



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones cuánticas seguras
Hoja de ruta de adopción de tecnologías híbridas: QKD+PQC

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: José Damián Gómez Gutiérrez

DIRECTORES: Javier Vales Alonso

José María Núñez Ortuño

CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones cuánticas seguras
Hoja de ruta de adopción de tecnologías híbridas: QKD+PQC

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

La estrategia *Harvest Now, Decrypt Later* (HNDL) figura entre una de las amenazas más contumaces y silenciosas del paisaje cibernético actual (Fedorov, 2023). Está respaldada por la sólida creencia del advenimiento futuro del primer ordenador cuántico criptológicamente relevante (CRQC, por sus siglas en inglés). Este modus operandi es particularmente preocupante porque el día Q en un futuro no muy lejano, este CRQC tendrá la capacidad de implementar algoritmos actuales como el de Shor o Grover que representan un peligro existencial para la criptografía actual.

Este riesgo futuro y peligro activo ya presente, ha provocado actualmente un terremoto en el ámbito de las comunicaciones seguras. Estas, están experimentando una transformación revolucionaria impulsadas por el cambio de paradigma que supone el avance de las tecnologías cuánticas con su máximo exponente en la distribución de clave cuántica (QKD) y una evolución en la criptografía poscuántica (PQC) de la computación clásica.

Este trabajo examina en profundidad ambas, la QKD y la PQC, sus fundamentos físicos y matemáticos con comparativas de protocolos en las dos tecnologías, con un estudio pormenorizado de las mismas resaltando fortalezas, debilidades, ventajas, limitaciones y requisitos técnicos de cada una de ellas. Acomete una comparativa entre ambas tecnologías, surgiendo analíticamente la vía de la sinergia inteligente con modelos híbridos emergentes. Evalúa su viabilidad para implementación en un ámbito Institucional/Defensa con un caso de uso en una Sede-delegación con valoración de diversos escenarios: PQC, QKD e híbrido. Se justifica la decisión de la elección más eficiente según criterios y aplicaciones.

Posteriormente se proporciona una hoja de ruta y guía estratégica para la toma de decisiones en el despliegue de la solución híbrida adoptada en este entorno, como la aproximación más robusta en términos comparativos de coste, escalabilidad y facilidad de implementación para enlaces críticos, mientras se aprovecha la flexibilidad y eficiencia económica de PQC para despliegues a gran escala.

Por último, para concluir, se exploran aplicaciones presentes y futuras, así como posibles sectores de adopción, Se aventuran recomendaciones estratégicas en distintos sectores y se aporta una opinión de prospección de futuro

ABSTRACT

The *Harvest Now, Decrypt Later* (HNDL) strategy is among the most persistent and silent threats in today's cyber landscape (Fedorov, 2023). It is underpinned by the firm belief in the future advent of the first cryptologically relevant quantum computer (CRQC). This modus operandi is particularly worrying because, on Q-day in the not-too-distant future, this CRQC will have the capacity to implement current algorithms such as Shor or Grover, which represent an existential threat to current cryptography.

This future risk, and the already present active threat, has caused a seismic shift in the field of secure communications. These are undergoing a revolutionary transformation driven by the paradigm shift brought about by the advancement of quantum technologies, with its prime example being quantum key distribution (QKD) and an evolution in post-quantum cryptography (PQC) of classical computing.

This work examines both QKD and PQC in depth, exploring their physical and mathematical foundations with protocol comparisons across the two technologies. A detailed study highlights the strengths, weaknesses, advantages, limitations, and technical requirements of each. It undertakes a comparison between the two technologies, analytically revealing the path of intelligent synergy with emerging hybrid models. It evaluates their feasibility for implementation in an institutional/defense context using a use case at a headquarters/branch, assessing various scenarios: PQC, QKD, and hybrid. The decision to select the most efficient option is justified based on specific criteria and applications.

Subsequently, a roadmap and strategic guide are provided for decision-making in the deployment of the hybrid solution adopted in this environment. This approach is presented as the most robust in terms of comparative cost, scalability, and ease of implementation for critical links, while leveraging the flexibility and economic efficiency of PQC for large-scale deployments.

Finally, to conclude, current and future applications are explored, as well as potential adoption sectors. Strategic recommendations are offered in different sectors, and a future outlook is provided.

PALABRAS CLAVE

HNDL, QKD, PQC, modelos híbridos QKD+PQC, MITM

AGRADECIMIENTOS

A mi pareja, por toda su paciencia y apoyo durante el tiempo dedicado a llevar a cabo este máster durante los últimos 16 meses, y especialmente para la elaboración de este estudio.

A mis Tutores por sus acertadas aportaciones y oportunas correcciones. A todo el profesorado del Máster DIRETIC por su colaboración colateral en la visión de conjunto aportada al Trabajo Fin de Máster (TFM) que he intentado plasmar en el mismo.

A mis compañeros de trabajo, por su comprensión y soporte al permitirme dedicar algún periodo de tiempo a la redacción de este TFM, en tiempos tan desenfrenados y volubles como los que nos ha tocado lidiar.

Contenido

Contenido	1
Índice de Figuras	5
Índice de Tablas.....	6
1 Introducción y objetivos.....	7
1.1 Amenazas Cuánticas	7
1.1.1 "Harvest Now, Decrypt Later" (HNDL).....	7
1.1.2 El algoritmo de Shor	8
1.1.3 El algoritmo de Deutsch-Jozsa:	9
1.2 Fundamentos de la Seguridad Cuántica y Clásica	9
1.2.1 Desglose de los Principios Físicos de la Computación Cuántica	10
1.2.2 Diferencias clave con la Computación Clásica:	15
1.2.3 Comparativa: Computación Cuántica vs. Clásica	15
2 Marco teórico: QKD y PQC	17
2.1 Tipos de Qubit: Comparación	17
2.2 QKD	18
2.2.1 El Paradigma de la seguridad cuántica: QKD	18
2.2.2 Comparativa de protocolos QKD	20
2.2.3 Métricas de Gestión y Rendimiento QKD	21
2.2.4 Estandarización ETSI ISG-QKD (Capa Física y de Gestión)	23
2.3 PQC.....	23
2.3.1 Comparativa de Protocolos PQC	23
2.3.2 Métricas de Gestión y Rendimiento PQC.....	25
2.4 Amenazas cuánticas (Shor, Grover, HDNL) & controles de seguridad post-cuánticos (PQC, QKD)	26
2.4.1 Analogía: El ecosistema de seguridad cuántica es como un banco.	28
3 Estado del arte y evaluación tecnológica.....	29
3.1 Estado del arte aplicado de comunicaciones/criptografía	29
3.1.1 QKD.....	29
3.1.2 PQC.....	31
3.1.3 Evaluación de Propiedades Criptográficas de PQC y QKD	31
3.1.4 Eval. de Viabilidad Práctica, Escalabilidad y Despliegue en PQC y QKD.....	32
3.1.5 Casos de Uso Desplegados y Aplicabilidad Estratégica en PQC y QKD	34
3.2 Integración entre PQC y QKD	35

3.3 Síntesis comparativa y Matriz de decisión.....	38
3.4 Conclusión y Perspectiva Estratégica en PQC y QKD	40
4 Análisis de viabilidad en sectores críticos y caso de uso sede-delegación.....	42
4.1 Factores a analizar.....	42
4.1.1 Requisitos Críticos.....	42
4.1.2 Limitaciones Operacionales.....	43
4.1.3 Riesgos y Dependencias Críticas	43
4.1.4 Mitigaciones Propuestas	44
4.2 Caso de uso: Enlace Sede-Delegación	44
4.2.1 Escenario de Implementación.....	44
4.2.2 Escenario A: Solo PQC	45
4.2.3 Escenario B: Solo QKD	47
4.2.4 Escenario C: Sistema Híbrido (QKD+PQC)	49
4.2.5 Comparativa Exhaustiva de Escenarios.....	52
4.2.6 Recomendación y Justificación	52
5 Hoja de ruta	56
5.1 Objetivo.....	56
5.2 Planificación Estratégica por Fases.....	57
5.2.1 Año 1: Análisis y Diseño Fundamental (TRL 4-5)	57
5.2.2 Año 2: Implementación Piloto y pruebas (TRL 6-7).....	58
5.2.3 Año 3: Despliegue en Producción (TRL 7-8).....	59
5.2.4 Años 4-5: Consolidación y Expansión (TRL 8-9).....	60
5.3 Fuentes de Financiación.....	61
5.4 RRHH.....	62
5.4.1 Perfiles Profesionales Necesarios	62
5.4.2 Programa de Formación.....	62
5.5 Gestión Integral de Riesgos	63
5.5.1 Riesgos Técnicos de Alto Impacto	63
5.5.2 Riesgos Operacionales.....	65
5.5.3 Riesgos de Negocio	65
5.5.4 Riesgos Financieros	66
5.6 Referencias Normativas y Estándares.....	67
5.7 Métricas de Éxito e Indicadores Claves de Rendimiento (KPIs).....	68
5.7.1 Métricas Técnicas	68
5.7.2 Métricas Operacionales.....	68
5.7.3 Métricas de Seguridad	69

6 Conclusiones y valoraciones	70
6.1 Síntesis de Resultados y Contribuciones	70
6.2 Aplicaciones Presentes: Nichos de Alto Valor	71
6.2.1 Sector Defensa e Inteligencia	71
6.2.2 Sector Financiero y Sanitario.....	71
6.3 Aplicaciones Futuras: Perspectivas de Evolución	71
6.3.1 Quantum Internet y Redes Globales (2030-2035)	71
6.3.2 Integración IoT y Edge Computing (2025-2030)	72
6.4 Desafíos Tecnológicos Persistentes	72
6.4.1 Limitaciones Físicas Fundamentales	72
6.4.2 Desafíos de Ingeniería	72
6.5 Recomendaciones Estratégicas	72
6.5.1 Para Organizaciones Implementadoras.....	72
6.5.2 Para responsables de Política.....	73
6.6 Perspectiva Temporal y Hoja de Ruta Tecnológica.....	73
7 Bibliografía.....	74
7.1 Referencias utilizadas para obtener las Figuras:	80
8 Anexo I: Acrónimos	82
9 Anexo II: Paradigma MOSCA	86
9.1 Paradigma MOSCA: Riesgo Cuántico y Migración Segura	86
9.1.1 Definición del Teorema MOSCA	86
9.1.2 La Urgencia Impulsada por HNDL y el CRQC.....	87
10 Anexo III: Comparativa CC & CQ: Matemática y Física	88
11 Anexo IV: Puertas Cuánticas	89
11.1 Puertas cuánticas	89
11.2 El Fundamento Físico de la Información	89
11.2.1 Bits Clásicos y Compuertas Irreversibles	89
11.2.2 Qúbits Cuánticos y Compuertas Unitarias.....	90
11.3 Implicaciones en Criptografía y Seguridad.....	91
11.3.1 Cuadro de Compuertas Cuánticas (Uniqubit y Multiqubit).....	92
11.3.2 Información Adicional y Fundamentos	93
12 Anexo V: QRNG y Orquestador SDN	94
12.1 Integración QRNG con HSM y KSM	94
12.2 SDN-QKD. El orquestador	94
12.2.1 Arquitectura SDN-QKD	94

12.2.2 Algoritmos de Enrutamiento de Claves	95
13 Anexo VI: Los SLA en la QKD	96
13.1 Vulnerabilidades Críticas	96
13.1.1 Ataque de Cegado de Detectores (Detector Blinding):	96
13.1.2 Ataque de Caballo de Troya (Trojan Horse):	96
13.1.3 Ataque de Desplazamiento Temporal (Time-Shift):	96
13.2 Contramedidas y Seguridad por Diseño.....	96
13.2.1 Monitor de Potencia (Watchdog):	96
13.2.2 Aisladores Ópticos:.....	96
13.2.3 MDI-QKD (Measurement-Device-Independent):	96
14 Anexo VII: QKD con TN en Sede-Delegación.....	97
14.1 Presupuesto de Enlace Óptico (Link Budget)	97
14.2 Selección Tecnológica y Análisis de Rendimiento	97
14.3 Modelo de Consumo y Buffer de Claves	97
14.4 Análisis de Nodos de Confianza (Trusted Nodes)	97
15 Anexo VIII: Diagramas de Arquitectura y Secuencias de Protocolo	99
15.1 Secuencia TLS 1.3 con ML-KEM y ML-DSA	99
15.1.1 Análisis del Flujo de Mensajes:	99
15.2 Flujo QKD-KMS-IPsec (ETSI GS QKD 014).....	100
15.2.1 Diagrama de Secuencia Operativa:.....	101

Índice de Figuras

Figura 1-1. Amenaza HNDL (Adaptada de Rich DuBose)	8
Figura 1-2. Algoritmo de Shor (Adaptado de Chaitanya Ravuri)	8
Figura 1-3. Algoritmo de Grover (Adaptado de Bender2k11)	9
Figura 1-4. Algoritmo de Deutsch-Jozsa (Adaptado de Pepml)	9
Figura 1-5. Esfera de Bloch (Adaptado de Ketterer)	10
Figura 1-6. Superposición (Adaptado de Enrique Solano)	11
Figura 1-7. Potencia de cálculo exponencial (Adaptado de Mariela León)	11
Figura 1-8. Entrelazamiento (Adaptado de Danilo Zia et. Al.)	12
Figura 1-9. Principio de Incertidumbre (Adaptado de Site123)	12
Figura 1-10. Teorema de no Clonación (Adaptado de Pablo Turmero)	13
Figura 1-11. Interferencia (Adaptado de Daniel Martello)	14
Figura 1-12 Medición: Colapso de Estado (Adaptado de Francisco R. Villatoro)	14
Figura 2-1. Protocolo E91 (Adaptado de Luís Marco Cáceres Álvarez)	19
Figura 2-2. Protocolo BB84 paso a paso (Adaptado de Jeeun Lee et al.)	21
Figura 2-3. Comparativas de protocolos QKD en función de métricas	22
Figura 3-1. Comparativa de PQC vs QKD vs Híbrido en 10 Criterios Clave (Esc. 1-10)	39
Figura 4-1. Comparativa QKD vs PQC para Enlace Sede-Delegación	49
Figura 4-2. Comparativa PQC, QKD, Híbrido según métricas	55
Figura 5-1. Hoja de Ruta para Adopción de Tecnologías Cuánticas (2025-2030)	61
Figura 6-1. Cronograma de previsión de despliegue de tec. de criptografía cuántica (2025-2035)	73
Figura 12-1. SDN-QKD	95
Figura 15-1. Secuencia TLS 1.3 con ML-KEM y ML-DSA	99
Figura 15-2. Flujo QKD-KMS-IPsec (ETSI GS QKD 014)	100

Índice de Tablas

Tabla 1-1. Comparativa CC & QC	16
Tabla 2-1. Comparativa de Plataforma Física de Qubit.....	18
Tabla 2-2. Comparativa de Protocolos QKD	20
Tabla 2-3. Métricas de Gestión y Rendimiento QKD.....	22
Tabla 2-4. Comparativa de Protocolos PQC	24
Tabla 2-5. Protocolo PQC basado en Códigos.....	24
Tabla 2-6. Métricas de Gestión y Rendimiento PQC.....	26
Tabla 2-7. Amenazas cuánticas & controles de seguridad post- cuánticos	27
Tabla 3-1. Comparativa entre protocolos QKD	31
Tabla 3-2. Parámetros de rendimiento de detectores	33
Tabla 3-3. Evaluación de viabilidad entre PQC y QKD	34
Tabla 3-4. Diferencias QKD y PQC en seguridad y HNDL	36
Tabla 3-5. Complementariedad entre QKD y PQC	38
Tabla 3-6. Síntesis comparativa entre opciones: PQC, QKD, Híbrida PQC+QKD	39
Tabla 4-1. Costos de Implementación PQC	46
Tabla 4-2. Costos de Implementación QKD	48
Tabla 4-3. Costes de Implementación del Sistema Híbrido QKD+PKC	51
Tabla 4-4. Comparativa según criterios	52
Tabla 4-5. Recomendación y Justificación según Escenario	53
Tabla 4-6. Según las restricciones del Escenario Operativo	54
Tabla 5-1. Umbrales de aceptación operativa	57
Tabla 5-2. Presupuesto Quinquenal implementación QKD+ PQC.....	61
Tabla 9-1. Explicación componentes formula MOSCA	86
Tabla 10-1. Comparación Dimensional y Funcional del Bit y el Qubit	88
Tabla 11-1. Comparativa de Compuertas: Clásicas & Cuánticas	89
Tabla 11-2. Compuertas Multiqubit y Universales.....	91
Tabla 11-3. Compuertas Cuánticas (Uniqubit y Multiqubit)	93

1 INTRODUCCIÓN Y OBJETIVOS

El enfoque de este trabajo es el análisis del efecto provocado por la irrupción de la computación cuántica en las comunicaciones seguras. Primeramente, lo contextualizo, con una breve revisión de sus principios y fundamentos, así como una comparativa con la computación clásica ya firmemente asentada. Profundizaremos con las dos tecnologías que se han erigido para soslayar la amenaza cuántica HNLD en ciberseguridad: QKD y PQC.

La motivación del trabajo surgió por la posibilidad de aglutinar en un solo documento la evaluación del estado del arte, potencial, ventajas y limitaciones de ambas tecnologías. Particularizarlo para un caso de uso concreto de enlace Sede-Delegación circunscrito a un ámbito Institucional/ Defensa, sondeando los distintos escenarios de implementación. Solo QKD, solo PQC, híbrido (QKD+PQC). Para una vez comparados, en arquitectura, implementación, rendimiento, costos y evaluación de seguridad ofrecer una recomendación justificada. Para a continuación, establecer una hoja de ruta para implementar la solución más eficiente analizada, en este nicho específico a 3-5 años. Con el objetivo de que esta, sea lo más pragmática y realista posible, explorando aspectos como diseño, pruebas, presupuestos, Recursos Humanos (RRHH) necesarios, Gestión de riesgos, normativa, así como métricas de éxito.

1.1 Amenazas Cuánticas

1.1.1 "Harvest Now, Decrypt Later" (HNLD)

Las comunicaciones seguras forman parte de un área estratégica que siempre se ha visto condicionada por los avances en criptografía y, más recientemente, con más énfasis por el probable impacto de la computación cuántica. La amenaza cuántica no es ya solo un riesgo futuro, sino que se ha convertido en un peligro presente y activo. La estrategia HNLD es una muestra de ello y ejemplifica una de las amenazas más tenaces y silenciosas en el espectro cibernético actual (Mosca, 2018). Los atacantes están acumulando datos cifrados hoy con la expectativa de descifrarlos el hipotético día "Q", que es cuando los ordenadores cuánticos pronostican que alcanzarán la madurez suficiente (Fedorov, 2023) (ver Figura 1-1 al principio de la página siguiente). El horizonte temporal estimado para disponer de ordenadores cuánticos criptológicamente relevantes (CRQC) es de 10-15 años (Wang, 2025) plasmados en las hojas de ruta nacionales de países líderes (Gobierno de España, 2025; Government of Canada, 2023). Por esta razón, *datos gubernamentales críticos, secretos militares e industriales, información sensible médica (genómica) o financiera, propiedad intelectual* (Acker, 2023). *Todos ellos con una vida útil de décadas están siendo comprometidos hoy, aunque su contenido permanezca hoy por hoy temporalmente indescifrable.*



Figura 1-1. Amenaza HNDL (Adaptada de Rich DuBose) [1]

En el supuesto de lograr descifrarse esta información en ordenadores cuánticos *pondría en riesgo la seguridad de casi todo nuestro ámbito digital. Nos referimos a comunicaciones, navegación en internet, transacciones comerciales online, infraestructuras críticas, sintetizando a muchos de nuestros datos* (Acker, 2023). Se amplía información en Anexo II: Paradigma Mosca.

1.1.2 El algoritmo de Shor

Representa el peligro más grave y existencial para la criptografía de clave asimétrica que utiliza una pareja de claves pública y privada (ej. Rivest, Shamir y Adleman (RSA), Diffie- Hellman (DH), Criptografía de Curva Elíptica (ECC), Infraestructura de clave pública (PKI)) (Wiedijk, 2022). Ya que puede resolver con una eficiencia temporal razonable los problemas de factorización de grandes números en sus componentes primos y logaritmos discretos en tiempo polinómico (Sahu y Mazumdar, 2024; Shor, 1994).

Para un computador clásico, este problema se vuelve inabordable para números de cientos de dígitos, requiriendo tiempos exageradamente largos (miles o incluso millones de años). Su eficiencia radica en el uso de la transformada de Fourier cuántica para encontrar eficientemente el periodo de una función con aritmética modular. Este algoritmo utiliza como base al algoritmo de Simon que resuelve el problema del subgrupo oculto para funciones periódicas, que es la base para el algoritmo de Shor (Mattsson et al., s.f.). La implicación directa es que un CRQC podría romper una clave RSA de 2048 bits en cuestión de horas, desmantelando la seguridad de protocolos como TLS/SSL y VPN IPsec que protegen el tráfico global de internet. (Ver Figura 1-2 al pie de esta página)

Es muy eficiente en la búsqueda en bases de datos no estructuradas. Propuesto por Lov Grover, reduce un 50% la seguridad efectiva de los algoritmos de clave simétrica como el Advanced Encryption Standard (AES) y las funciones hash criptográficas (Yang et al., 2024; Grover, 1996). Aunque no los rompe por completo, obliga a duplicar la longitud de las claves para mantener un nivel de seguridad equivalente (ej. pasar de AES-128 a AES-256) (Yang et al., 2024; Akter, 2023; NIST, 2024). Esto tiene implicaciones significativas en el rendimiento y la gestión de claves en sistemas con recursos limitados. (Ver Figura 1-3 al principio de la página siguiente)

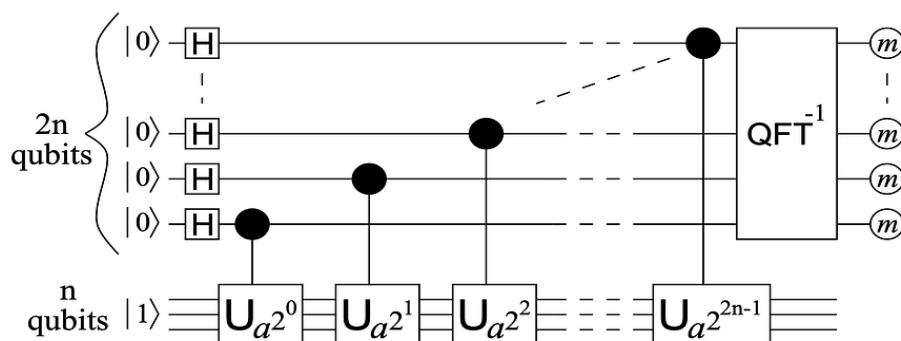


Figura 1-2. Algoritmo de Shor (Adaptado de Chaitanya Ravuri) [2]

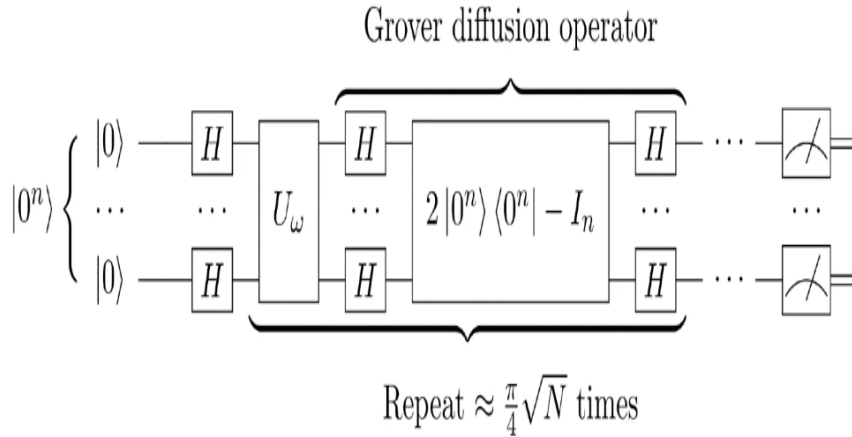


Figura 1-3. Algoritmo de Grover (Adaptado de Bender2k11) [3]

1.1.3 El algoritmo de Deutsch-Jozsa:

Su objetivo es determinar si una función binaria $f(x)$ que toma n bits de entrada y devuelve 0 o 1, es "constante" o "balanceada". Un algoritmo clásico, en el peor de los casos, necesitaría hasta $2^{(n+1)+1}$ evaluaciones de la función para determinar esto. Sin embargo, este algoritmo puede resolver este problema con una única evaluación de la función aprovechando el *paralelismo cuántico* y la *interferencia destructiva* (Paredes López et al., 2018). (Ver Figura 1-4 al pie de esta página)

La necesidad de migrar a sistemas resistentes a la cuántica está directamente impulsada por esta amenaza. Sustentado en el tiempo de vida útil requerido para la confidencialidad de datos críticos excede el tiempo estimado para el desarrollo de un ordenador cuántico operativo. Dado que la migración de sistemas criptográficos a gran escala (criptoagilidad, crypto-agility) puede tardar un tiempo comparable (10-15 años), retrasar la preparación compromete la confidencialidad futura de los datos sensibles recolectados hoy.

