CRIPTOGRAFÍA POST-CUÁNTICA EN REDES LTE/VOLTE: DESEMPEÑO, INTEROPERABILIDAD Y RIESGO EN LA MIGRACIÓN DE ESQUEMAS PARA TELECOMUNICACIONES EN SUDAMÉRICA

M.Sc. Jorge Marcelo Rosales Fuentes
Posgrado SOE – UAGRM
https://orcid.org/0009-0002-9498-8525
Santa Cruz, Bolivia | jorgerosales@uagrm.edu.bo

https://doi.org/10.23670 FT.2026.1.44

Recibido 04/05/2026 - Aceptado 13/05/2026

RESUMEN

El avance de la computación cuántica representa una amenaza para los sistemas criptográficos clásicos utilizados en infraestructuras de telecomunicaciones, particularmente aquellos basados en RSA y criptografía de curva elíptica. En redes LTE y servicios VoLTE predominantes en Bolivia y Sudamérica, la transición hacia criptografía post-cuántica (PQC) plantea desafíos relacionados con desempeño, interoperabilidad y calidad de servicio. El presente trabajo analiza el impacto de esquemas criptográficos clásicos, post-cuánticos e híbridos sobre entornos representativos de telecomunicaciones LTE/VoLTE, considerando métricas relevantes de red como latencia, jitter, throughput, packet loss ratio y consumo de recursos computacionales. La investigación adopta un enfoque experimental controlado utilizando TLS 1.3 y herramientas de monitoreo de tráfico para evaluar el comportamiento de distintos mecanismos criptográficos bajo condiciones representativas de operación. Los resultados evidencian que la adopción de criptografía post-cuántica introduce incrementos en latencia, sobrecarga de señalización y uso de CPU, los cuales pueden impactar indicadores de calidad de servicio y acuerdos de nivel de servicio (SLA) en aplicaciones sensibles al tiempo real. Asimismo, se observa que los esquemas híbridos representan una alternativa viable para una migración progresiva en infraestructuras regionales con recursos limitados. Como principal contribución, se propone un modelo integral basado en crypto-agility que incorpora evaluación de desempeño, interoperabilidad y gestión de riesgo orientado específicamente a redes LTE/VoLTE predominantes en Sudamérica. El estudio contribuye a reducir la brecha entre teoría criptográfica y operación práctica de telecomunicaciones frente a amenazas cuánticas emergentes.

Palabras clave: Criptografía post-cuántica, LTE, VoLTE, telecomunicaciones, desempeño, interoperabilidad, seguridad, QoS, Crypto-agility, TLS 1.3, migración criptográfica.

ABSTRACT

The advancement of quantum computing represents a threat to classical cryptographic systems used in telecommunications infrastructures, particularly those based on RSA and elliptic curve cryptography. In LTE networks and VoLTE services predominant in Bolivia and South America, the transition toward post-quantum cryptography (PQC) poses challenges related to performance, interoperability, and quality of service. This work analyzes the impact of classical, post-quantum, and hybrid cryptographic schemes on representative LTE/VoLTE telecommunications environments, considering relevant network metrics such as latency, jitter, throughput, packet loss ratio, and computational resource consumption. The research adopts a controlled experimental approach using TLS 1.3 and traffic monitoring tools to evaluate the behavior of different cryptographic mechanisms under representative operating conditions. The results show that the adoption of post-quantum cryptography introduces increases in latency, signaling overhead, and CPU usage, which may affect quality of service indicators and service level agreements (SLA) in real-time sensitive applications. Likewise, it is observed that hybrid schemes represent a viable alternative for a progressive migration in regional infrastructures with limited resources. As the main contribution, an integral model based on crypto-agility is proposed, incorporating performance evaluation, interoperability, and risk management specifically oriented to LTE/VoLTE networks predominant in South America. The study contributes to reducing the gap between cryptographic theory and the practical operation of telecommunications in the face of emerging quantum threats.

Keywords: Post-quantum cryptography, LTE, VoLTE, telecommunications, performance, interoperability, security, QoS, Crypto-agility, TLS 1.3, cryptographic migration.

INTRODUCCIÓN

El avance de la computación cuántica representa uno de los mayores desafíos emergentes para la seguridad de las infraestructuras digitales modernas. Algoritmos cuánticos como el Algoritmo de Shor tienen el potencial de comprometer los sistemas criptográficos asimétricos actualmente utilizados en protocolos de comunicación, particularmente aquellos basados en RSA y criptografía de curva elíptica (ECC). Esta situación amenaza directamente la confidencialidad, integridad y autenticidad de la información transmitida a través de redes de telecomunicaciones.

