riedel, C. J. (2020). *Forecasting timelines of quantum computing*. NTT Research, Inc. Recuperado de https://ntt-research.com/wp-content/uploads/2022/09/Forecasting-timelines-of-quantum-computing1.pdf

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. En S. Goldwasser (Ed.), *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). Los Alamitos, CA: IEEE Computer Society Press. doi:10.1109/SFCS.1994.365700

Singh, S. (1999). *The code book: The evolution of secrecy from Mary, Queen of Scots, to quantum cryptography*. New York, NY: Doubleday

Stebila, D., & Mosca, M. (2016). *Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project*. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2016/1017

Anexos

I Estructura de entrevista a profesionales directivos

1. Percepción de la Amenaza Cuántica:

* ¿Cuán real o inminente percibe la amenaza de la computación cuántica para los sistemas de criptografía que se usan actualmente, como RSA o la Criptografía de Curva Elíptica, en el contexto argentino o específicamente en su organización?

* En su ámbito profesional, ¿se están tomando actualmente medidas o se está planificando la transición hacia una criptografía resistente a los avances cuánticos? ¿Podría comentarme por qué sí o por qué no?

2. Conocimiento y Evaluación de CRYSTALS-Kyber:

* ¿Qué conocimiento tiene sobre los nuevos estándares de criptografía post-cuántica (es decir, resistente a ataques con computadoras cuánticas) que ha estado desarrollando el Instituto Nacional de Estándares y Tecnología de Estados Unidos, conocido como NIST? En particular, ¿qué sabe sobre el algoritmo CRYSTALS-Kyber?

* Desde su punto de vista, ¿considera que CRYSTALS-Kyber es una alternativa viable y segura para reemplazar a algoritmos como RSA? ¿Cuáles serían sus razones?

* ¿Qué ventajas o desventajas técnicas identifica usted en CRYSTALS-Kyber en comparación con RSA, incluso dejando de lado su mayor resistencia frente a la computación cuántica?

3. Desafíos de Implementación y Adopción (Técnicos y Operativos):

* Desde su perspectiva, ¿cuáles considera que serían los principales obstáculos técnicos al momento de migrar los sistemas que hoy utilizan criptografía clásica hacia un algoritmo como CRYSTALS-Kyber? (Por ejemplo: ¿piensa en el rendimiento en dispositivos con recursos limitados, el tamaño de las claves o el impacto en las comunicaciones, la compatibilidad con protocolos o hardware que ya existen, la necesidad de nuevas librerías de software o Interfaces de Programación de Aplicaciones?)

* Y en cuanto a los obstáculos operativos u organizacionales, ¿cuáles visualiza como los principales? (Por ejemplo: ¿los costos de la migración, la complejidad de realizar un inventario de todos los sistemas criptográficos que usa una organización, la posible falta de personal con la capacitación adecuada, la resistencia al cambio dentro de la organización, o la necesidad de coordinar estos cambios con terceras partes?)

* ¿Cómo cree usted que estos desafíos, tanto técnicos como operativos, podrían variar entre diferentes tipos de organizaciones aquí en Argentina?

4. Pautas y Estrategias para la Transición:

* ¿Qué pasos o estrategias considera que serían esenciales para que una organización en Argentina pueda planificar y ejecutar de manera exitosa una migración hacia una criptografía resistente a los avances cuánticos, utilizando como referencia un algoritmo como CRYSTALS-Kyber?

* En este proceso de transición, ¿qué rol considera que deberían jugar los proveedores de tecnología, las entidades gubernamentales y el sector académico? * Si tuviera que darle algunas recomendaciones a una organización que recién está comenzando a considerar la necesidad de esta transición criptográfica, ¿cuáles serían? * ¿Qué opina sobre los enfoques híbridos durante el período de transición, es decir, la idea de combinar

temporalmente la criptografía clásica que se usa hoy con la nueva criptografía post-cuántica?

5. Visión a Futuro:

* ¿Cómo imagina usted el panorama de la criptografía en Argentina durante los próximos 5 a 10 años, especialmente en lo que respecta a la adopción de esta criptografía resistente a las computadoras cuánticas?

II Estructura de consentimiento informado

Estimado/a Profesional,

Le invito cordialmente a participar en una entrevista como parte de la investigación para mi Trabajo Final de Grado (TFG) detallado arriba. El objetivo principal de este estudio es realizar un análisis comparativo entre el algoritmo criptográfico clásico RSA-2048 y el nuevo estándar post-cuántico CRYSTALS-Kyber. Su participación se centrará en recabar su valiosa perspectiva experta sobre la eficiencia, robustez criptográfica, los desafíos prácticos para la implementación y adopción de estos sistemas, y las estrategias para una migración segura hacia la criptografía post-cuántica.