1.2 Fundamentos de la Seguridad Cuántica y Clásica

En primer lugar, resaltar que la amenaza que implica la computación cuántica para la orgánica criptográfica actual es razón de la necesidad de entender sus principios físicos fundamentales y compararlos con las reglas que gobiernan la computación clásica.

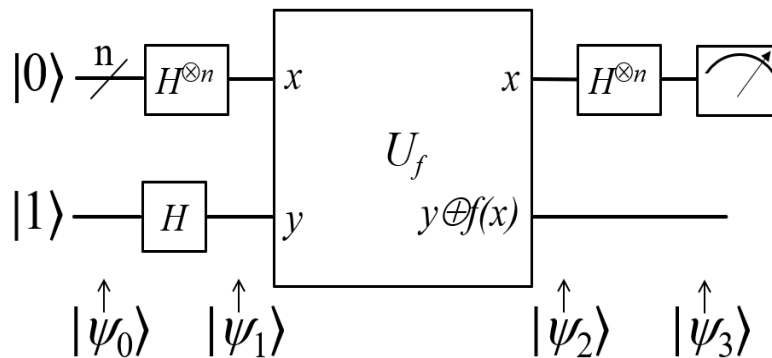


Figura 1-4. Algoritmo de Deutsch-Jozsa (Adaptado de Pepml) [4]

1.2.1 Desglose de los Principios Físicos de la Computación Cuántica

Los ordenadores cuánticos (QC) ejemplifican la próxima generación de soportes de computación. A diferencia de la tecnología clásica que se rige por la física tradicional, las tecnologías cuánticas aprovechan fenómenos cuánticos que se manifiestan en partículas subatómicas (Nielsen & Chuang, 2010). La computación cuántica se basa en el uso de las leyes de la mecánica cuántica para llevar a cabo operaciones muy complejas. Los *principios clave* que proporcionan a los ordenadores cuánticos su potencia exponencial son:

- El Bit Cuántico (*Qubit*). Es la unidad fundamental de almacenamiento e información en la computación cuántica:

Su representación, a diferencia del bit clásico (que solo puede tomar los valores discretos, el *qubit* puede estar en una superposición lineal de ambos estados $|0\rangle$ y $|1\rangle$ a la vez (Lidbjörk y Söderström Nylander, 2023). La Esfera de Bloch es una representación visual y geométrica de los estados de un solo qubit, donde un punto en la superficie de la esfera representa un estado cuántico (Ver Figura 1-5 al pie de esta página). Permite visualizar la superposición y los cambios de fase.

El soporte físico de los *qubits* puede basarse en *fotones polarizados* (luz), espines nucleares de átomos, o estados energéticos de un átomo. Por ejemplo, el giro (spin) de un electrón puede representar un '1' o un '0' o un '1' y un '0' simultáneamente. Se desarrollan tipos con más profusión en un apartado posterior analizando sus ventajas y limitaciones.

Formalmente, un *qubit* se describe como una combinación lineal compleja de los estados básicos representados por los estados $|0\rangle$ y $|1\rangle$ expresados como combinación lineal $\alpha |0\rangle + \beta |1\rangle$ con amplitudes complejas (α y β) que determinan la probabilidad de obtener cada estado al medir y donde estos coeficientes (α y β), satisfacen una condición de normalización $|\alpha|^2 + |\beta|^2 = 1$, por la reversibilidad.

- *Superposición, Paralelismo y capacidad de cálculo Cuántico:*

La *superposición* cuántica ocurre cuando un objeto posee simultáneamente dos o más valores de una cantidad observable. Gracias a esta propiedad, el ordenador cuántico puede procesar todas las opciones superpuestas simultáneamente o en un único ciclo de instrucción. Si un registro contiene n *qubits*, puede representar 2^n valores *simultáneos*. Esto permite que el ordenador cuántico analice los datos para cada resultado simultáneamente. Esta *escalabilidad es la base del paralelismo cuántico* (Yang et al., 2024; Sahu y Mazumdar, 2024). (Ver Figura 1-6 al principio de la siguiente página).

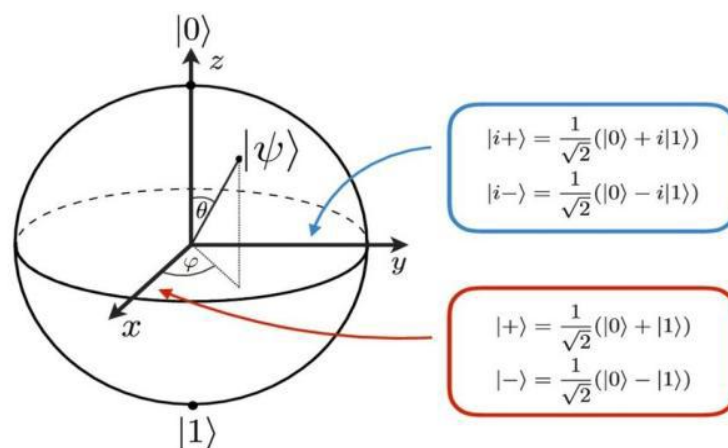


Figura 1-5. Esfera de Bloch (Adaptado de Ketterer) [5]

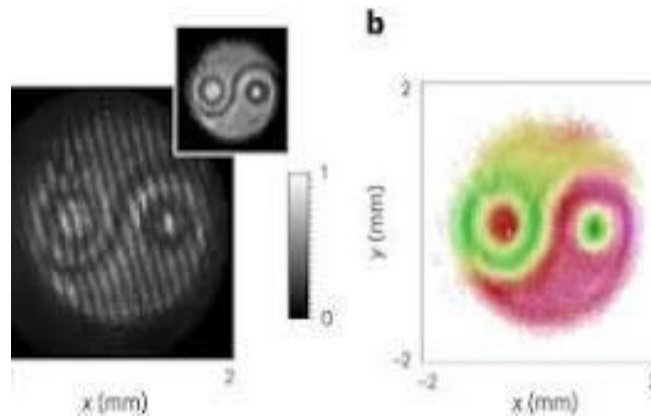


Figura 1-8. Entrelazamiento (Adaptado de Danilo Zia et. Al.) [8]

- *Monogamia* del entrelazamiento: El entrelazamiento no se puede compartir universalmente. Si dos qubits están entrelazados, no pueden compartir ese mismo entrelazamiento con otros qubits. Esto garantiza la privacidad.
- *Coordinación* máxima: Si los qubits entrelazados se miden en la misma base, no importa cuán lejos estén, los resultados de sus mediciones serán siempre los mismos (perfectamente correlacionados), lo que permite generar claves idénticas en ubicaciones remotas.

La aplicación principal del entrelazamiento cuántico incluye:

- *Criptografía cuántica*: Permite crear sistemas de comunicación más seguros, ya que cualquier intento de *escucha* en los qubits entrelazados alteraría su estado, revelando la intrusión. Esta seguridad es teóricamente *incondicional* y resistente a cualquier avance en la potencia de cómputo, ya sea clásico o cuántico. Cualquier intento de escucha es físicamente detectable. Se profundiza en este concepto con posterioridad con el Teorema de Bell y sus desigualdades. La criptografía cuántica se apoya en estos principios para garantizar la seguridad.
- *Teleportación* cuántica: Facilita la transferencia de *estados* cuánticos y *no de materia* de un lugar a otro, aunque no más rápido que la velocidad de la luz.
- *Computación* cuántica: Es un recurso clave para muchos algoritmos cuánticos que superan las capacidades de las computadoras clásicas, permitiendo operaciones que explotan las correlaciones entre qubits.
- *Principio de Incertidumbre* de Heisenberg: Cualquier intento de medir u observar un sistema cuántico alterará inevitablemente su estado. (Ver Figura 1-9 al pie de esta página)



Figura 1-9. Principio de Incertidumbre (Adaptado de Site123) [9]

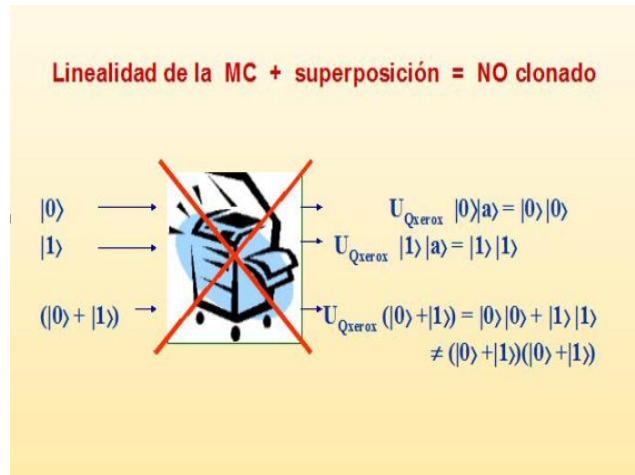


Figura 1-10. Teorema de no Clonación (Adaptado de Pablo Turmero) [10]

- **Teorema de No Clonación:** Enunciado por Wootters y Zurek en 1982, establece que es imposible que un atacante (Eve) pueda copiar un estado cuántico desconocido. En términos de seguridad, esto significa que un atacante no puede copiar los qubits que transmiten la clave para medirlos más tarde. Cualquier intento de medición perturba el estado original, introduciendo errores detectables (QBER, Quantum Bit Error Rate). (Ver Figura 1-10 al principio de esta página)
- **Interferencia y Manipulación.**

La interferencia cuántica es el mecanismo por el cual el ordenador cuántico controla y lee la superposición. Esta propiedad utiliza la naturaleza ondulatoria de los estados cuánticos para modular las amplitudes de probabilidad con:

- **Interferencia Constructiva.** Se utiliza para amplificar las amplitudes de probabilidad de las trayectorias o estados que contienen la solución correcta del problema.
- **Interferencia Destructiva.** Se utiliza para cancelar las amplitudes de probabilidad de los estados incorrectos o no deseados.

La habilidad para controlar la fase de un qubit y manipular la interferencia es la clave de la eficiencia de los algoritmos cuánticos, ya que las diferencias de fase entre los estados son las que permiten a los algoritmos *amplificar las respuestas correctas y cancelar las incorrectas*.

Los algoritmos cuánticos efectivos deben *manipular el estado de superposición para que las opciones no deseadas se eliminen mediante interferencia destructiva*, concentrando la probabilidad en la respuesta correcta antes de realizar la medición. Es decir, manipular resultados, abriendo vías más eficientes para problemas concretos. Físicamente, esta manipulación la realizo mediante las *compuertas cuánticas* son los bloques de construcción fundamentales de los circuitos cuánticos, análogos a las compuertas lógicas en la computación clásica (AND, OR, NOT). Sin embargo, operan en principios de la mecánica cuántica. (Ver Figura 1-11 al principio de la siguiente página)

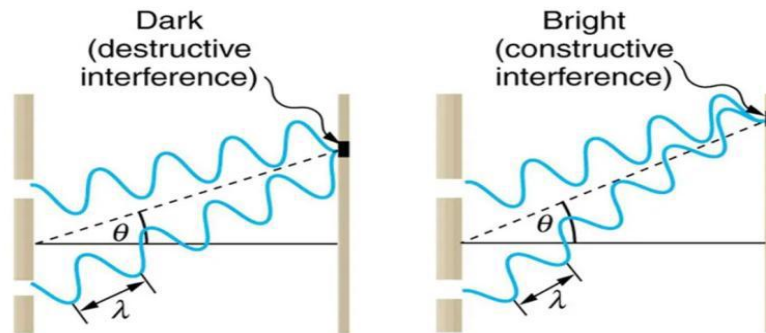


Figura 1-11. Interferencia (Adaptado de Daniel Martello) [11]

- Medición. (Rol crítico). Colapso de Estado.
 - Antes de la medición, el sistema está descrito por su función de onda en una mezcla de todos los estados posibles. Al interactuar con un aparato de medición (que se considera un sistema clásico), la función de onda sufre una *reducción abrupta no unitaria*, comúnmente denominada *colapso de la función de onda*. El sistema colapsa instantáneamente en un único estado propio, y el resultado es inherentemente probabilístico. Esta naturaleza probabilística significa que los ordenadores cuánticos son máquinas probabilistas.
 - Este proceso es irreversible, altera la entropía del sistema y es postulado por la mecánica cuántica. El hecho de que la evolución temporal de un sistema cuántico aislado sea perfectamente predecible y reversible (gobernada por las puertas unitarias) contrasta con la naturaleza no unitaria e irreversible del proceso de medición. Por lo tanto, el diseño de la arquitectura cuántica *debe maximizar el tiempo de cálculo en la fase unitaria de coherencia y relegar la fase no unitaria (el colapso) únicamente al paso final de la lectura de resultados.* (Ver Figura 1-12 al pie de esta página)

En resumen, la computación cuántica se basa en el control riguroso de tres propiedades interdependientes, la Superposición (que permite la evaluación simultánea y el paralelismo cuántico), el Entrelazamiento (que correlaciona las unidades de información) y la Interferencia (que amplifica los resultados correctos).

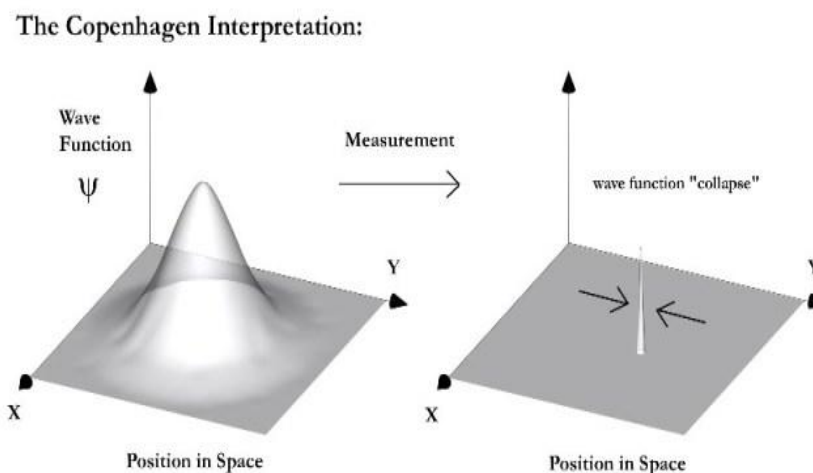


Figura 1-12 Medición: Colapso de Estado (Adaptado de Francisco R. Villatoro) [12]

1.2.2 Diferencias clave con la Computación Clásica:

- **Base de operación:** La información cuántica codificada en los qubits se procesa mediante secuencias de operaciones lógicas conocidas como puertas cuánticas. Estas puertas son el equivalente a las puertas lógicas clásicas, pero operan bajo los principios de la mecánica cuántica.
- **Reversibilidad:** Una puerta cuántica debe ser representada por una matriz unitaria. La unitariedad, $UU^\dagger=I$, asegura que la evolución del sistema sea reversible y que la probabilidad total del sistema se conserve (es decir, el estado final del qubit sigue siendo un vector de longitud unitaria en la Esfera de Bloch).
- **Naturaleza matricial:** Las compuertas cuánticas se representan como matrices unitarias (por ejemplo, las matrices de Pauli como X, Y, Z, o la compuerta de Hadamar H). La aplicación de una compuerta a un qubit se realiza mediante la multiplicación de la matriz de la compuerta por el vector de estado del qubit.
- **Tipos de compuertas cuánticas:** La hay que operan sobre *un qubit* como la de Hadamar (H) crean superposición de estados, mientras que otras como las CNOT (controlada NOT) generan entrelazamiento entre qubits. Las compuertas de fase (como Z, S, T) rotan el estado de un qubit en el plano horizontal de la esfera de Bloch, lo que es crucial para muchos algoritmos cuánticos. O bien *multiqubit* (2 o más qubits) como la CNOT, la CU (unitaria controlada) y la CZ (Z controlada), operan sobre dos o más qubits, donde un qubit de control determina si la operación se aplica al qubit objetivo. Se amplía información en Anexo IV: Puertas Cuánticas.
- **Aritmética modular:** Las compuertas cuánticas pueden usarse para realizar aritmética modular y otros cálculos complejos que son la base de algoritmos como el de Shor.

1.2.3 Comparativa: Computación Cuántica vs. Clásica

La computación clásica (CC) y la computación cuántica (QC) difieren fundamentalmente en los principios físicos que utilizan para codificar, almacenar y procesar la información. Se amplía información en Anexo III: Comparativa CC&CQ.

Aspecto	Computación Clásica (CC)	Computación Cuántica (QC)
Unidad Mínima	<i>Bit</i> (Binary Digit).	<i>Qubit</i> (Quantum Bit).
Estado	Solo puede tomar un valor <i>discreto</i> a la vez: 0 o 1.	Puede estar en una <i>superposición</i> de ambos estados (0 y 1 a la vez).
Representación Física	Basada en <i>transistores</i> que conmutan el flujo de electrones, correspondientes a los estados 'pasa' o 'no pasa' electricidad.	Basada en <i>estados</i> cuánticos de partículas subatómicas, como fotones polarizados, espines o corrientes superconductoras.
Aumento de Potencia	La potencia aumenta <i>linealmente</i> con el número de bits.	La potencia aumenta <i>exponencialmente</i> con cada <i>qubit</i> adicional.

Proceso	Ejecuta operaciones <i>secuencialmente</i> ; procesa cada elemento de una base de datos individualmente antes de combinarlos.	Trabaja en <i>paralelo</i> cuántico, procesando todas las opciones superpuestas simultáneamente.
Velocidad	Las operaciones complejas <i>tardan</i> cientos o miles de años.	<i>Reduce</i> el tiempo de procesamiento de años a segundos o microsegundos en problemas complejos.
Algoritmos	Limitada por <i>la complejidad</i> computacional. Problemas NP-completos siguen siendo difíciles.	Ofrece <i>ventaja</i> exponencial para ciertos problemas (ej. factorización con el algoritmo de Shor, búsqueda con Grover).
Medición	Las magnitudes físicas pueden medirse con precisión sin alterar el sistema (lectura no destructiva). <i>Determinista</i>	El acto de medición provoca que los estados <i>probabilísticos</i> colapsen (destructiva) y el sistema pase a comportarse como un sistema clásico (<i>decoherencia</i>).

Tabla 1-1. Comparativa CC & QC (Adaptación de NTB LM)

2 MARCO TEÓRICO: QKD Y PQC

Profundizaremos a continuación con la comparación de los tipos de *qubits* existentes en la actualidad, con un estudio pormenorizado de la tecnología que está más madura actualmente, como es su aplicación en QKD. Mostraremos también una comparativa de los principales protocolos de Criptografía Post-Cuántica (PQC), utilizando las métricas más fiables.

2.1 Tipos de Qubit: Comparación

Para materializar el qubit, se requiere un sistema físico de dos niveles cuánticos que pueda ser manipulado con alta precisión y aislado del entorno. Las distintas arquitecturas físicas enfrentan compensaciones entre la *fidelidad operativa*, la *velocidad* y la *resistencia a la decoherencia*.

La elección del soporte físico para construir *qubits* es una cuestión central en el progreso actual. El método de creación afecta la *calidad o eficiencia* de los *qubits*

Tipo de Qubit (Plataforma Física)	Requisitos HW / Entorno	*TRL (General)	Ventajas	Inconvenientes
**Fotónicos (Polarización, Fase)	<i>Fuentes de fotones únicos/coherentes atenuados, fibra óptica o espacio libre, Detectores monofotónicos (APD/SNSPD).</i>	Alto (7-8) en QKD sobre fibra.	<i>Ideal para Comunicación (QKD). Resistente a la decoherencia temporal durante la propagación. Compatible con infraestructura de fibra óptica.</i>	<i>Limitación de Distancia por atenuación. Vulnerable a ruido y pérdidas.</i>
Circuitos Superconductores	Circuitos electrónicos a temperaturas cercanas al Cero Absoluto (T ~13 mK a 2K). Requiere infraestructura criogénica intensiva.	Medio-Alto (6-8) en Computación	Fácilmente escalable a grandes tamaños de <i>chip</i> . Fuerte	<i>Tiempos de Coherencia Cortos debido al ruido y las pérdidas. Alto</i>

			acoplamiento para operaciones lógicas rápidas.	costo y complejidad criogénica.
Iones Atrapados	Trampas electromagnéticas, láseres altamente estables, ultra-alto vacío. Enfriamiento Doppler (hasta ~1 mK). El movimiento colectivo de los iones (fonones) puede actuar como un <i>bus</i> para el entrelazamiento entre qubits.	Medio (5-6) en Computación.	Tiempos de Coherencia Largos. Alta fiabilidad y precisión en la manipulación.	<i>Difícil de escalar</i> a gran número de <i>qubits</i> .
Puntos Cuánticos	Partículas semiconductoras que confinan electrones (espín). Sólido estado.	Bajo (4-5)	Potencial de integración en silicio y miniaturización.	<i>Coherencia relativamente corta</i> debido a la interacción con fonones.
Qubits Topológicos	<i>Cuasipartículas</i> llamadas anyones que existen en sistemas bidimensionales.	Bajo (4-5)	La información no se almacena localmente en una partícula individual	<i>robustez inherente contra la decoherencia</i>

Tabla 2-1. Comparativa de Plataforma Física de Qubit (Adaptado de NTB LM)

* *TRL* (Technological Readiness Level). El *Nivel de Madurez Tecnológica* es una métrica crucial para evaluar la preparación de una tecnología, con una escala de 1 (principios básicos) a 9 (operación probada en entorno real).