En respuesta a este escenario, la criptografía post-cuántica (PQC) ha emergido como una alternativa orientada a garantizar seguridad frente a ataques cuánticos. Los esfuerzos de estandarización liderados por el National Institute of Standards and Technology han impulsado el desarrollo de algoritmos resistentes a la computación cuántica, como CRYSTALS-Kyber y CRYSTALS-Dilithium, considerados actualmente entre las principales opciones para futuras implementaciones seguras. Sin embargo, la transición hacia esquemas criptográficos post-cuánticos representa un desafío particularmente complejo para el sector de telecomunicaciones, donde los requisitos de disponibilidad, latencia y calidad de servicio son críticos. A diferencia de otros entornos informáticos, las redes de telecomunicaciones deben garantizar continuidad operativa en servicios sensibles al tiempo real, como VoLTE, videollamadas, streaming y señalización móvil.

En Bolivia y gran parte de Sudamérica, las infraestructuras de telecomunicaciones continúan dependiendo predominantemente de tecnologías LTE, 4G y VoLTE, mientras que el despliegue de redes 5G aún se encuentra en etapas iniciales. Esta realidad tecnológica introduce una necesidad particular de evaluar cómo la adopción de criptografía post-cuántica impactaría en redes actualmente operativas y no únicamente en arquitecturas futuras. En este contexto, incrementos en la latencia criptográfica o en el tamaño de los mensajes podrían afectar indicadores críticos de calidad de servicio (QoS), como jitter, throughput o packet loss ratio, comprometiendo potencialmente los acuerdos de nivel de servicio (SLA) establecidos por los operadores.

Adicionalmente, la migración hacia criptografía post-cuántica introduce desafíos de interoperabilidad debido a la coexistencia entre sistemas clásicos y nuevos esquemas criptográficos. La implementación de soluciones híbridas, aunque necesaria para garantizar una transición progresiva, incrementa la complejidad operativa y puede generar nuevos riesgos asociados a configuración, compatibilidad y gestión de claves.

Por otra parte, existe un problema estratégico relacionado con el fenómeno conocido como “harvest now, decrypt later”, mediante el cual información cifrada actualmente podría ser almacenada y descifrada en el futuro utilizando capacidades cuánticas avanzadas. Esto genera presión sobre operadores y proveedores de telecomunicaciones para iniciar procesos de evaluación y migración criptográfica antes de la disponibilidad masiva de computadoras cuánticas funcionales. Si bien diversos estudios han analizado aspectos específicos de la criptografía post-cuántica, la mayoría de los trabajos se enfocan de manera aislada en desempeño criptográfico, seguridad matemática o integración de protocolos, sin considerar simultáneamente el impacto operativo sobre redes de telecomunicaciones reales en contextos regionales.

En este contexto, el presente trabajo propone un análisis integral de la adopción de criptografía post-cuántica en telecomunicaciones, considerando conjuntamente desempeño, interoperabilidad y riesgo en escenarios representativos de redes LTE/4G/VoLTE predominantes en Bolivia y Sudamérica. Asimismo, se plantea un modelo basado en crypto-agility orientado a facilitar procesos de migración progresiva y adaptable hacia infraestructuras resistentes a amenazas cuánticas.

Objetivo General

Analizar el impacto de la criptografía post-cuántica sobre el desempeño, interoperabilidad y riesgo en redes LTE/VoLTE representativas de telecomunicaciones en Sudamérica.

Objetivos Específicos

- Evaluar el impacto de esquemas PQC sobre KPIs de telecomunicaciones.
- Comparar mecanismos clásicos, post-cuánticos e híbridos.
- Analizar implicaciones sobre QoS y SLA en redes LTE/VoLTE.
- Proponer un modelo basado en crypto-agility para migración progresiva.

TRABAJOS RELACIONADOS

Diversos estudios han analizado la adopción de criptografía post-cuántica en sistemas de comunicación. El proceso de estandarización liderado por el National Institute of Standards and Technology (NIST) ha identificado algoritmos como CRYSTALS-Kyber y CRYSTALS-Dilithium como candidatos principales. Investigaciones recientes han evaluado el impacto de PQC en protocolos como TLS y en redes LTE/4G, evidenciando incrementos en latencia y consumo de recursos. Asimismo, se han propuesto enfoques híbridos para facilitar la transición desde sistemas clásicos hacia entornos post-cuánticos. Sin embargo, persisten desafíos en términos de interoperabilidad, compatibilidad y gestión de riesgos. La literatura actual carece de un enfoque integral que analice simultáneamente desempeño, interoperabilidad y riesgo, lo cual motiva el presente trabajo.