1. Propósito de la Investigación: Esta investigación busca evaluar la viabilidad técnica, operativa y de seguridad de la sustitución de RSA-2048 por CRYSTALS-Kyber en el contexto de la amenaza cuántica. Se analizará su eficiencia computacional, robustez frente a ataques y los desafíos prácticos de adopción, incorporando perspectivas de

expertos como usted para fundamentar estrategias y facilitar una migración segura y efectiva.

2. Naturaleza de su Participación: Si decide participar, se le solicitará:

- Conceder una entrevista semi-estructurada que será conducida por el investigador principal.
- La entrevista abordará temas como: su percepción de la amenaza cuántica, su conocimiento y evaluación de CRYSTALS-Kyber, los desafíos técnicos y operativos para la implementación y adopción de criptografía post-cuántica en su ámbito/contexto argentino, y sus recomendaciones o pautas para la transición.
- Con su permiso explícito, la entrevista será grabada en audio únicamente con el propósito de asegurar la fidelidad de la transcripción de sus respuestas y para el análisis posterior por parte del investigador. Estas grabaciones serán tratadas con estricta confidencialidad.

3. Participación Voluntaria y Derecho a Retirarse: Su participación en esta investigación es completamente voluntaria. Usted tiene el derecho de negarse a participar o de retirar su consentimiento y abandonar la entrevista en cualquier momento, sin necesidad de dar explicaciones y sin que esto implique ninguna consecuencia negativa para usted. Asimismo, puede optar por no responder a alguna pregunta específica si así lo desea.

4. Confidencialidad y Anonimato: Se tomarán todas las medidas necesarias para proteger su identidad y la confidencialidad de la información que proporcione.

- En el Trabajo Final de Grado y en cualquier publicación o presentación académica derivada de esta investigación, sus respuestas serán anonimizadas. No se utilizará su nombre ni ningún otro dato identificatorio directo.
- Se podrán utilizar citas directas de sus respuestas para ilustrar los hallazgos, pero estas serán atribuidas de forma anónima (ej: "Experto del sector financiero", "Participante 1") o con un pseudónimo acordado si usted lo prefiere.
- Las grabaciones de audio y las transcripciones serán almacenadas de forma segura por el investigador principal y solo él tendrá acceso a ellas. Serán destruidas una vez finalizado el período de evaluación del TFG (o según las normativas institucionales, ej: 5 años).

5. Riesgos y Beneficios:

- Riesgos: No se prevén riesgos significativos asociados a su participación, más allá del tiempo dedicado a la entrevista.
- Beneficios: Si bien no recibirá una compensación económica ni beneficios directos por participar, su contribución será de gran valor para generar conocimiento en un área emergente y crítica como es la criptografía post-cuántica. Los resultados de la investigación podrían ayudar a informar a otras organizaciones y profesionales sobre los desafíos y estrategias de migración.

6. Uso de la Información: La información recopilada se utilizará exclusivamente para los fines de este Trabajo Final de Grado y, potencialmente, para futuras publicaciones académicas o presentaciones científicas derivadas del mismo, siempre manteniendo el anonimato y la confidencialidad de los participantes.

7. Preguntas: Si tiene alguna pregunta sobre esta investigación o sobre su participación, puede contactar al investigador principal (Pedro Bazán) utilizando los datos de contacto provistos al inicio de este documento, antes, durante o después de la entrevista.

III Estructura de entrevista a analistas, licenciados y estudiantes avanzados de Siglo XXI

1. ¿Cuán real o inminente consideras la amenaza de la computación cuántica para la criptografía que usamos hoy en día? ¿Es algo que te preocupa como futuro profesional?

2. Durante tu formación académica, ¿qué has aprendido sobre la Criptografía Post-Cuántica (PQC)? ¿Has oído hablar de algoritmos como CRYSTALS-Kyber? ¿Sientes que la universidad te está preparando para este cambio tecnológico?

3. Desde tu punto de vista como estudiante/futuro profesional, ¿cuáles te imaginas que serán los mayores desafíos al momento de que las empresas argentinas tengan que migrar a PQC? ¿Te imaginas problemas más bien técnicos (de programación, rendimiento, etc.) u organizacionales (de costos, falta de gente capacitada, resistencia al cambio, etc.)?

4. Pensando a futuro, ¿quién crees que debería liderar esta transición en Argentina? ¿El gobierno (estableciendo normas), las propias empresas (invirtiendo y adaptándose), o las universidades (formando a la gente)?