** Con los datos aportados en esta tabla, se justifica la elección en el uso de los fotones en la QKD sobre el resto de tecnologías cuánticas en lo sucesivo.

2.2 QKD

2.2.1 El Paradigma de la seguridad cuántica: QKD

La QKD representa una revolución en el ámbito de las comunicaciones seguras, fundamentada en los principios inmutables de la mecánica cuántica más que en la complejidad computacional de los algoritmos clásicos. A diferencia de los sistemas criptográficos tradicionales, QKD surge como una *tecnología estratégica para garantizar la seguridad de la información a largo plazo* (ITS).

El objetivo de la Distribución Cuántica de Claves (QKD) no es cifrar el mensaje en sí, sino utilizar principios cuánticos para *distribuir de forma segura una clave secreta compartida entre dos partes*. Una vez que ambas partes poseen la misma clave, pueden utilizarla con algoritmos de cifrado simétrico robustos convencionales (como AES, OTP) para comunicarse de manera segura. Luego su funcionalidad es limitada, no cifra el contenido ni autentica la identidad de las partes.

	Medición 1	Medición 2	Medición 3	Medición 4	Medición 5	Medición 6
Esquema de Alice ⁶	$\odot$	$\otimes$	$\ominus$	$\odot$	$\odot$	$\otimes$
Partículas de Alice	$ \downarrow\rangle$	$ \uparrow\rangle$	$ \downarrow\rangle$	$ \uparrow\rangle$	$ \uparrow\rangle$	$ \downarrow\rangle$
Esquema de Bob ⁶	$\odot$	$\otimes$	$\otimes$	$\otimes$	$\odot$	$\otimes$
Partículas de Bob	$ \uparrow\rangle$	$ \downarrow\rangle$	$ \uparrow\rangle$	$ \downarrow\rangle$	$ \downarrow\rangle$	$ \uparrow\rangle$
Coincidencias en las Bases	✓	✗	✗	✗	✓	✓
Clave	0				1	0

Figura 2-1. Protocolo E91 (Adaptado de Luís Marco Cáceres Álvarez) [13]

- Fundamentos Cuánticos y Teorema de Bell

El protocolo E91, desarrollado por Artur Ekert en 1991, demostró la aplicación práctica del Teorema de Bell en criptografía. (Ver Figura 2- al principio de esta página) Este protocolo utiliza pares de fotones entrelazados para generar claves criptográficas, donde la violación de las desigualdades de Bell (la más común y utilizada en experimentos es la desigualdad de Clauser, Horne, Shimony y Holt (CHSH)) sirve como prueba de que las correlaciones cuánticas son genuinas y no pueden ser replicadas por sistemas clásicos.

La importancia práctica radica en que si un espía (Eve) intenta interceptar la comunicación proporcionando estados separables (no entrelazados), será detectado durante la fase de verificación por Alice y Bob. Sin embargo, si proporciona estados perfectamente entrelazados, puede pasar la verificación, pero no obtendrá información sobre la clave. Introduce conceptos como realismo local, la No localidad, aleatoriedad intrínseca, no comunicación superlumínica, variables ocultas locales (VHL).

- Propiedades de los Qubits y Limitaciones Prácticas

Los fotones, como portadores de información cuántica, presentan propiedades fundamentales que determinan tanto las fortalezas como las limitaciones de QKD. *El principio de incertidumbre cuántica y el teorema de no-clonación* establecen que cualquier intento de medición o copia de los estados cuánticos introduce perturbaciones detectables. Esta es por tanto la principal justificación para adoptar QKD es su promesa de seguridad a largo plazo. Una clave generada mediante QKD es teóricamente inmune a cualquier avance computacional futuro, ya sea clásico o cuántico. Sin embargo, esta robustez teórica se enfrenta a importantes limitaciones prácticas:

- *Sensibilidad al ruido ambiental*: La pérdida de coherencia ocurre cuando el sistema cuántico interactúa con el entorno, lo que resulta en la destrucción de los estados de superposición y el colapso a un estado único. Los fotones individuales son extremadamente vulnerables a la decoherencia causada por perturbaciones ambientales.
- *Necesidad de un canal clásico autenticado*: QKD solo distribuye claves secretas, no autentica a las partes. Por tanto, requiere un canal de comunicación clásico previamente autenticado para funcionar, creando un problema circular de seguridad si no se resuelve adecuadamente. Por tanto, es vulnerable a ataques de suplantación de identidad (man in the middle (MITM)).
- *Limitaciones de distancia y rendimiento*: La atenuación exponencial en fibras ópticas limita típicamente las comunicaciones QKD a distancias de 100-200 km sin repetidores. Esto limita la distancia de los enlaces punto a punto y reduce la tasa de generación de clave secreta (SKR).
- *Requisitos de hardware especializado y costoso*: Requiere una infraestructura física dedicada (canales cuánticos, como fibra óptica o enlaces de espacio libre). Se necesitan detectores de

fotón único operando a temperaturas criogénicas (13 milikelvin o -273.137 C^0) y fuentes láser de alta precisión.

- *Limitaciones Económicas:* Los costos de adquisición (180-250K € por enlace básico) y mantenimiento especializado (20-40K € anuales) limitan la adopción a aplicaciones con presupuestos significativos.
- *Limitaciones Operacionales:* La necesidad de personal especializado con formación en tecnologías cuánticas y protocolos criptográficos específicos introduce dependencias críticas de recursos humanos escasos

Estas limitaciones justifican el desarrollo de protocolos avanzados como MDI-QKD (Measurement-Device-Independent QKD) que elimina vulnerabilidades en los dispositivos de medición al externalizar estas operaciones a un nodo intermedio no confiable y TF QKD que aumentan la distancia (Fedorov, 2023).

2.2.2 Comparativa de protocolos QKD

Los protocolos de QKD utilizan *qubits* fotónicos, donde la información se codifica típicamente en la polarización o la fase de los fotones individuales. Existen distintos tipos de protocolos QKD. La elección del protocolo depende de factores como la distancia, el canal, el nivel de seguridad requerido y la madurez tecnológica.

Protocolo	Fundamento para codificar bits	TRL (Madurez)	Resistencia Clave	Limitaciones / Requisitos de Hardware
BB84(Bennett/Brassard)	Codificación en dos bases no ortogonales (Preparación y Medida).	Alta para fibra metropolitana.	Alta, incondicional en teoría. medir en la base incorrecta destruye la información, revelando al espía	Vulnerable a <i>Photon Number Splitting</i> (PNS) si usa fuentes no ideales (requiere estados señuelo para mitigación).
B92 (Bennett)	Codificación en dos estados no ortogonales.	Media/Baja.	Alta, incondicional.	Más simple que BB84, pero menor tasa secreta efectiva (SKR) por tener menos detecciones útiles.
E91 (Ekert)	Entrelazamiento cuántico.	Baja (Experimental)	La seguridad se verifica mediante la violación de las desigualdades de Bell. No existe VLO	<i>Requiere fuentes ópticas coherentes para pares entrelazados.</i> Es sensible a la decoherencia, lo que penaliza la SKR y el alcance.
SARG04	Variante de BB84/SSP.	Media/Alta.	<i>Refuerza la resistencia frente a ataques PNS.</i>	Lógica operativa más compleja que BB84.
MDI-QKD (Measurement Device Independent)	Preparación y Medida. Uso de nodo intermedio no confiable para medición conjunta, permite topologías en estrella, el nodo central no necesita ser seguro.	Media/Alta (Madurando).	<i>Inmunidad frente a ataques dirigidos al detector</i> (vulnerabilidades de <i>hardware</i> del receptor).ACL	Requiere fuentes moduladas con sincronización temporal subnanosegundo y alineación espectral precisa.
QDS (Firmas Digitales Cuánticas)	No clonación y entrelazamiento.	Baja	<i>Autenticación e integridad incondicional.</i>	Requiere infraestructura similar a QKD, pero con requisitos más estrictos en distribución multi-parte y estabilidad.

Tabla 2-2. Comparativa de Protocolos QKD (Adaptada de NTB LM)

- CV-QKD (Variable Continua): Utiliza estados coherentes y detección homodina, compatible con componentes de telecomunicaciones estándar.
- TF-QKD para largas distancias, pero con SKR y TLR muy bajos.

El cuadro anterior justifica en lo sucesivo, el uso del más popular BB84 (Ver Figura 2-2 al final de esta página)

2.2.3 Métricas de Gestión y Rendimiento QKD

La evaluación de los sistemas QKD se basa en métricas de rendimiento que vinculan la física cuántica con los procesos de cifrado y la gestión operativa.

- *Nivel de Madurez Tecnológico* (TRL – Technology Readiness Level) con la siguiente gradación:
 - TRL Alto (7-8): Alcanzado por soluciones QKD sobre fibra óptica metropolitana (ej. BB84 optimizado). Estos sistemas han demostrado viabilidad mediante pilotos pre-comerciales y se prueban en condiciones operacionales cercanas a las definitivas.
 - TRL Medio (5-6): Incluye protocolos más complejos o avanzados, como MDI-QKD y los primeros enlaces satelitales (espacio-tierra). El TRL 5 es el nivel mínimo que los estándares europeos exigen para la calificación espacial.
 - TRL Bajo (3-4): TRL de tecnologías más experimentales y sensibles, como la QKD basada en entrelazamiento (E91) o las Firmas Digitales Cuánticas (QDS).
- Tasa de Clave Secreta (SKR - Secret Key Rate): Es el parámetro de sistema más importante. Mide el número efectivo de bits utilizables para cifrado, obtenidos después de descontar pérdidas, errores y la información potencialmente adquirida por el adversario (post-procesado). La SKR está limitada por la distancia, lo que puede restringir la velocidad de comunicación en ciertas aplicaciones
- Tasa de Error Cuántico (QBER - Quantum Bit Error Rate): Mide la fracción de bits erróneos. Es el principal indicador para detectar espionaje o ruido ambiental. Si el QBER supera un umbral crítico (típicamente alrededor del 11% al 15% para BB84), la clave se descarta, garantizando que el adversario no haya obtenido información útil.aplicaciones.

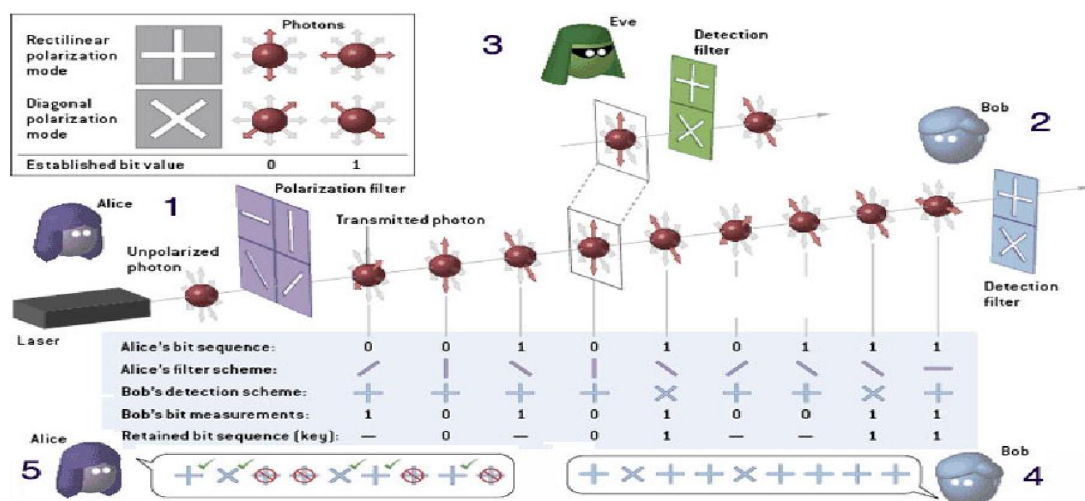


Figura 2-2. Protocolo BB84 paso a paso (Adaptado de Jeeun Lee et al.) [14]

- *Distancias Alcanzables*: QKD está limitado por la atenuación de los fotones a medida que viajan a través de la fibra. La distancia se limita a unos pocos cientos de kilómetros (ej. 100 km) en fibra óptica estándar sin repetidores cuánticos. Esta limitación se debe a la atenuación acumulada (aproximadamente 0.2 dB/km) que *reduce drásticamente la SKR y eleva el QBER*. (Ver Figura 2.3 al final de esta página)

Otras formas de analizarlo en una tabla:

Métrica	Descripción	Valoración y Factores Limitantes (Ej. BB84/MDI-QKD)
TRL (Nivel de Madurez)	Sistema demostrado y probado en un entorno operativo.	QKD sobre fibra metropolitana (BB84): TRL 7–8 (Sistema prototipo probado u operando). MDI-QKD/CV-QKD/Satélite: TRL 5–6. QDS: TRL 3–4.
QBER (Tasa de Error Cuántico)	Fracción de bits erróneos detectados. <i>Indicador primario de intrusión o ruido.</i>	Debe ser bajo. Si supera el 11%–15%, la clave se descarta. Valores experimentales: ~3% (25 km), 1.1% a 3.3% (10 km). El QBER aumenta con la atenuación y el ruido ambiental/intrínseco.
Distancia Alcanzable	Distancia máxima a la que se puede mantener una SKR útil antes de que la atenuación (0.2 dB/km) obligue a descartar la clave.	Limitada. Típicamente 80–100 km en fibra monomodo sin repetidores cuánticos. Se están desarrollando enlaces satelitales para largas distancias.
SKR (Tasa de Clave Secreta)	<i>Número efectivo de bits utilizables para el cifrado por unidad de tiempo</i> , tras post-procesado (reconciliación y amplificación de privacidad).	SKR es limitada y decrece exponencialmente con la distancia. Ejemplos experimentales: 5.10 ⁴ bps a 25 km, 100 bps a 100 km. E91 y MDI-QKD suelen tener SKR más bajas debido a mayores requisitos de control.
Eficiencia Energética	<i>Consumo asociado al hardware, especialmente los detectores.</i>	Baja eficiencia en ciertos HW. Los detectores SNSPD requieren criogenia estable cercana a 2K, lo que implica alto consumo energético (OPEX) y complejidad logística.

Tabla 2-3. Métricas de Gestión y Rendimiento QKD (Adaptada NTB LM)

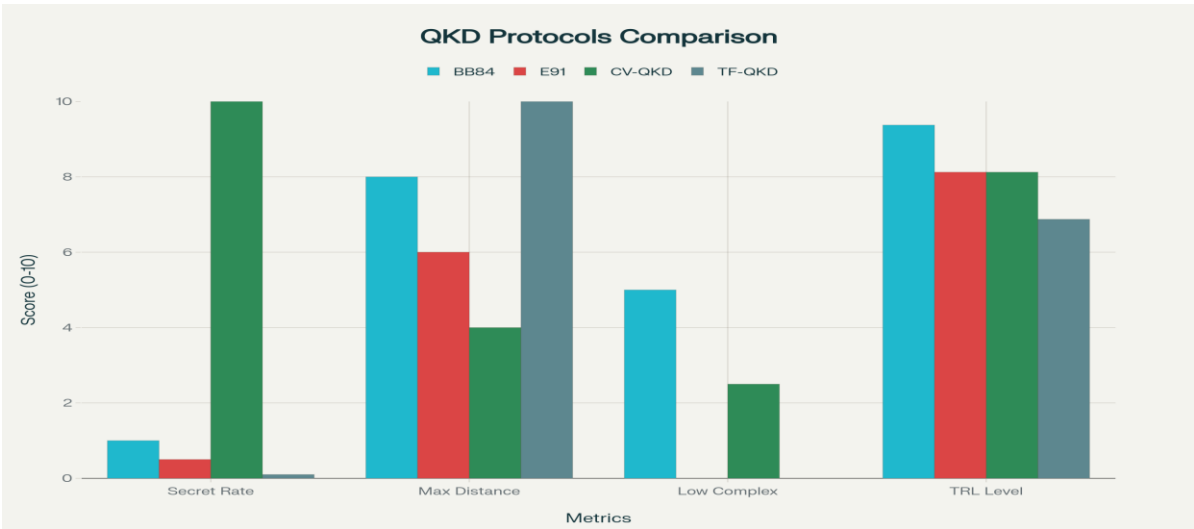


Figura 2-3. Comparativas de protocolos QKD en función de métricas (Adaptada de Perplexity)

- *Coexistencia:* A pesar de su enorme potencial, los ordenadores cuánticos no están diseñados para reemplazar a los clásicos, *sino para coexistir con ellos, actuando como un supercomputador de cálculo auxiliar para tareas específicas extremadamente complejas. Gran parte de los algoritmos cuánticos funcionan con una mezcla de procesamiento cuántico y clásico.*

2.2.4 Estandarización ETSI ISG-QKD (Capa Física y de Gestión)

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) lidera la estandarización de la implementación física y las interfaces de red para QKD.

- ETSI GS QKD 014: Define la API REST para la entrega de claves entre el Sistema de Gestión de Claves (KMS) y la Entidad de Aplicación Segura (SAE). Esta norma es crítica para la interoperabilidad, permitiendo que un firewall de un proveedor (ej. Fortinet, Palo Alto) solicite claves a un dispositivo cuántico de otro (ej. ID Quantique, Toshiba) (ETSI, 2019).
- ETSI GS QKD 004: Especifica la interfaz de aplicación a nivel de par, definiendo cómo dos dispositivos QKD coordinan la entrega de claves (ETSI, 2020).
- ETSI GS QKD 015: Establece la interfaz de control para Redes Definidas por Software (SDN). Permite que un controlador centralizado orqueste la topología de la red cuántica, gestionando rutas y asignando recursos de claves dinámicamente (ETSI, 2022).
- ETSI GS QKD 016: Perfil de Protección bajo Common Criteria. Define los requisitos de seguridad física y lógica para la certificación de módulos QKD de preparación y medida (P&M), esencial para su uso en entornos gubernamentales y financieros (ID Quantique, s.f.).

2.3 PQC

2.3.1 Comparativa de Protocolos PQC

La PQC surge como una respuesta a la amenaza cuántica y es también conocida como criptografía resistente a los ordenadores cuánticos, comprende un conjunto de algoritmos de clave pública que se ejecutan en computadoras. Utiliza algoritmos basados en la *dificultad computacional de problemas matemáticos* que se cree que son intratables incluso para un ordenador cuántico criptográficamente relevante (CRQC) (Dam et al., 2023). Al igual que RSA, no existe una prueba matemática absoluta de su invulnerabilidad. Los PQC están diseñados para reemplazar a RSA y ECC y son altamente escalables, siendo compatibles con la infraestructura de red existente (VPN, TLS).

El National Institute of Standards and Technology (NIST) está estandarizando estos algoritmos por fases que culminó en 2024 con la publicación de los primeros estándares FIPS. Esta transición, representa una de las migraciones de infraestructura criptográfica más complejas y de mayor prioridad en la historia de la ciberseguridad. Una ventaja fundamental de PQC es su alta compatibilidad y escalabilidad. Esto demuestra más robustez de PQC respecto a QKD debido a respaldo, estandarización e implementación real

Función	Algoritmo Original	Estandarización NIST (FIPS)	Tipo de Problema Matemático Base	Notas Clave
*KEM (Mecanismo de Cifrado/Intercambio (encapsulamiento) de Claves)	CRYSTALS-Kyber	ML-KEM (FIPS 203)	Basado en <i>Retículos</i> (Module-Lattice). Fundamentada en la dificultad de problemas como el Aprendizaje con Errores (LWE,	Es el principal estándar de KEM. Ofrece un equilibrio entre tamaño de clave y alta velocidad. Esta es una de las familias

			Learning With Errors)	más prometedoras y eficientes (NIST, 2024).
Firma Digital	CRYSTALS-Dilithium	ML-DSA (FIPS 204)	Basado en <i>Retículos</i> (Module-Lattice)	**Es el algoritmo de firma digital primario para autenticación e integridad recomendado por NIST (NIST, 2024).
Firma Digital	SPHINCS+	SLH-DSA (FIPS 205)	Basado en <i>Funciones</i> Hash. Sin estado (Stateless)	Seleccionado por su diversidad criptográfica, ya que no se basa en retículos, <i>sirviendo como respaldo</i> si los algoritmos basados en retículos fallan (NIST, 2024).
Firma Digital	FALCON	FN-DSA (FIPS 206, pendiente)	Basado en <i>Retículos</i> (FFT sobre NTRU-Lattice)	Orientado a aplicaciones que requieren un <i>tamaño de firma muy pequeño</i> .

Tabla 2-4. Comparativa de Protocolos PQC (Adapatada de NTB LM)

*Un KEM (Mecanismo de Encapsulación de Claves) es un algoritmo criptográfico que permite a dos partes establecer una clave secreta compartida a través de un canal público, utilizando la criptografía de clave pública. Para ello, una parte genera un secreto compartido y lo encapsula (cifra) usando la clave pública de la otra parte. La otra parte, usando su clave privada, desencapsula el mensaje para recuperar el secreto compartido. Este secreto se usa luego con algoritmos de clave simétrica para cifrar y descifrar los datos. Se amplía información en Anexo V.

** FIPS 204 (ML-DSA). Aunque ofrece una seguridad robusta, sus claves públicas y firmas son significativamente más grandes que las de ECDSA, lo que tiene implicaciones directas en el tamaño de los certificados digitales y la fragmentación de paquetes en el handshake TLS (National Institute of Standards and Technology [NIST], 2024).

Otras alternativa:

Basada en Códigos (Code-Based)	Pro Problema de decodificación del Síndrome (decodificación de códigos lineales aleatorios). Es un problema que ha demostrado ser NP-completo.	<i>Classic McEliece.</i>	Ha demostrado ser un PQC muy seguro a lo largo del tiempo, con alta confianza criptográfica.	<i>Tamaños de clave muy grandes</i> , lo que puede limitar su uso en comunicaciones con restricciones de ancho de banda, como **VPN y TLS.
---------------------------------------	--	--------------------------	--	--

Tabla 2-5. Protocolo PQC basado en Códigos (Adaptada de NTB LM)

****VPN (Red Privada Virtual)** crea un túnel cifrado a través de internet para conectar de forma segura tu dispositivo a una red privada, ocultando tu IP y protegiendo tus datos. TLS (Seguridad de la Capa de Transporte) es un protocolo criptográfico que cifra las comunicaciones entre dos sistemas, como un navegador web y un servidor, para garantizar la confidencialidad, integridad y autenticación de los datos. Las VPN suelen utilizar TLS para establecer sus túneles seguros.

Otros:

- Basada en Polinomios Multivariable: Se basa en la dificultad de resolver sistemas de ecuaciones polinómicas multivariable sobre un cuerpo finito.
- Basada en Isogenias: Utiliza la dificultad de encontrar un mapa de isogenia entre dos curvas elípticas supersingulares. Quebrado y en desuso
- Criptografía basada en códigos correctores de errores: (basada en la dificultad de decodificar un código lineal aleatorio, como los códigos de Goppa).