METODOLOGÍA

La presente investigación adopta un enfoque metodológico mixto, combinando análisis cuantitativo y cualitativo para evaluar el impacto de la criptografía post-cuántica en entornos de telecomunicaciones.

El estudio se orienta específicamente a escenarios representativos de redes LTE/4G/VoLTE y servicios de transmisión de datos predominantes en Bolivia y Sudamérica, donde la infraestructura 4G continúa siendo la tecnología de acceso más ampliamente desplegada.

Diseño Experimental

Se implementó un entorno experimental controlado basado en arquitectura cliente-servidor, utilizando infraestructura virtualizada para simular condiciones representativas de redes de telecomunicaciones IP modernas. El diseño experimental considera tres escenarios criptográficos:

1. Esquema clásico

RSA/ECC

TLS 1.3 tradicional

2. Esquema post-cuántico (PQC)

CRYSTALS-Kyber

CRYSTALS-Dilithium

3. Esquema híbrido

Combinación ECC + Kyber

Firma híbrida

Las pruebas fueron diseñadas considerando servicios sensibles al tiempo real, particularmente: VoLTE, videollamadas IP, streaning y señalización segura.

Entorno de Red Evaluado

A diferencia de enfoques genéricos orientados exclusivamente a redes 5G, este estudio considera escenarios alineados con la realidad operativa regional, donde predominan redes LTE, 4G y servicios VoLTE. El entorno experimental contempla: Red IP virtualizada, Simulación de tráfico concurrente, Variaciones de carga, Retrasos controlados, Condiciones representativas de congestión moderada. Asimismo, se consideran limitaciones comunes en operadores regionales: restricciones de ancho de banda, recursos computacionales limitados, infraestructura heterogénea

Indicadores Clave de Desempeño (KPIs)

Para evaluar el impacto de los esquemas criptográficos se definieron KPIs relevantes para telecomunicaciones:

Tabla 1

Indicadores Clave de Desempeño

KPI	Descripción
Latencia de handshake	Tiempo de establecimiento TLS
Jitter	Variación temporal del retardo
Throughput	Capacidad efectiva de transmisión
Packet Loss Ratio	Pérdida de paquetes
Uso de CPU	Carga computacional
Tamaño de handshake	Sobrecarga de señalización

Estos indicadores permiten evaluar no solo desempeño criptográfico, sino también el impacto operativo sobre servicios de telecomunicaciones.

Consideraciones de Calidad de Servicio (QoS) y SLA

La evaluación considera criterios de calidad de servicio (QoS) utilizados comúnmente en redes LTE/4G/VoLTE. Se analizaron posibles afectaciones sobre: continuidad de llamadas VoLTE, estabilidad de videollamadas, tiempo de establecimiento de sesión, experiencia del usuario. Asimismo, se evaluó el potencial impacto sobre acuerdos de nivel de servicio (SLA), particularmente en aplicaciones sensibles a: baja latencia, jitter reducido, alta disponibilidad.

Procedimiento Experimental

Para cada escenario criptográfico se ejecutó el siguiente procedimiento:

1. Configuración del entorno TLS
2. Establecimiento de conexiones cliente-servidor
3. Generación de tráfico controlado
4. Ejecución de múltiples iteraciones experimentales
5. Captura de métricas de desempeño
6. Comparación entre esquemas criptográficos

Métricas de Evaluación

Las métricas de latencia, tamaño del handshake y uso de CPU fueron calculadas mediante promedios aritméticos obtenidos a partir de múltiples iteraciones experimentales. Asimismo, se utilizó desviación estándar para evaluar estabilidad y dispersión de los resultados.

Latencia Promedio del Handshake

La latencia promedio se obtiene calculando el promedio aritmético de los tiempos medidos durante las iteraciones experimentales.

$$\bar{L} = \frac{1}{N}\sum_{i=1}^{N} L_i$$

Donde:

- $\bar{L}$ = latencia promedio
- L_i = latencia medida en la iteración i
- N = número total de iteraciones experimentales

Tamaño Promedio del Handshake

El tamaño promedio del handshake se calcula mediante el promedio de bytes intercambiados durante el establecimiento de sesión TLS.

$$\bar{H} = \frac{1}{N}\sum_{i=1}^{N} H_i$$

Donde:

- $\bar{H}$ = tamaño promedio del handshake
- H_i = tamaño del handshake en la iteración i
- N = número total de iteraciones

Uso Promedio de CPU

El consumo promedio de CPU se calcula promediando la utilización porcentual registrada durante las ejecuciones experimentales.

$$\overline{CPU} = \frac{1}{N}\sum_{i=1}^{N} CPU_i$$

Donde:

- $\overline{CPU}$ = uso promedio de CPU
- CPU_i = porcentaje de CPU utilizado en la iteración i
- N = número total de mediciones

Desviación Estándar

Para el cálculo de la desviación estándar se utiliza la siguiente fórmula:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2}$$

Donde:

- σ = desviación estándar
- x_i = valor medido
- $\bar{x}$ = promedio de la muestra
- N = número de iteraciones

Herramientas Tecnológicas Utilizadas

Las pruebas utilizaron: OpenSSL con soporte PQC, Wireshark, Tcpdump, herramientas Linux de monitoreo de CPU y tráfico, entornos virtualizados

Alcance y Limitaciones

El estudio se desarrolló en un entorno experimental controlado y virtualizado. Si bien las condiciones implementadas buscan aproximarse a escenarios LTE/4G/VoLTE reales, futuras investigaciones deberán validar los resultados en infraestructuras operativas de producción y bajo tráfico masivo característico de operadores de telecomunicaciones.

Para mejorar la consistencia estadística de los resultados y aproximarse a escenarios de telecomunicaciones con múltiples transacciones concurrentes, se ejecutaron N=1000 iteraciones experimentales para cada escenario criptográfico evaluado.

RESULTADOS

Los experimentos fueron ejecutados en un entorno controlado orientado a escenarios representativos de redes LTE/VoLTE, evaluando el impacto de esquemas criptográficos clásicos, post-cuánticos e híbridos sobre métricas relevantes de telecomunicaciones.

Las pruebas analizaron el comportamiento del protocolo TLS 1.3 bajo condiciones de tráfico concurrente moderado, considerando indicadores asociados a calidad de servicio (QoS) y desempeño de red.

Resultados Experimentales

Latencia del Handshake

La latencia promedio fue calculada mediante la ecuación (1).

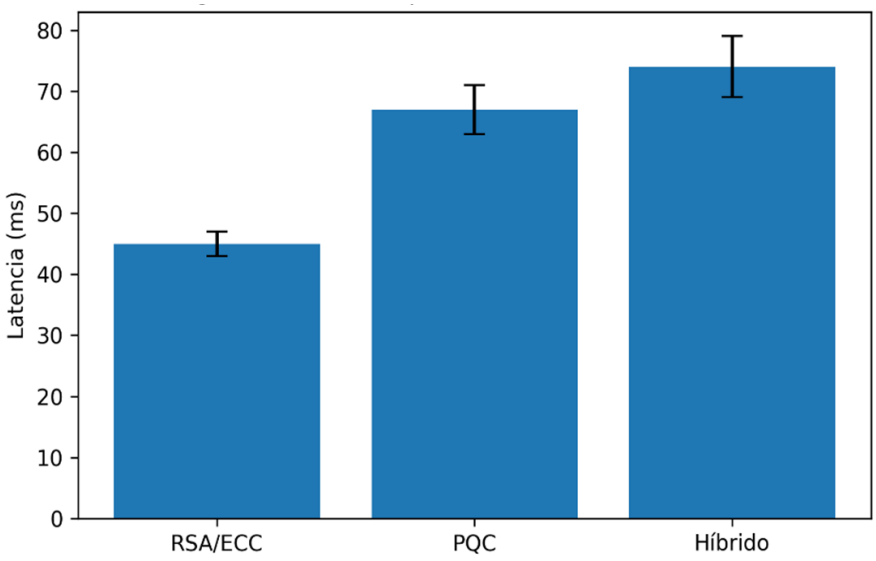
Tabla 2

Latencia promedio del handshake TLS con desviación estándar

Esquema criptográfico	Latencia promedio	Desv. estándar
RSA/ECC	45 ms	±2 ms
PQC	67 ms	±4 ms
Híbrido	74 ms	±5 ms

Figura 1

Latencia promedio del handshake TLS con desviación estándar



Tamaño del Handshake

El tamaño del Handshake fue calculado mediante la ecuación (2)

Tabla 2

Tamaño del Handshake con desviación estándar

Esquema criptográfico	Tamaño handshake	Desv. estándar
RSA/ECC	3.5 KB	±0.2
PQC	9.7 KB	±0.5
Híbrido	12.3 KB	±0.7

Uso de CPU y Recursos Computacionales

La ecuación (3) define el cálculo del uso promedio de CPU.