2.3.2 Métricas de Gestión y Rendimiento PQC

La PQC, en cambio, no se basa en tecnología *Hardware*, se basa en algoritmos de *software* y se evalúa por métricas de *rendimiento* algorítmico (tamaño de clave, latencia) y métricas de *gestión* (criptoagilidad, riesgo HNDL). Es fundamental para evaluar la viabilidad, la seguridad a largo plazo y la eficiencia operativa de los nuevos algoritmos que buscan resistir los ataques de las futuras computadoras cuánticas criptográficamente relevantes (CRQC).

- *TRL* para PQC. La Criptografía Post-Cuántica (PQC) tiene un TRL muy alto. Los algoritmos estandarizados por el NIST, como CRYSTALS-Kyber y CRYSTALS-Dilithium/Falcon, están listos para el uso masivo. La migración hacia un entorno PQC puro se estima que puede tardar de 5 a 10 años en consolidarse plenamente en el sector.
- *Criptoagilidad*: Es la capacidad de cambiar rápidamente entre algoritmos criptográficos en caso de que se descubran vulnerabilidades en un PQC. Esto requiere equipar a los equipos y diseñar la infraestructura y el software para que los algoritmos puedan intercambiarse eficazmente a medida que los estándares maduran.
- *Mitigación de Riesgo Cuántico* (HNDL). Implica que los atacantes roban datos cifrados hoy con la intención de descifrarlos en el futuro con un ordenador cuántico criptográficamente relevante (CRQC). Se debe mantener un inventario criptográfico activo y clasificar cada activo por sensibilidad para orientar la mitigación basada en el riesgo, teniendo en cuenta la vida útil de los datos.

Las métricas críticas de rendimiento para PQC se centran en el *trade-off* (equilibrio) entre seguridad y eficiencia en el software.

- *Tamaño de Clave/Firma*: Los protocolos PQC generalmente tienen tamaños de clave y tamaños de firma digital *más grandes* que la criptografía clásica (RSA o ECC). Un mayor tamaño puede afectar *negativamente la latencia* de las comunicaciones. Por ejemplo, el algoritmo como McEliece ofrecen alta seguridad, pero tienen grandes tamaños de clave. Para aplicaciones con restricciones de tamaño de clave, las funciones hash y los polinomios multivariable pueden ser más adecuados. Este factor puede limitar su uso en comunicaciones VPN y TLS.
- *Complejidad Computacional* (Eficiencia). Se evalúa la complejidad computacional para la resolución de problemas (*tiempo y espacio/memoria*). Esto es crucial para la adopción en dispositivos de bajo consumo como el IoT, que operan con recursos limitados (memoria a nivel de kilobyte). El aumento del tamaño de los algoritmos PQC impacta en el rendimiento de su cómputo en entornos restringidos.

- *Migración de Algoritmos.* El plan de transición debe identificar los algoritmos PQC más adecuados para proteger los activos, prestando atención a los estándares de NIST.

Resumidas y agrupadas en una tabla resultante:

Categoría de Métrica	Métrica Específica	Concepto Fundamental
Rendimiento Algorítmico (Eficiencia Técnica del Software)	Tamaño de Clave/Firma	Indica que los PQC suelen tener claves y firmas <i>significativamente más grandes que la criptografía clásica</i> (RSA/ECC), lo cual puede afectar la latencia y la capacidad de almacenamiento.
	Latencia	<i>Mide el retardo de tiempo que introducen las operaciones criptográficas PQC.</i> El aumento del tamaño de las claves en PQC puede aumentar la latencia de las comunicaciones.
	Complejidad Computacional	<i>Evalúa la eficiencia operativa de un algoritmo PQC en términos de velocidad y consumo de recursos</i> (CPU, memoria). Es crítica para la implementación en dispositivos de bajo consumo o IoT.
	Migración	La transición de algoritmos clásicos (vulnerables a Shor) a PQC. La estrategia clave es el <i>uso de claves o esquemas híbridos</i> (combinando PQC con algoritmos clásicos) para una adopción inmediata y seguridad en la transición.
Gestión Estratégica (Planificación y Resiliencia)	Criptoagilidad	La <i>capacidad de cambiar rápida y eficazmente entre algoritmos PQC</i> , o de un PQC comprometido a otro, a medida que evolucionan las amenazas y los estándares.
	Mitigación HNDL	La priorización de riesgos enfocada en <i>proteger los datos de larga duración que los atacantes roban hoy</i> (cifrados con algoritmos clásicos) para descifrarlos en el futuro con un ordenador cuántico criptográficamente relevante (CRQC).
	TRL	Mide el <i>nivel de madurez de una tecnología</i> (escala 1 a 9). Los algoritmos PQC estandarizados por NIST (como Kyber y Dilithium) se consideran de TRL muy alto (8-9), listos para el uso masivo.

Tabla 2-6. Métricas de Gestión y Rendimiento PQC (Adaptada de NTB LM)

2.4 Amenazas cuánticas (Shor, Grover, HDNL) & controles de seguridad post-cuánticos (PQC, QKD)

Para visualizar la distinción entre las amenazas cuánticas y los controles defensivos PQC y QKD, es necesario mapear cada ataque cuántico contra las tres funciones criptográficas esenciales en un cuadro: autenticación, distribución de claves y cifrado. *Esta matriz ilustra cómo PQC proporciona una solución integral para las funciones asimétricas comprometidas por Shor, mientras que QKD ofrece una solución de distribución de claves físicamente segura, complementada por PQC para la autenticación y por el cifrado simétrico para la confidencialidad de datos masivos.*

COMUNICACIONES CUÁNTICAS SEGURAS: HOJA DE RUTA DE APLICACIONES HÍBRIDAS:
QKD+PQC

Característica	AMENAZAS CUÁNTICAS (Ataques)		CONTROLES CUÁNTICOS (Defensa)	
Nombre	Algoritmo de Shor	Algoritmo de Grover	PQC	QKD
Fundamento	Propiedades de la mecánica cuántica para resolver problemas matemáticos clásicos complejos.	Uso de la superposición cuántica para acelerar cuadráticamente la búsqueda no estructurada.	Problemas matemáticos <i>clásicos</i> nuevos (ej. basados en retículos o códigos) que se creen intratables incluso para QC.	Leyes fundamentales de la física (Teorema de No Clonación, Principio de Incertidumbre).
Objetivo / Tipo de Ataque	Romper la criptografía asimétrica (Clave Pública).	Reducir a la mitad la fuerza efectiva de la criptografía simétrica (ej. AES y funciones <i>hash</i>).	Sustituir la criptografía asimétrica vulnerable (RSA, ECC, DH).	Establecer una clave simétrica secreta con seguridad incondicional.
Quién Autentica (Firmas Dig./Identidad)	COMPROMETIDO: Puede forjar firmas digitales al resolver el logaritmo discreto y obtener claves privadas de la pública	INDIRECTAMENTE COMPROMETIDO: Debilita la seguridad de las funciones hash utilizadas para integridad y validación de bloques.	PQC (Firmas Digitales): Utiliza algoritmos de firma digital post-cuántica (ej. CRYSTALS-Dilithium) para la autenticación e integridad.	REQUIERE APOYO EXTERNO: Los protocolos QKD puros carecen de autenticación nativa. Depende de un canal clásico autenticado (usualmente con PQC) para prevenir ataques MITM.
Quién Distribuye Claves (KEM) (Acuerdo de Secreto)	COMPROMETIDO: Rompe eficientemente el intercambio de claves (DH/ECDH) al factorizar números grandes en tiempo polinomial.	Acelera la fuerza bruta, obligando a duplicar el tamaño de la clave simétrica (ej. AES-128 debe migrar a AES-256).	PQC (KEMs): Utiliza Mecanismos de Encapsulación de Claves (KEM) resistentes a Shor (ej. CRYSTALS-Kyber) para el intercambio de claves.	QKD (Generación): Genera la clave secreta compartida utilizando <i>qubits</i> fotónicos (ej. Protocolo BB84). Es inquebrantable en teoría.
Quién Cifra (Confidencialidad de Datos Masivos)	La clave asimétrica/híbrida se rompe en segundos por un CRQC, permitiendo el descifrado del tráfico cifrado.	Reduce la dificultad del descifrado por fuerza bruta.	PQC (KEM/PKE): Provee algoritmos de cifrado de clave pública post-cuántica para asegurar la confidencialidad, ofreciendo resistencia matemática al HNDL.	Cifrado Simétrico Clásico (OTP/AES): La clave generada por QKD se utiliza para cifrar el mensaje en un canal clásico usando algoritmos simétricos robustos (ej. AES-256).
Resistencia al HNDL	El HNDL se basa en este algoritmo: Es la herramienta utilizada en el futuro por el CRQC para descifrar datos cifrados recopilados hoy.	El atacante tiene una ventaja cuadrática para descifrar claves simétricas recopiladas.	Seguridad Condicional: Ofrece resistencia a la recopilación (HNDL), pero su seguridad depende de supuestos matemáticos que podrían romperse en el futuro.	Seguridad Incondicional: Es la solución definitiva contra el HNDL, ya que la seguridad se basa en leyes físicas inquebrantables, independientemente del poder computacional futuro.

Tabla 2-7. Amenazas cuánticas & controles de seguridad post- cuánticos (Adaptada de NTB LM)

La tabla anterior resalta cómo las amenazas cuánticas, principalmente los algoritmos de Shor y Grover, atacan los dos pilares de la criptografía clásica: la clave pública (asimétrica) y la clave simétrica, respectivamente. Esta vulnerabilidad es la que alimenta la estrategia de espionaje HNDL. Frente a esta situación, han surgido dos enfoques complementarios: la PQC y la QKD.

2.4.1 Analogía: El ecosistema de seguridad cuántica es como un banco.

Shor y Grover son los ladrones con una herramienta maestra (el QC) que rompe cerraduras matemáticas antiguas (Shor ataca la caja fuerte principal RSA/ECC) y reduce la efectividad de las alarmas (Grover ataca AES/Hashes). HNDL es la estrategia de robar los planos y esperar a que la herramienta esté lista.

PQC es la nueva cerradura matemática (Kyber para la puerta, Dilithium para la identidad). Es mucho más fuerte, pero no es perfecta; podría haber una llave maestra desconocida.

QKD es el mensajero blindado que entrega la clave: si alguien intenta espiarlo o interceptarlo, el paquete se autodestruye inmediatamente (detección por QBER), garantizando que nadie pueda capturar la llave en el proceso. QKD necesita que un agente de seguridad PQC verifique la identidad del mensajero antes de que pueda entregar la llave (autenticación).

3 ESTADO DEL ARTE Y EVALUACIÓN TECNOLÓGICA

Los fundamentos y sus inherentes desafíos prácticos vistos en el apartado anterior, son el punto de partida para el análisis aplicado que se desarrollará a continuación, evaluando y comparando dónde y cómo estas tecnologías pueden aportar un valor real.

Empezaremos analizando a día de hoy la viabilidad y gestión tecnológica de las comunicaciones cuánticas seguras, centrándose principalmente en la QKD y su comparativa con la PQC como las tecnologías más maduras de ambos modelos cuántico y clásico.

Nos enfocaremos posteriormente en el análisis de ambas tecnologías por separado o juntas, en la gestión tecnológica, la evaluación de madurez y la viabilidad de despliegue en entornos críticos (institucionales y de defensa). Analizaremos un caso de uso para un enlace Sede-Delegación en este entorno. Por último y más importante elaboramos una hoja de ruta para su adopción, con la solución elegida como la más óptima del caso de uso anterior

3.1 Estado del arte aplicado de comunicaciones/criptografía

3.1.1 QKD

El estado actual de la tecnología cuántica se define como la era NISQ (Noisy Intermediate-Scale Quantum). Las computadoras actuales *son de escala intermedia* (decenas a cientos de cúbits) y ruidosas (*propensas a errores*). Estas carecen de los mecanismos de corrección de errores cuánticos necesarios para realizar cálculos complejos, lo que limita su aplicación actual. *Superar la decoherencia es el principal foco de la investigación*.

La QKD es la aplicación más madura, popular y desarrollada de la criptografía cuántica. Su objetivo no es transmitir la información cifrada, sino establecer una clave secreta compartida (una serie aleatoria de bits) a través de un canal cuántico, que luego puede usarse para cifrar y descifrar mensajes en un canal clásico. Este enfoque proporciona una forma de seguridad teórica de la información cuántica (Quantum Information-Theoretic Security, Q-ITS), garantizando la seguridad de la clave distribuida. La QKD ha alcanzado un nivel de madurez tecnológica (TRL) de 6-7 de media, con sistemas comerciales ya desplegados en entornos metropolitanos. Los protocolos más establecidos incluyen (Sahu y Mazumdar, 2024) (Wang y Ismail, 2025):

- Variable Discreta (DV-QKD): Codifica la información en propiedades de fotones individuales (polarización, fase, tiempo de llegada). Para detectarlos se requiere contadores de fotones

(SPAD/SNSPD). Como ventajas tiene su historial probado de seguridad y tolerancia superior a pérdidas (funciona hasta > 400 km con SNSPD, es decir domina en el backbone y larga distancia. Como desventajas que necesita hardware especializado y costoso y que los detectores tienen "tiempos muertos" tras cada detección, limitando la tasa máxima en distancias cortas. Ejemplos:

- BB84: Eficiencia del 50% en condiciones ideales, pero vulnerable a ataques PNS (Photon Number Splitting) cuando se usan pulsos coherentes débiles en lugar de fotones únicos (Primaatmaja et al., 2023) (Lidbjörk y Söderström Nylander, 2023).
- E91: Basado en entrelazamiento, teóricamente más seguro, pero con aproximadamente un 22% de eficiencia (Liu et al., 2025) (Hoque et al., 2024).
- CV-QKD: Codifica la información en las cuadraturas (X y P) del campo electromagnético de estados coherentes (láser atenuado). Usa modulación Gaussiana. Utiliza *Detección Homodina o Heterodina*, la misma tecnología empleada en los receptores coherentes de las telecomunicaciones clásicas de 100G/400G (J, Karthika Sorna Ilakkia y Jebadura, 2025).

Como ventajas tiene integración fotónica (PIC) más sencilla y barata y altísimas tasas de clave (SKR) del orden de Mbps en distancias cortas (< 10 km). Es la candidata ideal para redes de acceso metropolitanas (Zeng et al., 2024) y centros de datos (DC) debido a su compatibilidad de hardware y costo ya que no sufren de tiempo muerto del detector.

Como Limitaciones es extremadamente sensible al "Exceso de Ruido" (Excess Noise), el ruido de fase de los láseres y la diafonía en la fibra degradan rápidamente la seguridad. Típicamente limitada a distancias metropolitanas (< 80 km) (Jouguet et al., 2013) y que la reconciliación de datos en CV-QKD requiere algoritmos de corrección de errores muy pesados computacionalmente para bajas relaciones señal-ruido (SNR), lo que puede crear un cuello de botella en el post-procesado.

- Los sistemas actuales de protocolos de campo gemelo (Twin-Field QKD) han demostrado la capacidad de superar el límite fundamental de los sistemas sin repetidores, alcanzando distancias de más de 400 km en fibra óptica y se han demostrado enlaces satelitales de hasta 1.200 km. Las tasas de generación de claves han mejorado significativamente, con implementaciones recientes superando los límites sin repetidores (Zhang et al., 2025; Yang et al., 2024; Shamshad et al., 2022; García et al., 2024; Weger et al., 2024).
- Las firmas Digitales Cuánticas (QDS) son una extensión de los principios QKD, adaptada para proveer *autenticación e integridad* de mensajes aprovechando las leyes físicas fundamentales, como la imposibilidad de clonación. El objetivo de QDS es garantizar que el mensaje firmado pueda verificarse como auténtico por cualquier tercero. Estas han experimentado avances notables en eficiencia.

Protocolos recientes como OTUH-QDS logran tasas de 1.22 firmas por segundo, mejorando en varios órdenes de magnitud los métodos anteriores que requerían años para procesar documentos de megabit. Implementaciones chip-integradas han demostrado operación sobre 200 km, indicando viabilidad para redes de área extensa (Wiedijk, 2022). Esta arquitectura facilita la integración con infraestructuras de fibra existentes y permite el despliegue a escala comercial (Wang, 2025).

Protocolo	TRL	SKR (50km)	Tolerancia QBER	Requisitos Hw	Mad. Comercial
BB84	7-8	10-50 kbps	11%	Estándar	Alta

E91	5-6	1-10 kbps	7.5%	Fuentes entrelazadas	Media
SARG04	6-7	5-25 kbps	20%	Similar BB84	Media
MDI-QKD	6-7	1-5 kbps	25%	Interferómetros precisos	Baja-Media
QDS	4-5	N/A	N/A	Memoria cuántica	Investig.

Tabla 3-1. Comparativa entre protocolos QKD (Adaptada de Perplexity)

3.1.2 PQC

En lo que respecta a PQC, el NIST ha publicado tres estándares fundamentales (Dam et al., 2023):

- FIPS 203 (ML-KEM/CRYSTALS-Kyber): *Encapsulación de claves* con eficiencia superior a RSA/ECC
- FIPS 204 (ML-DSA/CRYSTALS-Dilithium): *Firmas digitales* con balance velocidad-seguridad
- FIPS 205 (SLH-DSA/SPHINCS+): *Firmas sin estado* para integridad a largo plazo.

Los análisis de rendimiento revelan ventajas significativas de PQC sobre criptografía clásica (Wang, 2025) (Organization for Economic Cooperation and Development, 2025):

- *Kyber-512 es unas 3 veces más rápido que RSA-2048 y ECDH P-256*
- Dilithium muestra tiempos competitivos para verificación de firmas
- *Los tamaños de clave y firma son mayores, pero manejables en infraestructuras modernas*

3.1.3 Evaluación de Propiedades Criptográficas de PQC y QKD

Los principios de seguridad de PQC y QKD dan lugar a diferentes garantías para propiedades esenciales como la *confidencialidad*, la *autenticidad* y la *seguridad a largo plazo* (Primaatmaja et al., 2023). Analizar estas diferencias es crucial para cualquier estrategia de seguridad que busque alinear la tecnología con los requisitos de protección de su organización.

- **Confidencialidad:** Asegura que la información solo sea accesible para las partes autorizadas.
 - PQC ofrece confidencialidad *computacional*. La protección de los datos depende de la dificultad computacional de romper los algoritmos de cifrado. Si un futuro avance permitiera resolver el problema matemático subyacente, la confidencialidad de todos los datos cifrados (pasados y futuros) quedaría comprometida.
 - QKD puede proporcionar seguridad cuántica-teórica de la información (*Q-ITS*) para la clave distribuida. Sin embargo, la confidencialidad del mensaje final depende de cómo se utilice esa clave:
 - **QKD + One-Time Pad (OTP):** Esta combinación ofrece confidencialidad Q-ITS para el mensaje, el nivel más alto de seguridad teórica posible.
 - **QKD + Cifrado Simétrico** (ej. AES): En este escenario híbrido, la confidencialidad del mensaje se basa en dos conjuntos de supuestos: los supuestos computacionales del cifrado simétrico (como AES) y los supuestos cuántico-teóricos de QKD para la distribución de la clave.

- *Autenticidad*: Se verifica la identidad de las partes y garantiza que los datos no han sido alterados en tránsito.
 - PQC aborda directamente la autenticidad a través de algoritmos de firma digital como Dilithium o FALCON. Estos esquemas proporcionan garantías de autenticidad, integridad y no repudio con seguridad *computacional* frente a atacantes cuánticos.
 - QKD, por sí misma, no proporciona ninguna garantía de autenticidad. Esta es una *limitación fundamental*. La QKD requiere un canal clásico previamente autenticado para intercambiar mensajes de post-procesamiento y verificar la identidad de los participantes. Esta autenticación debe lograrse mediante otros medios, como firmas digitales PQC o el uso de claves simétricas pre-compartidas, lo que crea una dependencia crítica en la criptografía computacional.
- *Secreto Hacia Adelante* (Forward Secrecy) y *Post-Compromiso* (PCS)

Estas son propiedades avanzadas de seguridad a largo plazo. El Secreto Hacia Adelante garantiza que la *corrupción de una clave a largo plazo no comprometa las claves de sesión pasadas*. La Seguridad Post-Compromiso (PCS) es la capacidad de un sistema para *recuperarse y restablecer* la seguridad después de que una clave de sesión haya sido comprometida.

- Ambas tecnologías pueden ser utilizadas en protocolos que implementen estas propiedades. La QKD, por su naturaleza de generar claves de sesión frescas y efímeras "sobre la marcha" (on the fly), ofrece una implementación particularmente natural y robusta de la Seguridad Post-Compromiso.

Aunque las garantías teóricas son un pilar del análisis, su valor práctico se mide al enfrentarlas a las realidades del despliegue, la escalabilidad y el coste.

3.1.4 Eval. de Viabilidad Práctica, Escalabilidad y Despliegue en PQC y QKD

Para los responsables de la toma de decisiones, la viabilidad técnica, la escalabilidad y el coste total de propiedad son factores tan determinantes como las garantías teóricas de seguridad (Liu et al., 2025). Un análisis pragmático revela diferencias drásticas entre PQC y QKD en el ámbito de la implementación. En cuanto al despliegue, para garantizar que este estudio de viabilidad sea aplicable a escenarios del mundo real, es necesario establecer unas referencias. Los siguientes parámetros y rangos definen los límites operativos de la arquitectura propuesta, basándose en datos empíricos de implementaciones comerciales y experimentales actuales.

- QKD:
 - El Canal Óptico. El medio de transmisión se asume como fibra óptica monomodo estándar (SMF-28), operando bajo las restricciones de coexistencia con tráfico clásico (DWDM). Con estas características:
 - Atenuación de Fibra (α):
 - Banda C (1550 nm): Se asume un coeficiente de pérdida de 0.20 dB/km. Este es el estándar industrial para redes metropolitanas y de larga distancia (Kiktenko et al., 2023).
 - Banda O (1310 nm): Se asume 0.35 dB/km. Esta banda se utiliza frecuentemente para canales de sincronización o para segregar el tráfico cuántico del clásico y evitar el ruido por dispersión Raman.
 - Pérdidas por Inserción. Empalmes: 0.05 - 0.1 dB por fusión. Conectores (FC/APC): 0.3 - 0.5 dB por par.
 - Conmutadores Ópticos (SDN): En una red mallada, el enrutamiento óptico introduce pérdidas significativas. Se asume 1.0 - 3.0 dB por salto (hop) en conmutadores MEMS o LCoS (European

Telecommunications Standards Institute [ETSI], 2021). Ver anexo V: QRNG y Orquestador SDN

- Ruido de Fondo (Noise Floor): La coexistencia con canales clásicos de alta potencia (+3 dBm) genera ruido por Raman Scattering. Se asume el uso de filtros espectrales con un rechazo >100 dB para aislar el canal cuántico (National Institutes of Health [NIH], 2026).
- Parámetros de Rendimiento de Detectores: La viabilidad del Secure Key Rate (SKR) depende críticamente de la tecnología de detección empleada en el receptor (Bob).