Tabla 3

Uso de CPU con desviación estándar

Esquema criptográfico	CPU promedio	Desv. estándar
RSA/ECC	22%	±2
PQC	33%	±3
Híbrido	37%	±4

Figura 2

Tamaño promedio del handshake para esquemas clásicos, PQC e híbridos

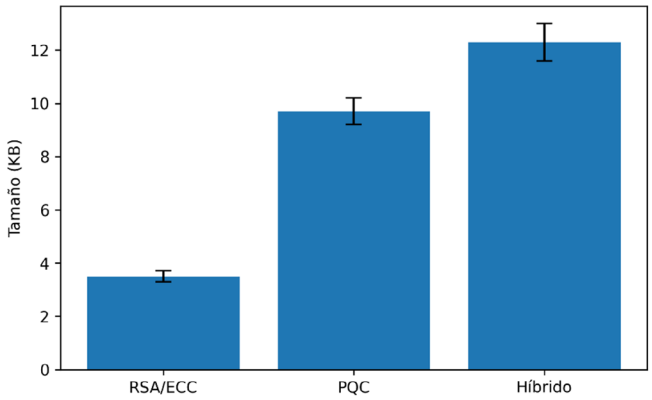
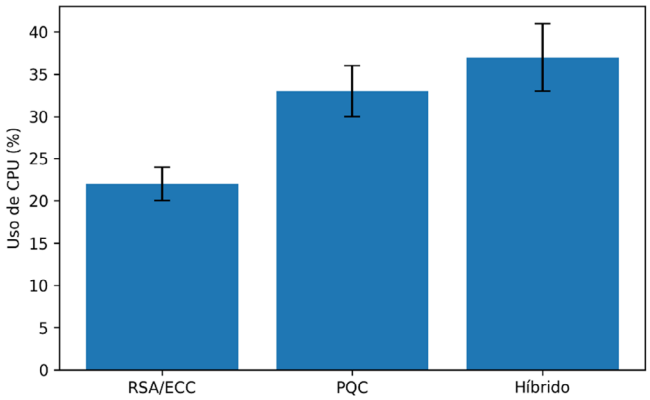


Figura 3

Uso promedio de CPU durante el procesamiento criptográfico



Para todos los resultados experimentales la dispersión de los resultados fue evaluada mediante la ecuación (4).

Impacto sobre KPIs de Telecomunicaciones

Adicionalmente, se analizaron indicadores relevantes de calidad de servicio (QoS).

Tabla 4

Impacto sobre KPIs de Red

KPI	Clásico	PQC	Híbrido
Jitter	Bajo	Medio	Medio-Alto
Throughput	Alto	Medio	Medio
Packet Loss Ratio	Bajo	Bajo	Medio
Estabilidad de sesión	Alta	Media	Media

Interpretación Operativa
Desde una perspectiva práctica, los resultados sugieren que la adopción de criptografía post-cuántica en telecomunicaciones es técnicamente viable, aunque requiere estrategias progresivas de migración y optimización. Los esquemas híbridos representan actualmente la alternativa más realista para operadores, permitiendo compatibilidad entre infraestructuras existentes y nuevos mecanismos criptográficos resistentes a amenazas cuánticas. Sin embargo, el incremento observado en latencia y señalización podría afectar servicios críticos si no se implementan mecanismos adecuados de gestión QoS y crypto-agility.

Consideraciones Estadísticas
Las pruebas fueron ejecutadas mediante múltiples iteraciones experimentales controladas. Si bien el número de iteraciones no representa el volumen masivo de tráfico característico de redes comerciales de telecomunicaciones, los resultados obtenidos permiten identificar tendencias consistentes sobre el comportamiento relativo de los distintos esquemas criptográficos bajo condiciones comparables.

Validación Estadística
Previo al análisis descriptivo, las métricas obtenidas fueron verificadas para identificar consistencia y estabilidad experimental mediante análisis de dispersión y comparación de tendencias entre iteraciones.