Parámetro	Detectores de Fotón Único (SPAD) (DV-QKD)	Superconductores (SNSPD) (DV-QKD)	Detección Homodina (CV-QKD)
Eficiencia de Detección (η)	10% - 25% (Gatillado)	> 85% (Crio-refrigerado)	> 60% (Eficiencia Cuántica)
Tasa de Cuentas Oscuras (DCR)	10^{-4} - 10^{-5} por puerta	< 10 Hz (Virtualmente nulo)	N/A (Limitado por Shot Noise)
Jitter Temporal	200 - 500 ps	< 50 ps (Islam et al., 2017)	N/A
Tiempo Muerto (Dead Time)	1 - 10 μ s	< 50 ns (Dixon et al., 2009)	Limitado por ancho de banda elec.
Costo Operativo	Bajo/Medio (Peltier)	Muy Alto (Criogenia < 2K)	Medio (Tecnología Telecom)
Rango de Viabilidad	Acceso/Metro (< 80 km)	Backbone (> 100 km)	Metro (< 50 km) de alta tasa

Tabla 3-2. Parámetros de rendimiento de detectores (Adaptado de Gemini)

- Renovación de Claves (Rekeying): A diferencia de IKEv2 estándar (vida útil de 8-24 horas), la arquitectura propuesta asume una rotación de claves agresiva impulsada por la disponibilidad de QKD cada 60 segundos o cada 1 GB de datos transferidos (Juniper Networks, 2022).
- Latencia de Red: Se asume una red de transporte óptica (OTN) con latencias de propagación de 5 μ s/km.

La siguiente tabla resume la comparación de los aspectos prácticos más relevantes:

Métrica	PQC	QKD
Infraestructura Requerida	<i>Software</i> y actualizaciones de protocolos sobre la infraestructura de comunicación clásica existente.	<i>Hardware</i> especializado y dedicado, incluyendo canales cuánticos (fibra óptica), fuentes de fotones únicos y detectores. Requiere nueva infraestructura.
Escalabilidad	<i>Altamente escalable</i> ; se integra en la arquitectura de Internet y redes existentes de forma similar a la criptografía actual.	Escalabilidad <i>pobre</i> . Fuertemente limitada por la distancia (típicamente < 100-200 km por fibra sin repetidores) y la topología de la red (requiere 'nodos de confianza' para redes más grandes).
Rendimiento y Sobrecarga	Introduce <i>sobrecarga en latencia y tamaño de claves/firmas</i> . Ej.: JPMorgan Chase reportó un aumento	<i>Limitado por la tasa de generación de claves (SKR), que disminuye exponencialmente con la distancia</i> . Las

	del 20% en la latencia de TLS y de 3 a 5 veces en el almacenamiento de claves.	tasas varían de kbps a Mbps en distancias cortas.
Madurez y Estandarización	Proceso de estandarización avanzado liderado por el NIST (EE. UU.), con algoritmos como Kyber y Dilithium ya seleccionados. Esfuerzos de estandarización también por ETSI e IETF.	Existen estándares (ej. ETSI, ITU-T), pero la tecnología es <i>menos madura</i> para un despliegue masivo. Considerada una <i>solución de nicho</i> por agencias como ANSSI (Francia) y la NSA (EE. UU.).
Coste	Coste asociado a la migración de software, inventario criptográfico, actualizaciones de sistemas y formación.	Coste <i>muy elevado</i> debido a la inversión en hardware, infraestructura dedicada y mantenimiento y formación especializado.

Tabla 3-3. Evaluación de viabilidad entre PQC y QKD (Adaptado de NTB LM)

El análisis de la implementación técnica y su viabilidad nos lleva a examinar los casos de uso reales donde estas tecnologías han sido desplegadas y han demostrado su valor estratégico.

3.1.5 Casos de Uso Desplegados y Aplicabilidad Estratégica en PQC y QKD

El análisis de los casos de uso reales es fundamental para determinar la idoneidad y el nivel de madurez de cada tecnología para diferentes escenarios de negocio y seguridad, revelando dónde cada enfoque aporta un valor tangible.

- Dominios de Aplicación de PQC

La PQC se posiciona como un reemplazo universal y basado en software para la criptografía de clave pública actual, diseñada para ser integrada en la infraestructura digital existente con un *impacto arquitectónico mínimo*. Sus aplicaciones son, por tanto, amplias y generalizadas.

- *Seguridad en Internet*: Protección de protocolos de comunicación esenciales como Transport Layer Security (TLS), asegurando la navegación web, las API y las comunicaciones en la nube.
- *Transacciones Financieras*: Migración de sistemas bancarios y redes de pago para proteger datos financieros sensibles. JPMorgan Chase es un ejemplo notable de una institución que ha implementado PQC para comunicaciones interbancarias.
- *Tecnología Blockchain*: Desarrollo de libros de contabilidad resistentes a ataques cuánticos (quantum-resistant ledgers), como el proyecto QRL, para asegurar la integridad a largo plazo de las criptomonedas y los contratos inteligentes.
- *Votaciones Electrónicas* (e-voting): Aseguramiento de la integridad, privacidad y anonimato en sistemas de votación digital, utilizando firmas PQC y criptosistemas basados en códigos.
- *Internet de las Cosas* (IoT): Aunque presenta desafíos de rendimiento en dispositivos con recursos limitados, la PQC es el enfoque previsto para asegurar las comunicaciones en el vasto y creciente ecosistema de IoT.

- Despliegues Reales de QKD

Las implementaciones de QKD se caracterizan por ser soluciones de *nicho*, orientadas a escenarios de *muy alta seguridad* que requieren protección de *enlaces físicos punto a punto o en redes metropolitanas*. Su despliegue está intrínsecamente ligado a la disponibilidad de infraestructura de fibra óptica dedicada.

- *Sector Gubernamental*: Se ha utilizado para la transmisión segura de resultados electorales entre el centro de recuento y una ubicación de almacenamiento en Ginebra, Suiza.
- *Infraestructura Crítica*: Protección de las comunicaciones de control en redes eléctricas, como lo demostró el Oak Ridge National Laboratory en Estados Unidos.
- *Centros de Datos*: Establecimiento de enlaces de comunicación ultra-seguros entre dos centros de datos para la sincronización y respaldo de información crítica, como en el caso de la empresa de servicios públicos SIG en Ginebra.
- *Sector Financiero*: Transmisión segura de datos bancarios en redes de área metropolitana (MAN) y extendida (WAN), como la red implementada por el Industrial and Commercial Bank of China (ICBC).
- *Salud*: Transferencia segura de datos genómicos sensibles y copias de seguridad de historiales médicos entre instituciones, con despliegues en Japón.
- *Redes a Gran Escala*: Construcción de redes troncales de larga distancia, como la red Beijing-Shanghai de 2000 km, que se basa en una cadena de "nodos de confianza" para retransmitir la clave a lo largo del enlace.

Estos despliegues subrayan los perfiles estratégicos divergentes de PQC y QKD, lo que nos conduce a una conclusión final sobre su posicionamiento en las futuras arquitecturas de seguridad.

3.2 Integración entre PQC y QKD

La tendencia actual no favorece la elección exclusiva entre QKD y PQC para asegurar la seguridad poscuántica. Estas son consideradas herramientas complementarias en lugar de excluyentes. Por ello se aboga por su *integración sinérgica hacia Modelos Híbridos Emergentes*. El diseño híbrido (QKD + PQC) es crucial en entornos como la Defensa o la Administración Pública, donde la *información mantiene su valor operativo durante décadas*. Se detalla a continuación, cómo difieren y se complementan QKD, PQC y Híbrido QKD+PQC para lograr una seguridad criptográfica robusta en la era post-cuántica.

- *Diferencias Fundamentales entre QKD y PQC*

QKD y PQC divergen significativamente en su base de seguridad, requisitos de implementación, coste y alcance de protección:

- Base de la Seguridad

La diferencia más crítica radica en el fundamento de su *seguridad*, lo que determina su resistencia a largo plazo, especialmente *contra ataques del tipo HNDL*.

Aspecto	QKD	PQC
Fundamento	Se basa en las leyes fundamentales de la <i>física</i> cuántica, como el principio de incertidumbre de Heisenberg, el teorema de no clonación, el entrelazamiento y la superposición.	Se basa en la dificultad computacional de resolver nuevos problemas <i>matemáticos</i> , que se consideran intratables tanto para ordenadores clásicos como cuánticos (Complejidad computacional).
Tipo de Seguridad	Ofrece seguridad <i>incondicional</i> (o <i>perfecta</i>) en teoría, ya que se sustenta en principios físicos inviolables, independientemente del poder	Ofrece seguridad condicional o <i>resistente a la cuántica</i> , ya que su fortaleza depende de <i>supuestos matemáticos</i> que podrían romperse si se descubre un nuevo avance criptoanalítico

	computacional futuro del atacante (Forward Secrecy físico).	teórico (Condicional a avances en criptoanálisis).
Mecanismo de Detección	Detecta <i>inmediatamente</i> cualquier intento de espionaje, ya que la observación o medición de los estados cuánticos (qubits fotónicos) los perturba, introduciendo errores detectables (QBER).	<i>No detecta la interceptación o el espionaje pasivo</i> ; su seguridad reside en la imposibilidad matemática de descifrar la clave.

Tabla 3-4. Diferencias QKD y PQC en seguridad y HNDL (Adaptada de NTB LM)

- Requisitos de Implementación y Rendimiento. Los requisitos prácticos para desplegar QKD y PQC difieren drásticamente:

- QKD (Hardware): QKD se basa en hardware especializado (óptica, fuentes de fotones, detectores monofotónicos). Esto conlleva un *mayor coste* (CAPEX/OPEX) y *una mayor complejidad* de implementación y mantenimiento.
- PQC (Software): PQC se implementa mediante software/firmware. Puede adoptarse mediante una actualización de software en la infraestructura de TIC existente, lo que facilita una *transición rápida y masiva*.

En términos de rendimiento, el QKD está *limitado por factores físicos* como la atenuación óptica y el ruido, que restringen la distancia alcanzable (típicamente a unos 80-100 km sin repetidores cuánticos) y limitan la Tasa de Clave Secreta (SKR). Por su parte, la PQC no tiene limitaciones de distancia física, pero los nuevos algoritmos suelen tener *tamaños de clave y de firma digital significativamente más grandes* que la criptografía clásica, lo que puede aumentar la latencia y el tamaño de los archivos cifrados.

- Alcance Criptográfico. QKD y PQC abordan diferentes aspectos de la seguridad criptográfica:

- QKD: Su objetivo principal es la distribución de claves simétricas, funcionando como un *Mecanismo de Intercambio de Claves* (KEM). Los protocolos QKD puros, como BB84, carecen de autenticación nativa, lo que los hace *vulnerables a ataques MITM* si no se complementan con otros mecanismos.
- PQC: Los algoritmos PQC están diseñados para reemplazar los algoritmos criptográficos asimétricos clásicos vulnerables (como RSA y ECC). Esto incluye soluciones resistentes a la cuántica para el intercambio de claves (KEM, ej. CRYSTALS-Kyber), el cifrado y crucialmente, las firmas digitales (autenticación, ej. CRYSTALS-Dilithium).

- Complementariedad: La Arquitectura Híbrida QKD+PQC. La tendencia actual y la práctica recomendada para la seguridad post-cuántica y cuántica es *combinar* QKD y PQC en arquitecturas híbridas. Esta sinergia se justifica al compensar las debilidades de cada tecnología.

- Rol de QKD: *Seguridad Incondicional y Anti-HNDL*. El principal valor de QKD en una arquitectura híbrida es proporcionar seguridad incondicional a largo plazo.

- *Neutralización de HNDL*: El QKD es la solución definitiva contra el ataque HNDL, donde los atacantes roban datos cifrados hoy para descifrarlos en el futuro con un CRQC. Dado que la clave QKD se genera y distribuye basándose en la física (imposibilidad de clonación) y se desecha si se detecta intrusión, el material de clave robado carecerá del secreto incondicional necesario para el descifrado futuro.

- *Generación de Claves Simétricas Maestras:* QKD se utiliza para generar la clave simétrica maestra que alimenta algoritmos robustos como AES-256. Al combinar la clave simétrica QKD con una clave PQC, el secreto final está protegido por dos suposiciones independientes.
- Rol de PQC: *Autenticación y Cobertura Lógica.* El principal rol de PQC es cerrar la vulnerabilidad de autenticación de QKD y proporcionar resistencia lógica y *escalable*.
 - *Autenticación Robusta:* La PQC (especialmente algoritmos de firma digital como CRYSTALS-Dilithium) se utiliza para autenticar el canal de comunicación clásico necesario para el post-procesado de QKD. Esto *mitiga los ataques MITM* que el QKD puro no puede prevenir, ya que estos ataques solo ocurren en el momento de la conexión.
 - *Criptoagilidad y Redundancia:* PQC proporciona criptoagilidad (la capacidad de cambiar rápidamente los algoritmos criptográficos en caso de compromiso). En un modelo híbrido, si el componente QKD falla temporalmente, el cifrado puede conmutar a PQC puro como respaldo.
 - *Transición Pragmática:* PQC permite una transición *inmediata y masiva*. Es la opción para *tramos amplios o menos críticos*, mientras que el costoso hardware QKD se limita a los enlaces críticos de alto valor (ej., centros de datos o defensa) donde el riesgo HNDL es inaceptable.
- Mecanismos Híbridos. La clave híbrida (que utiliza tanto QKD como PQC) se considera el estándar durante el período de transición.
 - *Doble Blindaje:* Las claves híbridas proporcionan una *capa adicional de seguridad*. Para romper la clave final, un atacante debe comprometer simultáneamente la capa física (QKD) y la capa matemática (PQC).
 - *Métodos de Combinación:* Las claves generadas por QKD y los secretos derivados de Mecanismos de Encapsulación de Clave (KEM) PQC (como CRYSTALS-Kyber) *pueden combinarse mediante operaciones de Concatenación o Exclusively-OR (XOR)* para formar el secreto maestro o *premaster secret*.
- Implicaciones y Casos de Uso. La elección entre QKD y PQC, o su combinación, *depende de la criticidad de los datos, la vida útil esperada del secreto y las restricciones operativas*.
 - Resistencia al Ataque HNDL. La amenaza HNDL es inmediata para los datos de larga duración.
 - La QKD ofrece *la máxima protección* posible contra HNDL, ya que la seguridad incondicional se mantiene independientemente de los avances tecnológicos futuros.
 - La PQC ofrece *resistencia a la recopilación* al reemplazar los algoritmos asimétricos vulnerables al algoritmo de Shor. Sin embargo, si se rompe el supuesto matemático, el secreto puede verse comprometido.
 - El diseño híbrido (QKD + PQC) es crucial en entornos como la Defensa o la Administración Pública, donde la *información mantiene su valor operativo durante décadas*.
 - Estandarización e Integración Práctica
 - La PQC ha avanzado rápidamente en la estandarización mediante el NIST, que ha publicado estándares como ML-KEM (Kyber) y ML-DSA (Dilithium). Esta estandarización facilita su integración en protocolos existentes.
 - La integración de QKD con la infraestructura clásica se gestiona a menudo mediante *interfaces estandarizadas* como la *API ETSI-QKD*, lo que permite inyectar la clave cuántica

en cifradores simétricos estándar (como AES-256) que ya son robustos frente a los ataques conocidos de Grover.

- *VPN IKEv2 Resistente a la Cuántica*: Los estándares *RFC 8784*, *RFC 9242* y *RFC 9370* permiten la creación de VPN IKEv2 resistentes a la cuántica mediante claves híbridas que combinan Mecanismos de Intercambio de Claves (KEM) clásicos y PQC (p.ej., Diffie-Hellman + Kyber). Estos marcos son esenciales durante la transición post-cuántica.
- *Limitaciones en la Adopción*. Los desafíos prácticos a menudo impulsan el uso complementario de ambas tecnologías.

Desafío Principal	QKD	PQC
Costo / Implementación	Requiere <i>hardware especializado</i> y personal altamente calificado, resultando en un <i>CAPEX y OPEX altos</i> .	Se implementa por <i>software</i> sobre infraestructura existente, con un <i>coste inicial bajo</i> .
Escalabilidad / Distancia	<i>Limitado</i> por la atenuación óptica a cortas distancias (generalmente <100 km) sin repetidores cuánticos.	Puede implementarse a <i>cualquier distancia</i> utilizando la infraestructura de red clásica.
Seguridad de la Implementación	Teóricamente seguro, pero las implementaciones prácticas son vulnerables a <i>ataques dirigidos al hardware</i> (ej., ataques PNS o ataques al detector), lo que exige protocolos avanzados como MDI-QKD o SARG04.	Su seguridad es <i>matemática</i> . Los desafíos se centran en el rendimiento del software (tamaño de clave/latencia) y en la agilidad criptográfica ante posibles vulnerabilidades teóricas futuras.

Tabla 3-5. Complementariedad entre QKD y PQC (Adaptada de NTB LM)

3.3 Síntesis comparativa y Matriz de decisión

- Síntesis Comparativa:

La siguiente tabla y figura ofrecen un resumen de alto nivel de comparativa entre PQC, QKD y la opción híbrida PQC+QKD, diseñado para facilitar la toma de decisiones ejecutivas.

Criterio	Solo PQC (Kyber/Dilithium)	Solo QKD (BB84/MDI-QKD)	Híbrido QKD + PQC
Fundamento de Seguridad	Problemas matemáticos computacionalmente difíciles (lattice-based)	Leyes fundamentales de física cuántica (no-clonación, incertidumbre)	Combinación: Física cuántica (QKD) + Matemática (PQC)
Protección HNDL	Media: Protege contra QC conocidos, pero vulnerable a futuros avances	Muy Alta: Seguridad incondicional independiente de avances futuros	Muy Alta: Doble capa de protección, máxima resiliencia
Garantía de Seguridad a Largo Plazo	Moderada: Depende de suposiciones matemáticas no probadas	Máxima: Seguridad teóricamente incondicional probada	Máxima: Combina incondicionalidad QKD con redundancia PQC
Detección de Interceptación	No: Sin capacidad de detección intrínseca	Sí: Detección garantizada de cualquier interceptación	Sí: QKD proporciona detección de interceptación
Resistencia a Computación Cuántica	Alta: Resistente a algoritmos cuánticos conocidos (Shor, Grover)	Absoluta: Inmune a cualquier computadora cuántica	Absoluta: Protección multicapa contra todas las amenazas
Tiempo de	3-6 meses	18-24 meses	12-18 meses

COMUNICACIONES CUÁNTICAS SEGURAS: HOJA DE RUTA DE APLICACIONES HÍBRIDAS:
QKD+PQC

Implementación			
Complejidad de Despliegue	Baja: Similar a despliegue criptográfico tradicional (software)	Muy Alta: Requiere instalación de hardware cuántico especializado	Media-Alta: Integración de dos tecnologías complementarias
Requisitos de Infraestructura	Mínimos: Usa infraestructura estándar	Extensivos: Fibra dedicada, entornos controlados, estabilización	Moderados: Combina requisitos de ambas tecnologías
Compatibilidad con Redes Existentes	Excelente: Reemplazo directo (Drop-in replacement) para algoritmos clásicos	Limitada: Requiere canales dedicados o WDM con filtrado	Buena: PQC mantiene compatibilidad, QKD en canales específicos
Rendimiento (Tasa de Clave/ Throughput (rendimiento))	Muy Alto: >1 Gbps sin degradación significativa	Bajo-Medio: 1-100 kbps (tasa de clave secreta)	Alto: 100 Mbps - 1 Gbps (limitado por QKD, pero optimizado)
Escalabilidad y Coste	Alta escalabilidad, coste moderado. Solo software.	Baja escalabilidad, coste muy elevado. Limitada por la distancia y el hardware especializado.	Buena, flexible según criticidad. El más elevado al confluir 2 tecnologías
Autenticidad	Integrada: Ofrece autenticación y firmas digitales de forma nativa.	No integrada: Requiere un canal clásico autenticado, a menudo usando PQC.	Aportada por PQC
Recomendación de Agencias e industria	Recomendada como estándar principal por agencias como NIST (EE. UU.), NSA y ANSSI (Francia) para la migración general.	<i>No recomendada para uso general. Considerada una tecnología de nicho para aplicaciones especializadas.</i>	La tendencia está convergiendo hacia modelos híbridos como estándar de facto para aplic. críticas, con PQC como base universal y QKD como capa adicional para enlaces de máxima seg.

Tabla 3-6. Síntesis comparativa entre opciones: PQC, QKD, Híbrida PQC+QKD (Adaptado de NTB LM)

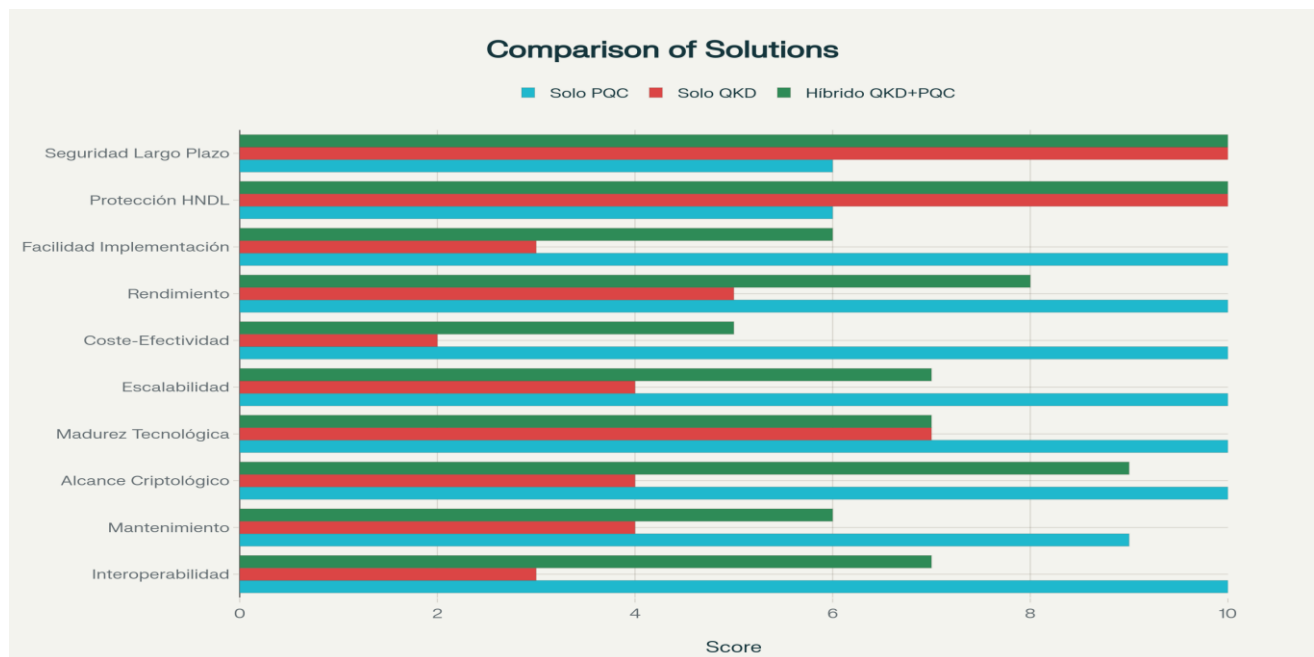


Figura 3-1. Comparativa de PQC vs QKD vs Híbrido en 10 Criterios Clave (Esc. 1-10) (Adaptado de Perplexity)

Sustentado en esta comparativa de decisión multicriterio la puntuación Total según solución adoptada es:

- Solo PQC: 91/100
- Solo QKD: 52/100
- Híbrido QKD+PQC: 75/100

Observaciones Clave a resaltar de la figura 3-1:

- Criterios donde PQC destaca: Facilidad de Implementación, Rendimiento, Coste-Efectividad, Escalabilidad, Alcance Criptológico, Interoperabilidad - claramente superior en aspectos prácticos y operativos.
- Criterios donde QKD se posiciona mejor: Seguridad a Largo Plazo y Protección HNDL, alcanzando puntuación máxima (10) pero con desventajas significativas en implementación y costes.
- Criterios donde el Híbrido muestra equilibrio: Protección HNDL (10), Rendimiento mejorado (8), Alcance Criptológico (9) - combinando las fortalezas de ambas tecnologías con compromisos aceptables en implementación.

3.4 Conclusión y Perspectiva Estratégica en PQC y QKD

La elección entre PQC y QKD no es una decisión de una talla para todos. Se trata, más bien, de una *evaluación estratégica que debe equilibrar el nivel de seguridad deseado, la viabilidad práctica, el coste de implementación y el perfil de riesgo específico de cada organización y caso de uso*. Surgiendo la posibilidad de la integración híbrida como tendencia actual. La seguridad criptográfica del futuro no será definida por una única tecnología, sino por la integración inteligente y adaptativa de soluciones (*criptoagilidad*). Tanto PQC como QKD tienen roles esenciales, pero diferenciados, en la mitigación de las amenazas cuánticas.

El análisis comparativo conduce a una conclusión clara sobre el posicionamiento estratégico de cada tecnología:

- La **PQC** se establece como la ***solución prioritaria inmediata, pragmática, escalable y fundamental para la próxima era de la seguridad digital y es un imperativo de seguridad actual***. Designada por organismos de estandarización globales como el NIST y respaldada por agencias de ciberseguridad como la NSA y ANSSI, la PQC representa el camino principal y *más viable para la migración criptográfica a gran escala*. El foco debe estar en la auditoría y el reemplazo de los algoritmos de clave pública (RSA/ECC) utilizados en funciones de KEM y DSA, especialmente en certificados X.509, TLS y VPN. Su naturaleza basada en software permite su integración en la vasta mayoría de las aplicaciones existentes, desde la seguridad de Internet y las transacciones financieras hasta la del sector salud
- La **QKD** debe reservarse para aplicaciones ***de muy alto valor, de misión crítica y de corto alcance***, donde el coste de implementación se justifica por la necesidad de una garantía de seguridad física incondicional. Tiene que ser vista como una *tecnología complementaria y de nicho*. Ofrece el más alto nivel teórico de confidencialidad para la distribución de claves, una garantía anclada en las leyes de la física. Sin embargo, sus significativas limitaciones prácticas como distancia, coste, dependencia de infraestructura dedicada y la necesidad de una autenticación externa, la restringen a *escenarios muy específicos*. Su aplicabilidad se centra en la *protección de enlaces punto a punto de altísimo valor* (por ejemplo, entre centros de datos gubernamentales o infraestructuras críticas) o en *redes metropolitanas donde el despliegue de fibra dedicada y nodos de confianza es factible*.

- *Sinergia QKD+PQC*: QKD ofrece la máxima garantía de seguridad (incondicional), lo que la convierte en el blindaje definitivo contra la amenaza HNDL. Sin embargo, PQC es esencial para la autenticación del canal clásico y proporciona una solución escalable y práctica a corto plazo para la migración de toda la infraestructura digital. La arquitectura híbrida QKD+PQC *aprovecha lo mejor de ambos mundos, proporcionando defensa en profundidad mediante redundancia física y matemática*
- *Fomento de la Criptoagilidad*: La estrategia a largo plazo debe ser adaptable. La coexistencia de QKD y PQC en un mosaico híbrido, junto con la capacidad de cambiar rápidamente los algoritmos, será fundamental para proteger la privacidad y la confidencialidad en la inminente era cuántica.

En definitiva, una estrategia de seguridad cuántica madura y con visión de futuro debe priorizar una *transición ordenada y completa hacia los estándares de PQC. Simultáneamente, las organizaciones con requisitos de seguridad excepcionales deben evaluar la estrategia QKD+pqc para casos de uso altamente especializados*, donde sus beneficios únicos en confidencialidad de claves puedan justificar sus considerables desafíos de implementación.

Para concluir, una *propuesta de arquitectura híbrida típica sería*:

- *PQC para autenticación*: Algoritmos como ML-DSA (CRYSTALS-Dilithium) proporcionan firmas digitales resistentes a ataques cuánticos. Esto garantiza que el eslabón de la autenticación en el sistema QKD sea también resistente a Shor y resuelve la vulnerabilidad MITM de la QKD.
- *QKD para generación de claves de cifrado*: Genera claves simétricas con seguridad teórica. O bien, los protocolos híbridos QKD+PQC pueden generar una clave de sesión combinada, donde el secreto compartido es la unión de la clave PQC (generada por ML-KEM) y la clave QKD (generada físicamente). Para que un atacante comprometa el secreto, requeriría romper simultáneamente la complejidad matemática del PQC y la seguridad física incondicional del QKD. Esto proporciona una capa de seguridad superior, mitigando el riesgo de que una de las tecnologías falle o tenga vulnerabilidades inesperadas. Proporciona seguridad contra HNDL
- *AES para cifrado de datos*: Utiliza las claves distribuidas por QKD para cifrado simétrico de alto rendimiento

La adopción de esta sinergia maximiza la resiliencia al proteger contra atacantes con capacidad computacional ilimitada (amenaza matemática, mitigada por PQC) y atacantes con capacidad de interceptación física del canal (amenaza física, mitigada por QKD).

Las ventajas que el enfoque híbrido genéricamente aportaría:

- *Redundancia de seguridad*: Fallo en un componente no compromete el sistema completo
- *Flexibilidad operacional*: Adaptación automática a condiciones de red variables
- *Migración gradual*: Transición suave desde sistemas clásicos

4 ANÁLISIS DE VIABILIDAD EN SECTORES CRÍTICOS Y CASO DE USO SEDE-DELEGACIÓN

Las implementaciones en entornos institucionales y de defensa presentan requisitos únicos como confidencialidad de muy larga duración (+20 años), resistencia a actores estatales y alta disponibilidad. Estos influyen significativamente en la selección tecnológica. Los casos de uso documentados incluyen comunicaciones seguras de mando, control, comunicaciones y cómputo (C4) para sistemas de campo de batalla de próxima generación, es decir, información clasificada (*secreto*).

4.1 Factores a analizar

4.1.1 Requisitos Críticos

- *Seguridad:*
 - Blindaje físico incondicional anti-HNDL. Resistencia demostrable contra ataques cuánticos y clásicos durante más de 20 años
 - Protocolos de autenticación robustos (certificación Common Criteria *EAL4+)
 - Mecanismos de detección de intrusión en tiempo real.
 - *Criptoagilidad:* Capacidad de cambiar rápidamente entre algoritmos criptográficos en caso de que se descubran vulnerabilidades

*EAL 4+ es un **certificado de seguridad de alto nivel** que asegura que un producto de TI ha pasado por un proceso de evaluación riguroso y metódico por parte de un laboratorio independiente, demostrando una seguridad robusta y fiable, a menudo requerida para licitaciones de agencias públicas o clientes importantes (como bancos u operadores de telecomunicaciones).

- *Rendimiento:*
 - *Tasas de clave secreta:* Mínimo 1 Mbps para aplicaciones críticas
 - *Latencia:* <100 ms para señalización, <10 ms para datos críticos
 - *Disponibilidad:* 99.9% uptime (activo), con redundancia automática
 - *Escalabilidad:* Soporte para +100 nodos
 - *Mantenimiento:* Personal especializado disponible

- Interoperabilidad:

- Compatibilidad con la infraestructura clásica existente (WDM, Fibra monomodo) y con estándares ETSI QKD 014
- Integración con IPsec y TLS/SSL existentes
- APIs estandarizadas para gestión de claves
- Integración con sistemas PKI existentes

4.1.2 Limitaciones Operacionales

- *Técnicas:*
 - *Distancia:* Limitado a redes metropolitanas, a aproximadamente 100 km sin repetidores cuánticos.
 - *Throughput o rendimiento (Tasa de transferencia de datos en una red):* 3-4 órdenes de magnitud menor que comunicaciones clásicas
 - *Condiciones ambientales:* Sensibilidad a vibración, temperatura, interferencias electromagnéticas, ruido y atenuación, lo que puede afectar a la SKR y al QBER.
 - *Disponibilidad:* Pocos proveedores comerciales maduros
 - *Vulnerabilidades Prácticas:* Aunque teóricamente inquebrantable, las implementaciones reales de QKD son vulnerables a ataques dirigidos al *hardware* (ACL de timing y análisis de potencia, DoS, ataques PNS o ataques al detector), lo que exige protocolos avanzados como SARG04 o MDI-QKD. Se amplía información en Anexo VI: Los SLA en la QKD
 - *Expertos:* Escasez crítica de personal cualificado.
- *Económicas:*
 - *CAPEX inicial:* 100-500 K€ por enlace punto a punto. Alto coste del HW cuántico especializado para QKD. En contraste, las implementaciones PQC pueden realizarse con inversiones iniciales de 20-100K€ y costes operacionales anuales de 10-50K€.
 - *OPEX anual:* 15- 25% del CAPEX para mantenimiento especializado intensivo en QKD. En contraste, las implementaciones PQC pueden realizarse con un 20% del CAPEX para mantenimiento.
 - *Dependencia de Talento:* La escasez de personal cualificado en física cuántica aplicada y gestión de redes QKD es un riesgo que puede comprometer la operación y el mantenimiento.
 - *Volumen de Pedidos (Defensa):* Los volúmenes de pedidos de defensa suelen ser significativamente *menores que los del sector civil*, lo que relega a los programas de defensa a una posición trasera en la cadena de suministro, afectando el acceso a tecnologías maduras
- *Regulatorias:*
 - Falta de estándares de certificación específicos para aplicaciones clasificadas
 - Restricciones de exportación para tecnologías cuánticas avanzadas
 - Cumplimiento con normativas de telecomunicaciones nacionales

4.1.3 Riesgos y Dependencias Críticas

- *Riesgos Tecnológicos*
 - *Obsolescencia temprana:* Medio. Rápida evolución tecnológica puede hacer obsoletos sistemas desplegados
 - *Vulnerabilidades de implementación:* Medio. Gap entre seguridad teórica y práctica.

- *Dependencia de proveedores*: Alto. Ecosistema limitado de fabricantes especializados.
- *Operacional*: Alto. Complejidad de mantenimiento.
- *Técnico*: Alto. Tecnología aún en desarrollo

- *Dependencias de Infraestructura*

- *Fibra óptica dedicada*: Requerimiento de dark fiber (fibra oscura) o WDM cuidadosamente diseñada.
- *Sincronización temporal*: Necesidad de referencia GPS para aplicaciones distribuidas
- *Alimentación estable*: Sistemas UPS (SAI) dimensionados para equipamiento criogénico

4.1.4 Mitigaciones Propuestas

- *Diversificación tecnológica*:

- Implementación de múltiples protocolos QKD en paralelo
- Integración con PQC como fallback automático
- Contratos multi-vendor para evitar lock-in
- Auditoría criptográfica completa.

- *Redundancia de infraestructura*:

- Rutas de fibra diversificadas geográficamente
- Sistemas de backup power con autonomía >24h
- Centros de operación de red (NOC) distribuidos

- *Interoperabilidad*:

- Compatibilidad con estándares ETSI QKD 014
- Integración con IPsec y TLS/SSL existentes
- APIs estandarizadas para gestión de claves

4.2 Caso de uso: Enlace Sede-Delegación

Se evalúa la implementación de seguridad cuántica en un enlace de comunicaciones críticas entre una sede central y una delegación, considerando tres escenarios: Solo PQC, Solo QKD y Híbrido QKD+PQC. El enlace maneja información crítica de confidencialidad de larga duración, por lo que la amenaza HNDL es el principal impulsor de la migración. **Remarcar que los cálculos numéricos plasmado en este trabajo son estimativos y han tenido como referente las estrategias nacionales de España (2025), Canadá (2023) y Reino Unido (2023). Han sido adaptados según este contexto específico de implementación** (Gobierno de España, 2025; Gobierno de Canadá, 2023; Gobierno del Reino Unido, 2023).

El método de extrapolación usado para estimar los costes están basados en precios de mercado de ID Quantique/Toshiba.

4.2.1 Escenario de Implementación

Contexto Operacional:

- Distancia: 100 km entre sede central y delegación regional

- Infraestructura: Fibra óptica monomodo existente G.652.D (que es un estándar robusto y versátil que sigue siendo la base de la infraestructura de fibra óptica a nivel mundial debido a su excelente rendimiento en un amplio rango de longitudes de onda y su compatibilidad con equipos existentes).
- Tráfico de datos: 500 GB/día de información clasificada y de 10 Mbps para datos operacionales
- Requisitos de seguridad: Nivel SECRETO, retención 25 años. Luego criticidad alta (información muy sensible y regulación estricta, p. ej., registros sanitarios, I+D, finanzas).
- Cifradores de red AES-256/GCM con KMS corporativo; objetivo de rotación de claves de sesión < 1 minuto sin aumentar latencia de datos.
- Requisito de defensa frente a HNDL a largo plazo.
- Disponibilidad: 99.5% anual requerida

4.2.2 Escenario A: Solo PQC

La implementación exclusiva de criptografía post-cuántica utilizando algoritmos estandarizados por NIST proporciona una solución inmediatamente desplegable para protección contra amenazas cuánticas futuras. Se utilizaría infraestructura IP existente con actualizaciones de software y posibles mejoras de hardware para aceleración criptográfica

- Arquitectura Técnica.

Algoritmos Seleccionados:

- Intercambio y encapsulación de claves: ML-KEM-768 (Kyber)
 - Tamaño clave pública: 1,184 bytes
 - Tamaño texto cifrado (ciphertext): 1,088 bytes
 - Seguridad: Nivel NIST 3 (~192 bits AES equivalente)
- Firmas digitales: ML-DSA-65 (Dilithium) (FIPS-204)
 - Tamaño clave pública: 1,952 bytes
 - Tamaño firma: 3,309 bytes promedio
 - Velocidad de verificación: ~1.500 ops/seg
 - SLH-DSA (SPHINCS+): Firma de respaldo basada en hash (FIPS-205)

Implementación:

- Cifrado de sesión: AES-256-GCM con claves derivadas de ML-KEM
- Autenticación: ML-DSA para todos los handshakes
- PKI: Certificados X.509 híbridos (RSA+Dilithium durante transición)
- Integración transparente en TLS/IPsec/MACsec.
- Protocolos: TLS 1.3 con extensiones PQC.

Infraestructura:

- Servidores TLS 1.3 con soporte PQC
 - HSMs (Hardware Security Modules) certificados FIPS 140-2 Nivel 3
 - VPN IPsec con algoritmos post-cuánticos
- Análisis de Rendimiento

Rendimiento de Red:

- Latencia adicional: ~5-15 ms por handshake debido a tamaños de clave mayores. El total <50 ms (similar a criptografía clásica actual)
 - Ancho de banda: Incremento 15-30% en overhead de protocolo
 - Throughput: 1-10 Gbps (limitado por ancho de banda, no por criptografía). Sin degradación significativa en transferencia de datos
 - CPU: Aumento 10-20% en carga computacional
 - Disponibilidad: 99.95% (utiliza infraestructura de red existente)
 - Incremento en tamaño de claves y firmas que requieren consideración en protocolos de red
- Costos de Implementación: (5 años)

Componentes	Año 1	Años 2-5	Total
Licencias software	75 k €	30 k/año €	195 k €
Hardware/HSM	40 k €	10 k/año €	80 k €
Certificación	25 k €	5 k/año €	45 k €
Personal/Training	30 k €	15 k/año €	90 k €
TOTAL	170 k €	60 k/año €	410 k €

Tabla 4-1. Costos de Implementación PQC (Adaptado de Fuente propia)

- Costes y O&M: bajo CAPEX incremental (software/firmware, HSMs crypto-ágiles), alto esfuerzo de inventario y migración plurianual.
 - ROI: 2-3 años
- Evaluación de Seguridad

Fortalezas:

- Resistencia cuántica: Basado en problemas de lattice, considerado seguro contra CRQC
- Madurez estándar: Algoritmos estandarizados por NIST (2024)
- Interoperabilidad: Compatible con protocolos estándar y con sistemas legacy mediante túneles híbridos.
- Implementación inmediata en hardware existente.
- Escalabilidad: Fácil despliegue en múltiples ubicaciones mediante infraestructura PKI establecida

Vulnerabilidades:

- Supuestos matemáticos: Seguridad basada en dificultad de problemas de retículos
- Ataques de Canal Laterales: Susceptible a timing attacks y power analysis (ACL)
- No genera entropía física continua como servicio.
- Amenaza HNDL: Sin protección retrospectiva si PQC es comprometido
- Criptoanálisis futuro: Posibles mejoras en algoritmos de ataque.

- Las implementaciones PQC introducen overhead computacional del 10-15% comparado con algoritmos clásicos.
- Tamaños de clave: Incremento 2-10x vs RSA/ECC (ML-KEM-768: 1184 bytes vs RSA-2048: 256 bytes)

Conclusión: Bajo coste, alta escalabilidad y no ofrece garantías físicas contra HNDL. Adecuado para información sensible de vida media, pero insuficiente para secretos de estado críticos a largo plazo.

4.2.3 Escenario B: Solo QKD

La implementación exclusiva de QKD mediante protocolo BB84 proporciona seguridad incondicional demostrada, pero presenta vulnerabilidades operacionales (mantenimiento especializado, personal técnico cuántico y consumibles específicos) significativas que requieren mitigación cuidadosa

- **Arquitectura Técnica**

Sistema QKD Seleccionado:

- Protocolo: BB84 con fuentes láser débiles, detección de avalancha de silicio, procesamiento clásico mediante canales autenticados independientes y con estado de señuelo (decoy states)
- Longitud de onda: 1550 nm (banda C)
- Hardware: Sistema comercial ID Quantique Cerberis3
- Tasa nominal: 10 kbps por 100 km
- QBER objetivo: < 5%

Infraestructura:

- Fibra óptica dedicada: Canal fibra oscura dedicado para QKD
- Sincronización: GPS + sincronización óptica de respaldo
- Gestión de claves: QKD Key Management System (QKD-KMS)
- Cifrado: AES-256 con claves QKD

Equipamiento por nodo:

- Transmisor QKD: Láser pulsado + modulador electroóptico
- Receptor QKD: Detectores SNSPD criogénicos
- Sistema de control clásico: Procesamiento post-cuántico

- **Análisis de Rendimiento**

Rendimiento QKD:

- Aporta claves simétricas continuas (Kbit/s–Mbit/s según distancia y tecnología), integrables en cifradores AES para alta tasa de datos; latencia de datos independiente del proceso de clave.
- Tasa de clave secreta: ~2.5 kbps por 100 km (estimado)
- Eficiencia post-procesada: ~15% (tamizado + corrección errores + privacy amplification)
- Disponibilidad: 95-98% (afectado por condiciones ambientales)
- Generación diaria: ~21.6 MB de claves frescas
- Consumo de claves: 500 GB/día requiere ~64 MB claves pre-compartidas (AES-256) o PKI clásica (vulnerabilidad)
- Throughput: ~1 kbps tasa de clave secreta extremo a extremo

Análisis de Viabilidad:

- Déficit de claves: Insuficiente generación para requisitos de tráfico
 - Solución: Pre-posicionamiento de claves y key stretching con KDF (función derivada de clave)
 - Buffer de claves: Reserva de 30 días (~650 MB) para mantener operaciones
- Costos de Implementación (5 años)

Componentes	Año 1	Años 2-5	Total
Equipos QKD (2 nodos)	400 k €	20 k/año €	480 k €
Fibra dedicada	100 k €	10 k/año €	140 k €
Instalación/Comisionado	50 k €	-	50 k €
Mantenimiento especializado	-	80 k/año €	320 k €
Personal técnico cuántico	40 k €	80 k/año €	360 k €
TOTAL	590 k €	190 k/año €	1.350 k €

Tabla 4-2. Costos de Implementación QKD (Fuente propia)

- Costes y O&M: CAPEX medio–alto (módulos QKD, detectores, instalación), requisitos ambientales, soporte especializado; mitigable con coexistencia en fibra existente para reducir coste.
 - ROI: 4-7 años (solo activos críticos)
- Evaluación de Seguridad

Fortalezas:

- Seguridad incondicional: Basada en leyes de la física
- Detección de interceptación: Automática vía QBER monitoring
- Forward secrecy: Cada bit de clave es único e irrecuperable.
- Inmunidad cuántica: No afectado por algoritmos cuánticos

Vulnerabilidades Críticas:

- Distancia/atenuación, coexistencia WDM exige ingeniería, sensibilidad a temperatura/vibración, TRL alto, pero no universal.
- Autenticación inicial: Requiere canal autenticado clásico y este debe autenticarse mediante criptografía tradicional. Esta autenticación inicial típicamente utiliza claves pre-compartidas o certificados PKI, creando una dependencia circular (chicken-and-egg) donde la seguridad de QKD depende de métodos clásicos potencialmente vulnerables.
- MITM: Sin autenticación criptográfica del protocolo QKD. Sin autenticación robusta del canal clásico, adversarios pueden interceptar completamente la comunicación QKD estableciendo sesiones separadas con Alice y Bob.

- Ataques de implementación: Side-channel attacks (ACL) en hardware real como detector blinding, time-shift attacks, y photon-number-splitting. Para ampliar información ver anexo VI
- Requisitos de infraestructura dedicada que impiden integración transparente con redes existentes
- Disponibilidad: Vulnerable a DoS por interferencia del canal

Soluciones de Mitigación:

- Claves pre-compartidas: Para autenticación inicial (problemática a largo plazo)
- Protección física: Seguridad física estricta del canal de fibra
- Monitorización continua: Detección de anomalías en QBER y tasa de claves
- Backup links: Enlaces secundarios para redundancia

Conclusión: Excelente confidencialidad, pero operatividad y despliegue complejo y riesgos de disponibilidad (requiere autenticación inicial segura).