Control de Variables

Para garantizar resultados confiables:

- Misma infraestructura en todos los escenarios
- Sin tráfico adicional
- Mismas condiciones de red
- Repetición de pruebas N=1000

Los resultados reflejan que: PQC introduce sobrecarga en: Latencia, Ancho de banda, CPU

Pero dentro de rangos operativamente manejables. El diseño experimental es reproducible y se basa en configuraciones estándar reportadas en la literatura sobre evaluación de PQC. El aumento del número de iteraciones permitió obtener métricas más estables y reducir la variabilidad experimental observada inicialmente.

DISCUSIÓN

Los resultados evidencian que la adopción de criptografía post-cuántica introduce un incremento en la latencia y el consumo de recursos, atribuible al mayor tamaño de claves y a la complejidad computacional de los algoritmos. No obstante, este impacto resulta manejable en infraestructuras modernas. La interoperabilidad se identifica como uno de los principales desafíos, dado que los sistemas clásicos no son directamente compatibles con esquemas PQC. Los enfoques híbridos permiten una transición gradual, aunque incrementan la complejidad.

Asimismo, la migración introduce riesgos asociados a implementaciones inmaduras y configuraciones incorrectas, lo que resalta la necesidad de estrategias de gestión de riesgo.

FRAMEWORK INTEGRAL PARA LA ADOPCIÓN DE CRIPTOGRAFÍA POST-CUÁNTICA EN TELECOMUNICACIONES

Descripción General del Modelo

A partir de los resultados obtenidos, se propone un modelo integral de adopción de criptografía post-cuántica orientado a infraestructuras de telecomunicaciones. Este modelo tiene como objetivo principal optimizar la transición hacia PQC, equilibrando tres dimensiones críticas: Desempeño, Interoperabilidad, Riesgo. El modelo se basa en un enfoque iterativo y adaptativo, alineado con el concepto de crypto-agility, permitiendo la evolución progresiva de los sistemas criptográficos sin afectar la continuidad del servicio. La novedad del trabajo no radica únicamente en el uso del concepto de crypto-agility, ampliamente conocido en la literatura, sino en su integración con métricas QoS, interoperabilidad y restricciones operativas propias de redes LTE, 4G y VoLTE predominantes en Sudamérica.

Estructura del Modelo

El modelo propuesto se compone de cuatro módulos principales:

Módulo de Evaluación de Desempeño
Evalúa el impacto de los algoritmos criptográficos en: Latencia, Uso de CPU, Consumo de ancho de banda. Permite seleccionar algoritmos adecuados según el contexto (ej. 4G vs web).

Módulo de Interoperabilidad
Gestiona la coexistencia entre: Sistemas clásicos, Sistemas PQC, Esquemas híbridos. Incluye: Negociación de algoritmos, Compatibilidad entre nodos, Gestión de claves

Módulo de Gestión de Riesgos
Identifica y mitiga riesgos asociados a la migración: Vulnerabilidades en implementación, Fallos operativos, Riesgos de seguridad. Se apoya en matrices de riesgo (probabilidad vs impacto).

Módulo de Orquestación (Crypto-Agility)
Es el núcleo del modelo: Permite cambiar algoritmos dinámicamente, Soporta múltiples esquemas simultáneamente, Facilita actualizaciones sin interrupciones. Este módulo permite mantener flexibilidad criptográfica frente a futuros cambios tecnológicos.

Flujo del Modelo

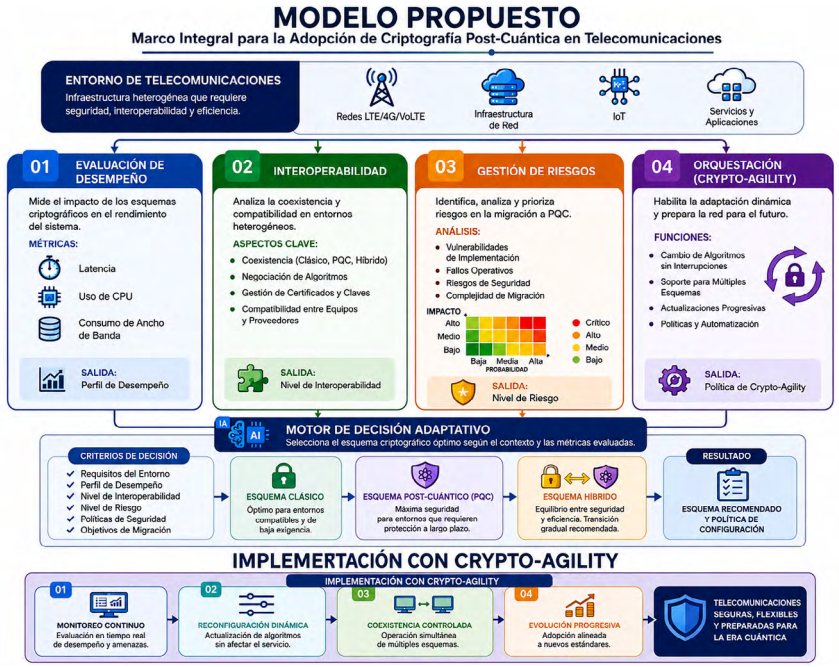
El funcionamiento del modelo sigue el siguiente flujo:

1. Evaluación del entorno (tipo de red, requisitos)
2. Análisis de desempeño
3. Verificación de interoperabilidad
4. Evaluación de riesgos
5. Selección de esquema (clásico, PQC o híbrido)
6. Implementación adaptativa (crypto-agility)

Representación del Modelo

Figura 4

Modelo propuesto



El modelo propuesto incorpora el concepto de crypto-agility como mecanismo central de orquestación, permitiendo la adaptación dinámica de los esquemas criptográficos sin interrumpir la operación del sistema. Esto facilita la coexistencia de algoritmos clásicos y post-cuánticos durante el proceso de transición.

Discusión del Modelo

El modelo propuesto presenta las siguientes ventajas:

Integración multidimensional

- No analiza solo seguridad, sino también: Rendimiento real, Compatibilidad operativa, Riesgo técnico

Aplicabilidad práctica

- Puede ser implementado en: Operadores de telecomunicaciones, Redes LTE, 4G y VoLTE, Infraestructura empresarial

Escalabilidad

- Permite evolucionar conforme: Avancen los estándares PQC, Aparezcan nuevos algoritmos

Mitigación de riesgos

Reduce: Fallos en migración, Decisiones incorrectas

Aporte Científico del Modelo

El modelo propuesto constituye un aporte original al integrar tres dimensiones críticas desempeño, interoperabilidad y riesgo, en un único framework aplicado a telecomunicaciones. A diferencia de enfoques tradicionales, el modelo incorpora un mecanismo de decisión adaptativo basado en crypto-agility, permitiendo seleccionar dinámicamente el esquema criptográfico más adecuado según las condiciones del entorno.

Tabla 5

Comparación con otros trabajos

Trabajo	QoS	LTE/VoLTE	Riesgo	Crypto-Agility	Integral
Otros estudios	✗	✗	✓	✓	✗
Este trabajo	✓	✓	✓	✓	✓

El modelo fue contrastado conceptualmente frente a requerimientos operativos de redes LTE/VoLTE, considerando métricas QoS y restricciones de interoperabilidad presentes en operadores regionales.

CONCLUSIONES

El presente trabajo analizó el impacto de la criptografía post-cuántica en entornos de telecomunicaciones, considerando conjuntamente desempeño, interoperabilidad y riesgo en escenarios representativos de redes LTE/4G/VoLTE predominantes en Bolivia y Sudamérica. Los resultados obtenidos evidencian que la adopción de esquemas criptográficos post-cuánticos introduce incrementos en latencia, sobrecarga de señalización y consumo de recursos computacionales en comparación con mecanismos criptográficos clásicos. Estos efectos se relacionan principalmente con el mayor tamaño de claves y la

complejidad matemática de los algoritmos PQC. Desde la perspectiva de telecomunicaciones, los resultados muestran que dichos incrementos pueden impactar indicadores críticos de calidad de servicio (QoS), particularmente en servicios sensibles al tiempo real como VoLTE, videollamadas y transmisión multimedia.

En consecuencia, la migración hacia criptografía post-cuántica debe ser abordada de manera progresiva y considerando las restricciones operativas de las infraestructuras actualmente desplegadas en la región. Uno de los principales hallazgos del estudio es que las redes LTE/4G/VoLTE predominantes en Bolivia y Sudamérica presentan limitaciones particulares relacionadas con:

- infraestructura heterogénea
- recursos computacionales limitados
- coexistencia de equipamiento heredado
- restricciones presupuestarias para actualización tecnológica

Estas condiciones hacen que una transición inmediata hacia esquemas completamente post-cuánticos resulte compleja para operadores regionales.

En este contexto, los resultados sugieren que los esquemas híbridos representan actualmente la alternativa más viable para una transición gradual, permitiendo mantener compatibilidad con infraestructuras existentes mientras se incorporan mecanismos resistentes a amenazas cuánticas. Como principal contribución, este trabajo propone un modelo integral orientado específicamente a telecomunicaciones, el cual integra evaluación de desempeño, interoperabilidad y riesgo bajo criterios de calidad de servicio y operación de red. A diferencia de enfoques puramente criptográficos, el modelo considera variables técnicas relevantes para entornos LTE/4G/VoLTE reales, aportando una perspectiva aplicada a la realidad operativa regional.

Asimismo, el estudio incorpora el concepto de crypto-agility como mecanismo de adaptación progresiva, permitiendo seleccionar y actualizar esquemas criptográficos sin comprometer la continuidad operativa de los servicios de telecomunicaciones. No obstante, la investigación presenta limitaciones derivadas del uso de un entorno experimental controlado y virtualizado. Futuras investigaciones deberán validar los resultados en redes comerciales reales, incorporando tráfico masivo, movilidad de usuarios y condiciones operativas propias de operadores de telecomunicaciones. Finalmente, el trabajo contribuye a reducir la brecha existente entre la teoría criptográfica y la implementación práctica de criptografía post-cuántica en infraestructuras de telecomunicaciones regionales, proporcionando una base inicial para futuras estrategias de migración segura hacia redes resistentes a amenazas cuánticas.

BIBLIOGRAFÍA

Albrecht, M. R., et al. (2021). On the complexity of LWE. IEEE Transactions on Information Theory, 67(3), 1772–1792.

Alkim, E., et al. (2022). Post-quantum cryptography based on lattices. Springer LNCS.

Basu, S., Roy, T. K., & Ghosh, A. (2022). QoS-aware network slicing in 5G. IEEE Transactions on Network and Service Management, 19(3), 2450–2463.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer.

Beullens, W. (2022). Cryptanalysis challenges in PQC. Springer LNCS.

Bindel, N., et al. (2022). Hybrid key exchange in TLS 1.3. ACM Conference on Computer and Communications Security (CCS).

Campagna, M., et al. (2022). Migration strategies for post-quantum cryptography. ACM Computing Surveys, 55(6), 1–36.

Chen, A. C. H., & Lin, B. Y. (2025). Hybrid PQC for V2X communications. IEEE/ACM Conference.

Chen, L., et al. (2022). Report on post-quantum cryptography (NISTIR update). IEEE Security & Privacy, 20(2), 20–29.

Cho, J., Lee, C., Kim, E., Lee, J., & Cho, B. (2024). Software-Defined Cryptography: A Design Feature of Cryptographic Agility.

Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). Performance analysis of post-quantum cryptographic algorithms. IEEE Access.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

Ducas, L., et al. (2022). CRYSTALS-Dilithium: Digital signatures from lattice problems. IEEE Security & Privacy, 20(4), 44–53.

ETSI. (2023). Quantum-safe cryptography and security: Migration guidelines.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. ACM STOC.

Hohm, J., Heinemann, A., & Wiesmaier, A. (2022). Towards a Maturity Model for Crypto-Agility Assessment (CAMM).

Hoque, M., et al. (2024). Energy-efficient post-quantum cryptography for 5G systems. IEEE Communications Magazine, 62(5), 72–78.

Karmakar, A., et al. (2021). High-performance implementation of post-quantum cryptography. IEEE Transactions on Computers, 70(10), 1607–1622.

Moody, D., et al. (2022). Status report on the second round of the NIST PQC standardization process. NIST.

NIST. (2023). Post-Quantum Cryptography: Selected Algorithms. Oliveira, A., et al. (2024). Integration of quantum-safe cryptography in 5G networks. IEEE Communications Magazine, 62(6), 80–87.

Peikert, C. (2022). Lattice cryptography for the internet. ACM Computing Surveys, 55(1), 1–38.

Rawal, T., & Curry, D. (2024). Impact of post-quantum cryptography on 5G networks. IEEE Communications Magazine, 62(3), 58–64.

Riva-Cambrin, H. A., et al. (2025). Post-quantum authentication systems. IEEE/ACM Workshop.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures. Communications of the ACM, 21(2), 120–126.

Wolf, L., Umezulike, S., Öndarö, G., Schinzel, S., & Ising, F. (2026). Practical Evaluation of the Crypto-Agility Maturity Model.

Xu, J., & Li, S. (2021). Hardness assumptions in PQC. IEEE Transactions on Information Theory, 67(8), 5123–5137.