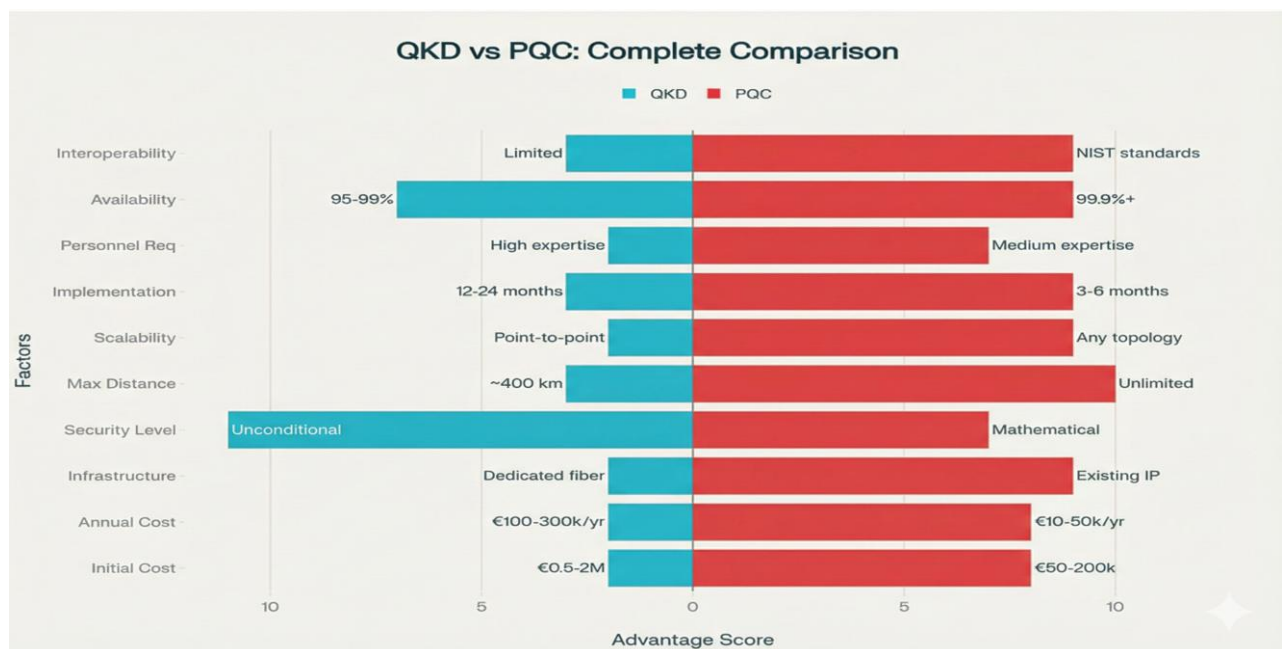


Figura 4-1. Comparativa QKD vs PQC para Enlace Sede-Delegación (Adaptado de Perplexity)

4.2.4 Escenario C: Sistema Híbrido (QKD+PQC)

La arquitectura híbrida representa la aproximación más robusta, combinando las fortalezas complementarias de QKD y PQC mientras se mitigan sus limitaciones individuales

- Arquitectura Sinérgica Integrada

Diseño de Sistema Híbrido:

- Capa de autenticación de canal: PQC (ML-DSA) autentica todas las comunicaciones clásicas, evita MITM
- Capa de generación de claves: QKD proporciona claves simétricas para cifrado de datos
- Capa de integración: Funciones de derivación de claves (HMAC-SHA3). Combinación criptográfica de claves QKD y PQC (XOR/KDF) para generar la clave maestra.
- Cifrado de datos: AES-256 con claves híbridas derivadas.
- Fallback automático: Conmutación a PQC puro si QKD falla

- Implementación de Protocolo Híbrido

Fase de Establecimiento (bootstrap):

1. Handshake PQC: Establecimiento de identidades y canal autenticado mediante certificados (ML-DSA)
2. Inicio QKD: Activación de generación de claves cuánticas con protocolo BB84 sobre canal autenticado, con verificación continua de QBER
3. Autenticación continua: PQC valida integridad del canal clásico QKD
4. Derivación híbrida: Generación de claves de sesión combinadas de claves QKD y PQC mediante XOR o funciones KDF robustas.

Operación Continua

- Renovación de claves: Cada 24 horas o 1 GB de datos transferidos
- QKD genera claves simétricas frescas cada 60 segundos
- Monitorización QKD: QBER < 5%, tasa umbral mínimo
- Validación PQC: Verificación firmas en mensajes de control QKD

Gestión de Fallos:

- Degradación automática a PQC si QBER > 15%
- Alertas de seguridad para intervención manual
- Recuperación automática cuando condiciones QKD se normalizan

- Análisis de Rendimiento Integrado

Métricas de Seguridad:

- Nivel de seguridad: Máximo de ambos sistemas
- Resistencia o resiliencia a HNDL: Protección completa incluso si PQC es comprometido en el futuro
- Detección de interceptación: Capacidades QKD mantenidas proporcionando forward secrecy perfecto.
- Autenticación robusta: PQC elimina vulnerabilidades MITM, eliminando la dependencia de claves precompartidas
- KMS capaz de integrar *aportes de entropía cuántica*. Estos sistemas, a menudo denominados Sistemas de Gestión de Claves Cuánticos (Q-KMS), están diseñados para aprovechar la aleatoriedad intrínseca de los fenómenos cuánticos para generar claves criptográficas de alta calidad y verdaderamente aleatorias. Estos son los *Generadores Cuánticos de Números Aleatorios* (QRNG). Para más información ver Anexo V: QRNG

Rendimiento Operacional:

- Latencia: Incremento mínimo (~2-3 ms) sobre solo PQC
- Throughput: Limitado por la menor tasa (QKD o PQC)
- Disponibilidad: 99.5% (degradación automática a solo PQC)
- Complejidad: Alta - requiere gestión coordinada de ambos sistemas
- Escalabilidad mejorada mediante infraestructura PKI-PQC para gestión de certificados
- Overhead adicional del 5-8% comparado con QKD puro debido a procesamiento PQC
- Mantenimiento de tasas de clave QKD nativas (sin degradación significativa)

- Costos del Sistema Híbrido (5 años)

Componente	Año 1	Años 2-5	Total
QKD Infraestructura			
Equipos QKD (2 endpoints)	400 k €	20 k/año €	500 k €
Fibra óptica (compartida)	50 k €	10 k/año €	90 k €
PQC Infraestructura			
Software/Licencias	50 k €	20 k/año €	130 k €
HSMs híbridos	75 k €	15 k/año €	135 k €
Integración y Soporte			
Desarrollo/Integración	150 k €	-	150 k €
Personal especializado	100 k €	120 k/año €	580 k €
Mantenimiento	-	80 k/año €	320 k €
TOTAL	825 k €	265 k/año €	1.885 k €

Tabla 4-3. Costes de Implementación del Sistema Híbrido QKD+PKC (Fuente propia)

- Costes: mayor CAPEX que solo PQC, pero focalizable en enlaces de alto valor; coexistencia en fibra reduce coste; OPEX mayor por O&M fotónico pero limitado al perímetro crítico.
- ROI y Justificación (en euros):
 - Valor de activos protegidos: 50M+ (información clasificada)
 - Costo de compromiso: 10M+ (estimación conservadora)
 - ROI de seguridad: Periodo de amortización de 5 a 7 años considerando riesgos mitigados
- Implementación Mediante Estándares
 - ETSI GS QKD 004: Interface estándar para integración de sistemas QKD en arquitecturas de red
 - NIST SP 800-56C: Directrices para derivación de claves híbridas combinando múltiples fuentes
 - RFC 8696: Especificación para algoritmos PQC en protocolos TLS/IPsec

Conclusión: Ofrece defensa en profundidad. Si la criptografía matemática falla (ruptura de PQC), la componente QKD protege los datos (inmunidad HNDL). Si el enlace QKD cae, el sistema puede degradar a modo PQC para mantener la disponibilidad. El modelo híbrido implica el coste más alto (suma de ambos), pero es el único que mitiga los riesgos existenciales de la Defensa.

4.2.5 Comparativa Exhaustiva de Escenarios

Matriz de evaluación

Criterio	Solo PQC	Solo QKD	Híbrido QKD+PQC
Seguridad a Corto Plazo (5 años)	★★★★☆	★★★★★	★★★★★
Seguridad a Largo Plazo (25 años)	★★★★☆☆	★★★★★	★★★★★
Resistencia HNDL	★★☆☆☆☆	★★★★★	★★★★★
Coste Inicial	★★★★★	★★☆☆☆☆	★★☆☆☆☆
Coste Operacional	★★★★☆	★★☆☆☆☆	★★☆☆☆☆
Complejidad Técnica	★★★★☆☆	★★★★☆☆	★★☆☆☆☆
Tiempo de Despliegue	★★★★★	★★☆☆☆☆	★★☆☆☆☆
Escalabilidad	★★★★★	★★☆☆☆☆	★★☆☆☆☆
Mantenimiento	★★★★★	★★☆☆☆☆	★★☆☆☆☆
Madurez Tecnológica (TRL)	★★★★☆	★★★★☆☆	★★★★☆☆
Disponibilidad de Proveedores	★★★★☆	★★☆☆☆☆	★★☆☆☆☆
*Complejidad operativa	★★★☆☆	★★★★★	★★★★☆
*Rendimiento (Throughput)	>1 Gbps	<1 Mbps	100 Mbps
*Latencia	<50 ms	<200 ms	<100 ms
*Disponibilidad del servicio	99.95%	95%	99.5%

Tabla 4-4. Comparativa según criterios (Adaptada de Perplexity)

* Bajo la premisa que la opción Híbrida solo se ejecutaría en el enlace principal y el resto iría en PQC. Por tanto, son *medias* de toda la infraestructura y estos parámetros se ven poco afectados al ser una parte proporcionalmente pequeña del conjunto

4.2.6 Recomendación y Justificación

Según la entidad de la empresa o administración y la sensibilidad y latencia de sus datos:

Escenario	Recomendación	Justificación
Empresa general / Cloud	Solo PQC	Coste-efectividad, facilidad despliegue, suficiente seguridad
Banca / Finanzas críticas	Híbrido QKD+PQC	Valor activo justifica inversión, cumplimiento regulatorio
Gobierno / Defensa nacional	Híbrido QKD+PQC	Máxima seguridad, inmunidad a amenazas estatales
Investigación / Academia	Solo PQC (general) / Híbrido (sensible)	Balance entre seguridad y presupuesto académico
Salud / Datos médicos largo plazo	Híbrido QKD+PQC	Protección datos 20-30 años, requisitos HNDL
IoT / Edge computing	Solo PQC	Limitaciones recursos, alto volumen dispositivos
Telecomunicaciones backbone	Híbrido QKD+PQC (core) / PQC (edge)	Enlaces críticos QKD, distribución masiva PQC
Infraestructuras críticas	Híbrido QKD+PQC	Seguridad incondicional para servicios esenciales
Startups / PyMEs (SMEs)	Solo PQC	Recursos limitados, prioridad time-to-market
Organizaciones internacionales	Híbrido QKD+PQC	Riesgos geopolíticos, requisitos multi-jurisdicción

Tabla 4-5. Recomendación y Justificación según Escenario (Adaptada de Perplexity)

Luego la recomendación para optar por una u otra tecnología quedaría:

- *Cuando elegir Solo PQC:*

- Empresas generales y entornos cloud
- Presupuestos limitados (<200 K €)
- Necesidad de despliegue rápido (3-6 meses)
- Alto volumen de transacciones
- Datos con vida útil <10 años
- IoT y edge computing

- *Cuando elegir Solo QKD:*

Raramente recomendado de forma aislada debido a:

- Vulnerabilidad MITM sin autenticación robusta
- Alcance criptológico limitado
- Costes muy elevados vs beneficio marginal sobre híbrido

- *Cuando elegir Híbrido QKD+PQC (RECOMENDADO):*

- Defensa y seguridad nacional
 - Infraestructuras críticas
 - Banca y finanzas de alto valor
 - Datos médicos con retención >20 años
 - Investigación sensible
 - Organizaciones con amenazas geopolíticas
 - Cumplimiento normativo estricto
 - Protección contra amenaza HNDL prioritaria
- Desde la perspectiva del tiempo a:
 - Corto plazo: Aconsejaría solo PQC ya que ofrece cobertura rápida, estandarizada y escalable para el conjunto de sistemas; recomendable como cimiento base organizativo.
 - Largo plazo y datos de alta vida útil: Aconsejaría un sistema híbrido QKD+PQC ya que representa la opción óptima, proporcionando seguridad robusta presente y futura, mitigando las vulnerabilidades individuales de cada tecnología y ofreciendo un equilibrio pragmático entre seguridad, coste y operatividad. Es preferible en enlaces críticos por seguridad informacional frente a HNDL y eliminación del eslabón débil de autenticación de QKD, ya que evita dependencia exclusiva de supuestos computacionales.
 - En función de las restricciones del escenario:

Escenario Operativo	Restricción Primaria	Tecnología Recomendada	Justificación Técnica y Estándar
Acceso Metro (< 20km)	Costo de fibra y hardware	CV-QKD (Homodino)	Permite usar componentes COTS de telecomunicaciones. Alta tasa de clave (>1 Mbps). Compatible con WDM.
Regional (< 80km)	Estabilidad / Fibra Compartida	DV-QKD (APD InGaAs)	Tecnología madura y estable. Tolerancia media a pérdidas (aprox. 20 dB). Compatible con ETSI 014.
Backbone (> 100km)	Distancia física / Atenuación	DV-QKD (SNSPD)	Detectores superconductores ofrecen la eficiencia necesaria para superar los 30 dB de pérdida. Costo elevado.
Interurb. (> 150km)	Límite físico de transmisión	Trusted Nodes (TN)+ QKD	Necesidad de repetidores de confianza (descifrado/recifrado) para extender el alcance más allá (Laudenbach et al., 2018).
Última Milla Móvil	Ausencia de fibra óptica	PQC (ML-KEM)	La QKD no es viable sin línea de vista o fibra. PQC en capa de aplicación es la única solución robusta.
Enlace Satelital	Cobertura global	Free-Space QKD	Emergente. Dependiente de condiciones atmosféricas y alineación óptica precisa.
Latencia Crítica	Tiempo de establecim.	Pre-Shared Key (QKD)	Elimina la latencia computacional del handshake asimétrico PQC. Ideal para HFT (High Frequency Trading).

Tabla 4-6. Según las restricciones del Escenario Operativo (Adaptada de NTB LM)

- *Justificación Estratégica genérica de la opción Híbrida QKD+PQC:*
 - Seguridad compuesta, máxima y robusta: Ofrece el mayor nivel de protección contra amenazas actuales y futuras, incluyendo HNDL.
 - Redundancia Crítica: Si cualquier tecnología es comprometida, la otra mantiene la seguridad

- Fiabilidad: Protección contra amenazas desconocidas y avances en criptoanálisis
- Complejidad operacional moderada con herramientas de gestión integradas
- Requisitos de formación extendidos, pero aprovechando sinergias tecnológicas
- Valor de activos: Los altos costos están justificados por el valor crítico de los activos protegidos
- Requisitos regulatorios: Cumple con estándares de seguridad más estrictos para información clasificada
- Costo-beneficio equilibrado: 25% más costoso que QKD puro, pero con seguridad superior a PQC solo
- Flexibilidad operacional que permite operación degradada durante mantenimiento
- Resiliencia operacional: Degradación elegante bajo condiciones adversas
- Preparación futura: Arquitectura lista para mejoras tecnológicas incrementales sin reemplazos completos de arquitectura, cryptoagilidad.

- **Implementación Recomendada:**

- Fase 1 (Años 1-2): Despliegue de PQC + diseño integración QKD
- Fase 2 (Años 2-3): Instalación y Pruebas sistema híbrido
- Fase 3 (Años 3-5): Operación completa y optimización continua

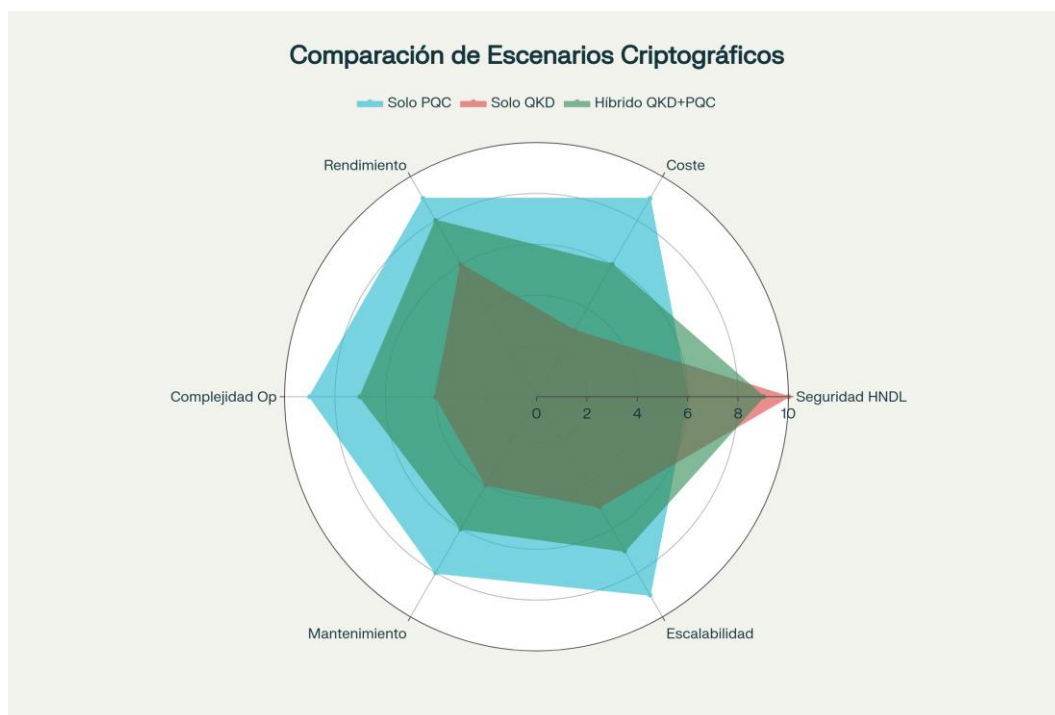


Figura 4-2. Comparativa PQC, QKD, Híbrido según métricas (Adaptada de Perplexity)

5 HOJA DE RUTA

La hoja de ruta se enfoca en la implementación práctica de un proyecto piloto híbrido QKD+PQC para el enlace sede-delegación en una organización gubernamental o de defensa, con extensión posterior a infraestructura crítica nacional. **Remarcar que los cálculos numéricos plasmado en este trabajo son estimativos y han tenido como referentes a las hojas de ruta nacionales (España, Canadá 2026–2035; UK 2026–2030). Han sido adaptados según este contexto específico de implementación** (Gobierno de España, 2025; Gobierno de Canadá, 2023; Gobierno del Reino Unido, 2023).

El método de extrapolación usado para estimar los costes en este capítulo están basados en precios de análisis comparativo de costes de mercado en licitaciones públicas de 2024-2025 y en tarifas medias de consultoría TIC en España.

5.1 Objetivo

Objetivo Primario:

Establecer un canal seguro híbrido para protección de datos de larga vida útil (defensa/sanitario/ financiero/ I+D), integrando KMS y cifradores AES existentes, de 80-100 km entre una sede central y delegación regional, con capacidad de 10 Mbps de datos cifrados y generación de 100 kbps de claves cuánticas

Objetivo Secundario:

- Minimizar la ventana de vulnerabilidad ante amenazas cuánticas
- Validación de integración QKD en redes DWDM (Multiplicación Densa por División de Longitud de Onda, Dense Wavelength Division Multiplexing) existentes
- Certificación de cumplimiento con estándares ETSI QKD y NIST PQC
- Desarrollo de competencias internas en tecnologías cuánticas
- Establecimiento de métricas de rendimiento y protocolos de mantenimiento

Métrica	Umbral de Aceptación	Descripción y Justificación
QBER (Quantum Bit Error Rate)	< 4% (DV-QKD)	Un QBER superior indica posible presencia de Eve (espía) o degradación severa de la fibra. El sistema debe abortar la generación de claves si se supera este umbral

		(Adnane & Potortì, 2023).
Tasa de Clave Secreta (SKR)	> 1 kbps (a 20dB)	Mínimo necesario para garantizar la rotación de claves sin agotar el buffer en escenarios de tráfico estándar.
Estado del Buffer KMS	> 1000 claves	El buffer nunca debe llegar a cero. Si ocurre, el sistema debe tener una política de fallback (PQC o PSK preestablecida) o bloquear el tráfico (Fail-Closed).
Latencia de Recuperación KMS	< 200 ms	Tiempo transcurrido desde que la SAE solicita la clave (GET_KEY) hasta que la recibe. Crítico para evitar timeouts en el protocolo IKEv2 (De Santis & Mancini, 2025).
Disponibilidad del Servicio	99.9%	A diferencia del 99.999% de telecomunicaciones, la tecnología QKD es sensible a calibraciones térmicas y mecánicas. Se debe planificar redundancia de enlaces.
Fugas de Canal Lateral	Indetectable	Verificado mediante pruebas de penetración óptica (ej. inyección de luz brillante) según ETSI GS QKD 016.

Tabla 5-1. Umbrales de aceptación operativa (Adaptada de NTB LM)

- Desarrollar un caso piloto replicable con capacidad de expansión futura

5.2 Planificación Estratégica por Fases

5.2.1 Año 1: Análisis y Diseño Fundamental (TRL 4-5)

Q1-Q2: Estudios de Viabilidad

- *Auditoría criptográfica completa*: Inventario de todos los sistemas que requieren actualización post-cuántica y análisis de dependencias (NIST, 2024) (World Journal of Advanced Research and Reviews, 2025).
- *Diseño de Arquitectura*: Definición de requisitos para el sistema híbrido, alineados con ETSI GS QKD 014 (API de entrega de claves) y ETSI GS QKD 004 (Interfaz de aplicación).
- *Análisis de infraestructura de fibra*: Evaluación de compatibilidad de fibra WDM existente con QKD (pérdidas, WDM, conectividad, atenuación, dispersión).
- Análisis de interferencias electromagnéticas y estabilidad ambiental
- Evaluación de puntos de conexión y requisitos de amplificación
- Selección de módulos QRNG
- *Evaluación y selección de proveedores*: RFP para sistemas QKD comerciales (ID Quantique, Toshiba, MagiQ) evaluando interoperabilidad con estándares ETSI.
Criterios de selección:
 - Madurez tecnológica ($TRL \geq 7$)
 - Soporte técnico local disponible
 - Hoja de ruta (Roadmap) de producto a 5 años
 - Certificaciones de seguridad
 - Prueba de Concepto: Testing de 30 días con 2 proveedores finalistas
 - Presupuesto: 150 K € para evaluación y PoC
- Presupuesto Q1-Q2: 200 K €
 - Consultoría especializada: 25 K €
 - Pruebas de fibra y equipos: 15 K €
 - Estudios de viabilidad: 5 K €

Q3-Q4: *Diseño de Arquitectura*

- *Diseño de red híbrida*: Especificaciones técnicas detalladas para integración QKD+PQC y con PKI existente
- Selección de algoritmos PQC: Implementación de ML-KEM, ML-DSA según estándares NIST
- Protocolos de integración: Desarrollo de APIs para interoperabilidad HSM-QKD Planificación de redundancia y procedimientos de contingencia (caída y recuperación)
- Especificación de interfaces con cifradores AES existentes
- Evaluación de riesgos de seguridad y análisis de amenazas específicas
- Desarrollo de políticas de gestión de claves híbridas
- Desarrollo de especificaciones de formación y certificación personal
- Plan de certificación: Preparación para evaluación Common Criteria
- Presupuesto Q3-Q4: 100 K €
 - Ingeniería de diseño: 60 K €
 - Documentación técnica: 30 K €
 - Especificaciones de formación: 10 K €

Entregables Año 1:

- Documentación de arquitectura técnica completa
- Plan de migración criptográfica
- Contratos firmados con proveedores principales
- Personal técnico contratado y entrenado

5.2.2 Año 2: *Implementación Piloto y pruebas (TRL 6-7)*

Los proyectos piloto permiten validación práctica de tecnologías seleccionadas en entornos controlados. La implementación debe incluir tanto soluciones QKD como PQC para permitir comparación directa de rendimiento, operatividad e integración con sistemas existentes. Los ambientes de prueba aislados minimizan riesgos operacionales mientras proporcionan datos de rendimiento realistas

Q1-Q2: *Adquisición e Instalación*

- Adquisición de equipos: 2 sistemas QKD punto a punto (endpoint) y componentes PQC
- Instalación y configuración de hardware en ambos extremos del enlace en laboratorio controlado
- Instalación de equipos en entornos controlados con estabilización ambiental
- Desarrollo de software: Middleware de integración QKD+PQC personalizados con sistemas AES
- Integración con multiplexores DWDM y sistemas de gestión de red
- Configuración inicial de software de gestión de claves (LKMS)
- Presupuesto: 320 K € Equipos QKD (2 unidades): 200 K €
 - Integración WDM: 60 K €
 - Software LKMS: 40 K €
 - Instalación profesional: 20 K €

Q3-Q4: *Pruebas y Validación*

- Testeado funcional: Verificación de tasas de clave secreta, QBER y disponibilidad

- Pruebas de integración: Interoperabilidad con sistemas legados
- Implementación de algoritmos de combinación de claves QKD+PQC
- Pruebas de compatibilidad y rendimiento inicial
- Medición de Indicador y Objetivo de Nivel de Servicio (SLI, SLO) de clave y disponibilidad
- Instalación de equipos en entornos controlados con estabilización ambiental
- Evaluación de seguridad: Pruebas de detección de intrusión, respuesta a fallos.
- Optimización de rendimiento: Desarrollo de procedimiento y parámetros operacionales
- Auditoría de seguridad física por terceros independientes
- Formación especializada de técnicos y operadores (40 horas/persona)
- Presupuesto: 150 K €

Métricas de Éxito y criterios de aceptación Año 2:

- Tasa de clave secreta: >1 kbps a 50 km. Como: Monitoreo continuo del sistema QKD. Cuando: Durante pruebas de carga
- QBER promedio: <3,5% bajo operación normal 24/7. Como: Monitoreo continuo del sistema QKD. Cuando: Semanalmente
- Disponibilidad sistema: >99,5% de operatividad del enlace QKD. Como: Logs del sistema. Cuando: Al final de la fase
- Disponibilidad del servicio E2E: >99,9% para el túnel IPsec aprovisionado con claves cuánticas
- Tiempo de conmutación a fallback: <30 segundos

5.2.3 Año 3: *Despliegue en Producción (TRL 7-8)*

La transición gradual comienza con enlaces y sistemas más críticos, aplicando lecciones aprendidas de proyectos piloto. La implementación prioriza sistemas con mayor exposición a riesgos cuánticos y valor operacional más alto. Los mecanismos de restauración (rollback) deben permanecer operacionales hasta que la estabilidad de nuevos sistemas esté completamente validada.

La integración con sistemas existentes presenta desafíos técnicos significativos. Los sistemas legados pueden requerir actualizaciones de middleware o gateways de protocolo para interoperar con tecnologías cuánticas. La planificación debe incluir ventanas de mantenimiento extendidas y procedimientos de emergencia para restauración rápida de servicios críticos.

Evaluación de seguridad conforme a perfiles de protección (ej. ETSI GS QKD 016) y normativas nacionales (CCN-STIC).

Q1-Q2: *Despliegue Inicial*

- Instalación en producción: Enlace sede-delegación principal
- Migración gradual: 20% del tráfico crítico inicialmente
- Monitorización 24/7: Establecimiento de NOC especializado
- Presupuesto: 400 K €

Q3-Q4: *Escalado y Optimización*

- Expansión de tráfico: Migración del 80% de comunicaciones sensibles.
- Ajuste fino de parámetros basado en datos operativos
- Actualización de protocolos y firmware
- Optimización de rendimiento y reducción de QBER
- Optimización operacional: Automatización de procesos de mantenimiento

- Formación de operadores: Certificación de personal técnico
- Automatización: Scripts de monitorización y alertas
- Procedimientos normalizados operativos (SOPs) completos para operación y mantenimiento
- Certificación final: Aprobación para uso con información clasificada
- Presupuesto: 200 K €

Métricas de Éxito y Criterios de aceptación:

- Escalabilidad del KMS y SDN probada con > 5 enlaces QKD
- Protocolo de respuesta a incidentes de QBER (>4%) probado con éxito en simulacros

5.2.4 Años 4-5: Consolidación y Expansión (TRL 8-9)

El despliegue completo extiende tecnologías cuánticas *a toda la infraestructura institucional*. Esta fase requiere coordinación cuidadosa para minimizar interrupciones operacionales mientras se asegura cobertura total. Los sistemas de monitorización deben proporcionar visibilidad completa del estado de migración y rendimiento de nuevas tecnologías.

La optimización continua, basada en métricas operacionales permite refinamiento de configuraciones y procedimientos. Los sistemas criptoagiles facilitan actualizaciones futuras y adaptación a evoluciones tecnológicas. El establecimiento de métricas de rendimiento de referencia es esencial para identificación temprana de degradaciones o problemas emergentes como implementación de orquestación definida por software (ETSI GS QKD 015/018) para gestión dinámica de claves.

La fase final establece operaciones sostenibles a largo plazo. El mantenimiento preventivo y actualizaciones regulares aseguran que sistemas permanezcan efectivos contra amenazas emergentes. La vigilancia tecnológica continua identifica desarrollos que puedan impactar seguridad o requerir modificaciones arquitectónicas.

Objetivos estratégicos:

- Expansión geográfica: Extensión a 5 sitios o enlaces institucionales críticos adicionales
- Integración completa: 100% del tráfico clasificado por QKD+PQC
- Métricas de rendimiento: KPIs establecidos y monitorizados
- Actualización tecnológica: Migración a protocolos de próxima generación
- Comercialización: Potencial oferta de servicios a tercero
- Integración con marcos normativos emergentes (EuroQCI, ETSI QT)
- Establecimiento como referencia nacional en QKDs

Presupuesto consolidado:

- Año 4: 600 K € (optimización)
- Año 5: 400 K € (expansión)

Presupuesto Estimado Quinquenal

Desglose por Categorías (en €)

Categoría	Año 1	Año 2	Año 3	Año 4	Año 5	Total
Hardware QKD	100K	400K	200K	300K	100K	1.100K
Software/PQC	50K	100K	50K	75K	50K	325K
Infraestructura	150K	50K	150K	100K	50K	500K
Personal	200K	150K	200K	250K	300K	1.100K
Operaciones	0K	50K	150K	200K	200K	600K
Contingencia (15%)	75K	113K	113K	139K	105K	545K
TOTAL ANUAL	575K	863K	863K	1.064K	805K	4.170K

Tabla 5-2. Presupuesto Quinquenal implementación QKD+ PQC (Fuente propia)

- CAPEx por enlace piloto: módulos QKD DV con decoy y detectores + instalación e ingeniería coexistencia WDM + integración KMS: rango bajo-medio de seis cifras por enlace, sensible a mercado y aranceles; coexistencia reduce necesidad de dark fiber; contemplar 15% de variación por cadena de suministro regional.
- OPEx: contratos de mantenimiento, calibración, soporte 24/7, auditorías, etc.

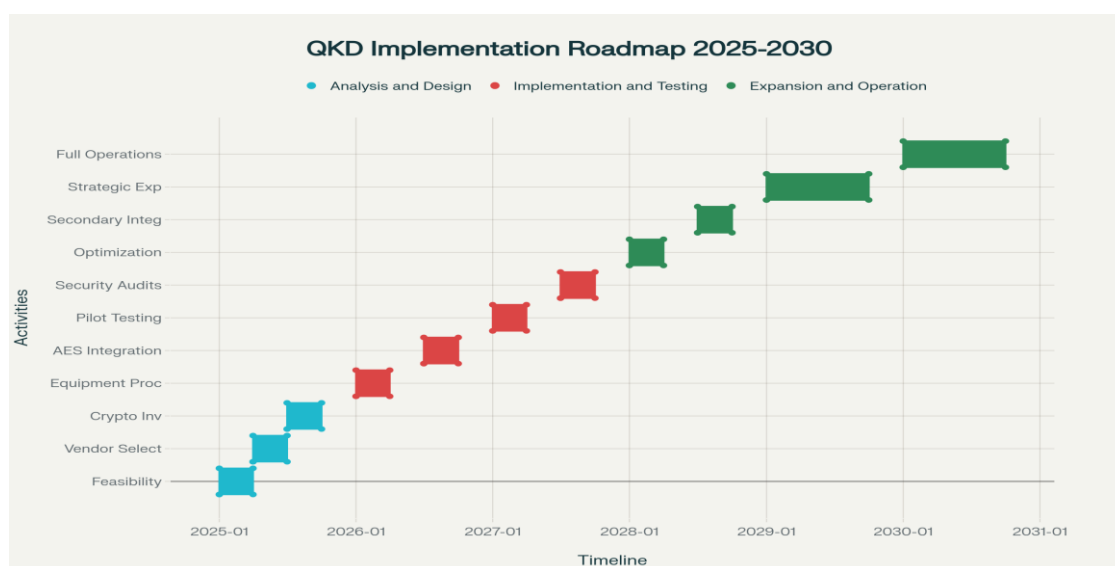


Figura 5-1. Hoja de Ruta para Adopción de Tecnologías Cuánticas (2025-2030) (Adaptada de Perplexity)

5.3 Fuentes de Financiación

Presupuesto institucional: 60% (2.500 K €)

- Fondos de modernización IT existentes
- Partidas específicas de ciberseguridad

Subvenciones públicas: 25% (1.040 K €)

- Programas nacionales cuántica/ciberseguridad
- Fondos europeos Programa Digital Europeo (EuroQCI, Digital Europe) y nacionales para I+D+i.

- Co-financiación privada: 15% (630 K €)
- Partnerships con proveedores tecnológicos
- Proyectos de I+D colaborativos

5.4 RRHH

5.4.1 Perfiles Profesionales Necesarios

Plantilla Técnica Especializada

Año 1-2: Equipo Central (4 FTE)

1. Ingeniero QKD (1 Full Time Equivalent (FTE) a tiempo completo)
 - Formación: Master en Física/Ingeniería + especialización cuántica
 - Experiencia: 3+ años en fotónica/óptica
 - Responsabilidades: Diseño y optimización de enlaces QKD
 - Salario: 80-100 K €
2. Criptógrafo Post-cuántico (1 FTE)
 - Formación: Doctor en Matemáticas/ Ciencias de la Computación
 - Especialización: Conocimiento profundo en algoritmos NIST
 - Responsabilidades: Implementación y validación PQC
 - Salario: 70-90 K €
3. Director de Proyecto (1 FTE)
 - Formación: Ingeniería Informática + certificaciones
 - Experiencia: 5+ años en sistemas críticos
 - Responsabilidades: Arquitectura híbrida QKD-PQC
 - Salario: 75-95 K €
4. Auditor de Seguridad (1 FTE)
 - Certificaciones: CISSP, CISM + formación cuántica
 - Experiencia: Auditorías de seguridad, cumplimiento (Compliance)
 - Responsabilidades: Monitorización 24/7, Evaluación continua de riesgos, respuesta a incidentes
 - Salario: 65-85 K €

Año 3-5: Técnico de Redes (+3 FTE)

- Operador NOC (Centro de Operaciones de Red) (2 FTE): Monitorización 24/7
- Ingeniero de redes (1 FTE): Mantenimiento especializado y experiencia en integración de sistemas críticos

5.4.2 Programa de Formación

Formación interna obligatoria:

- Fundamentos de Cuántica (40h): Principios de mecánica cuántica aplicada
- Implementación de PQC (60h): Algoritmos NIST y mejores prácticas

- Seguridad en las Operaciones (30h): Procedimientos específicos QKD+PQC

Certificaciones externas:

- Certified Quantum Network Professional (QNP)
- Post-Quantum Cryptography Specialist (PQCS)
- Quantum Security Analyst (QSA)

Presupuesto formación: 50 K €/año (250 K € total)

5.5 Gestión Integral de Riesgos

RP (primordial): Ataque con CRQC en día Q (*criptoapocalipsis*) HNDL

- Probabilidad: Alta (80%)
- Impacto: Muy Alto (exposición de datos sensibles)
- Mitigación:
 - Migración acelerada a proyectos piloto PQC+QKD.
 - Evaluación de la vida útil de los datos
 - Criptoagilidad

5.5.1 Riesgos Técnicos de Alto Impacto

R0: Autenticación del canal clásico (ataques MITM)

- Probabilidad: Alta (80%)
- Impacto: Alto (retraso 6-12 meses)
- Mitigación:
 - Firmas PQC en canal clásico de QKD.
 - Validación de identidad y registro de eventos.
 - Políticas de clave de anclaje

R1: Incompatibilidad de Estándares

- Probabilidad: Media (40%)
- Impacto: Alto (retraso 6-12 meses)
- Mitigación:
 - Selección de proveedores con cumplimiento en ETSI QKD 014
 - Pruebas de interoperabilidad tempranas
 - Contratos con cláusulas de evolución estándar

R2: Pruebas de QKD degradado

- Probabilidad: Alta (60%)
- Impacto: Medio (reducción 50% Throughput (velocidad efectiva de transmisión de información) esperado)
- Mitigación:
 - Arquitectura híbrida con fallback (plan de contingencia) automático a PQC

- Over-provisioning (sobre aprovisionamiento) de capacidad QKD (150% de requerimientos) para garantizar la seguridad o el rendimiento de red
- SLAs contractuales con penalizaciones por underperformance (bajo rendimiento)

R3: Dificultad de Integración en Redes WDM

- Probabilidad: Media (50%)
- Impacto: Alto
- Mitigación:
 - Reserva de canales dedicados para QKD (1310 nm o 1550 nm)
 - Implementación de filtros ópticos especializados
 - Segmentación de tráfico crítico vs. convencional
 - Desarrollo de interfaces de red híbridas
 - Segmentación espectral.
 - SLAs con operador
 - Pruebas de coexistencia con control de potencias y filtrado

R4: Sensibilidad Ambiental de Equipos

- Probabilidad: Media (50%)
- Impacto: Alto
- Mitigación:
 - Instalación en salas climatizadas con control de temperatura ($\pm 2^{\circ}\text{C}$)
 - Sistemas de monitorización continua (temperatura, humedad, vibraciones)
 - Aislamiento antivibratorio en equipos críticos
 - Contratos de mantenimiento preventivo especializados
 - Selección de rutas y fibra de baja pérdida.
 - Monitorización de QBER.
 - Política de fallback PQC

R5: Vulnerabilidades de Implementación

- Probabilidad: Media (35%)
- Impacto: Crítico (compromiso total de seguridad)
- Mitigación:
 - Auditorías de seguridad trimestrales por terceros
 - Implementación de controles compensatorios
 - Bug bounty program (programa de recompensas por errores) para identificación de vulnerabilidades

R6: Rendimiento insuficiente de QKD. Tasa de clave secreta inferior a requisitos operacionales

- Probabilidad: Media (30%)
- Impacto: Alto
- Mitigación:
 - Caracterización previa exhaustiva del canal
 - Sistemas QKD redundantes
 - Buffer de claves pre-generadas
 - SLA estrictos con proveedores

5.5.2 Riesgos Operacionales

R7: Escasez de Personal Cualificado

- Probabilidad: Alta (70%)
- Impacto: Alto (retrasos en implementación)
- Mitigación:
 - Partnerships con universidades para criaderos de talento
 - Programa de retención con incentivos competitivos
 - Externalización o subcontratación estratégica para funciones no principales

R8: Obsolescencia Tecnológica Acelerada

- Probabilidad: Media (45%)
- Impacto: Medio (necesidad de re-inversión temprana)
- Mitigación:
 - Arquitectura modular para permitir actualizaciones incrementales
 - Contratos de mantenimiento con programas de evolución
 - Reserva presupuestaria del 10% para actualizaciones anuales.
 - Participación en consorcios tecnológicos europeos

R9: Complejidad operacional excesiva. Dificultades en operación y mantenimiento diaria

- Probabilidad: Media (35%)
- Impacto: Medio
- Mitigación:
 - Automatización extensiva de operaciones
 - Monitorización proactiva y alertas
 - Procedimientos operacionales detallados
 - Contratos de soporte 24/7 con proveedores

5.5.3 Riesgos de Negocio

R10: Coste Elevado del Hardware QKD

- Probabilidad: Alta (80%)
- Impacto: Crítico
- Mitigación:
 - Negociación de contratos escalonados con proveedores
 - Financiación mediante fondos europeos (Digital Europe Programme, EuroQCI)
 - Implementación por fases priorizando enlaces más críticos
 - Evaluación ROI basada en valor de activos protegidos.
 - Múltiples proveedores.
 - Aprovechar infraestructuras existentes.
 - Financiación pública para innovación.

R11: Cambios Regulatorios

- Probabilidad: Media (50%)
- Impacto: Variable (compliance adicional)
- Mitigación:
 - Monitorizar activos de desarrollos regulatorios
 - Participación en comités de estandarización
 - Flexibilidad arquitectónica para adaptación

R12: Certificación y conformidad

- Probabilidad: Media (35%)
- Impacto: Variable
- Mitigación:
 - Ensayos contra side-channels y loopholes.
 - Adopción de guías de certificación.
 - pruebas de penetración periódica

R13: Disrupción de la cadena de suministros

- Probabilidad: Media (40%)
- Impacto: Alto (retrasos de 12-18 meses)
- Mitigación:
 - Diversificación de proveedores (mínimo 2 por componente crítico)
 - Inventario estratégico de componentes de larga entrega
 - Contratos con penalizaciones por incumplimiento

R14: Soporte técnico inadecuado. Soporte técnico insuficiente de proveedores QKD

- Probabilidad: Media (30%)
- Impacto: Medio-Alto
- Mitigación:
 - SLAs estrictos con tiempos de respuesta definidos
 - Contratos de soporte premium
 - Formación interna extensiva
 - Partnerships técnicos directos con fabricantes

5.5.4 Riesgos Financieros

R15: Sobrecostos significativos. Costos superiores a presupuesto por complejidad imprevista

- Probabilidad: Alta (50%)
- Impacto: Medio
- Mitigación:
 - Contingencia del 20% en presupuesto
 - Contratos a precio cerrado donde sea posible
 - Pagos por objetivos alcanzados
 - Auditorías de costos trimestrales

5.6 Referencias Normativas y Estándares

Estándares Técnicos Aplicables

ETSI (European Telecommunications Standards Institute) 002-018:

- ETSI GS QKD 014: Protocolo para interfaces QKD
- ETSI GS QKD 015: Control y gestión de redes QKD
- ETSI GS QKD 016: Criterio Común de preparación y medida QKD
- ETSI GS QKD 018: Interfaces de gestión de claves cuánticas

NIST (National Institute of Standards and Technology) (Toshiba Europe, s.f.):

- FIPS 203: ML-KEM (Module-Lattice Key Encapsulation Mechanism)
- FIPS 204: ML-DSA (Module-Lattice Digital Signature Algorithm)
- FIPS 205: SLH-DSA (Stateless Hash-Based Digital Signatures)

ISO/IEC Estándares:

- ISO/IEC 27000 proporciona el marco de gestión de seguridad de información que debe incorporar consideraciones de seguridad cuántica
- ISO/IEC 23837-1: Security requirements for QKD.
- ISO/IEC 16290: Niveles de madurez tecnológica
- ISO/IEC 23053: Quantum key distribution vocabulary
- ISO/IEC 4922: Quantum cryptography security evaluation

Standards de integración:

- ETSI TR 103 619: Quantum-Safe Cryptography migration guidelines
- ETSI GS QKD 014 para gestión de claves
- ETSI GS QKD 016 para perfiles de protección Common Criteria
- IETF RFC 8784: Mixing Preshared Keys for Machine-to-Machine (M2M) Communications
- IEEE 802.1AE: MACsec standard for quantum-safe adaptations

Marcos Normativos de Cumplimiento

Unión Europea (PostQuantum, 2024) (IndustrialCyber, 2024):

- NIS2 Directiva: Ciberseguridad para infraestructuras críticas
- GDPR: Protección de datos con criptografía resistente a cuántica.
- EuroQCI Framework y hoja de ruta: Infraestructura cuántica europea.
- ANSSI Guidelines: Recomendaciones criptográficas francesas
- Cyber Resilience Act: Requisitos de seguridad para productos IoT/ICT
- NSM-10: National Security Memorandum on Quantum Computing
- EU Cybersecurity Act: Certification requirements for quantum technologies

España:

- Esquema Nacional de Seguridad (ENS): Aplicación de controles cuánticos
 - CCN-STIC: Guías del Centro Criptológico Nacional
 - Reglamento eIDAS: Identificación y firmas digitales post-cuánticas
- Certificaciones de Seguridad:

- Common Criteria EAL4+: Evaluación formal de seguridad QKD
- FIPS 140-2 Level 3: Módulos de Seguridad de Hardware (HSMs) para gestión de claves híbridas
- ISO 27001: Sistema de gestión de seguridad de la información
- NATO TEMPEST: Para protección contra emanaciones electromagnéticas

Checklist de cumplimiento

Requisitos mínimos de cumplimiento:

- ☐ Certificación ETSI QKD 014 de todos los componentes QKD
- ☐ Validación NIST de algoritmos PQC implementados
- ☐ Auditoría de seguridad independiente (anual)
- ☐ Documentación de arquitectura según ISO 27001
- ☐ Plan de contingencia y recuperación ante desastres
- ☐ Formación certificada de personal técnico
- ☐ Monitorización y anotación (logging) de eventos de seguridad
- ☐ Procedimientos de escalado ante incidentes

5.7 Métricas de Éxito e Indicadores Claves de Rendimiento (KPIs)

5.7.1 Métricas Técnicas

- Rendimiento QKD:
 - Tasa de clave secreta: ≥ 2 kbps a 80 km
 - QBER: $< 5\%$ en condiciones normales
 - Disponibilidad sistema: $\geq 99.5\%$
 - Tiempo de establecimiento de clave: < 300 segundos
- Rendimiento PQC:
 - Latencia handshake: < 50 ms adicional
 - Throughput: Sin degradación $> 5\%$
 - Tasa de éxito: $> 99.9\%$ para todas las operaciones criptográficas
- Sistema Híbrido:
 - Tiempo de recuperación: < 30 segundos
 - Sincronización de claves: 100% consistencia
 - Overhead total: $< 20\%$ vs. Sistemas convencionales

5.7.2 Métricas Operacionales

- Operación y Mantenimiento:
 - Tiempo medio entre fallos. Mean Time Between Failures (MTBF): $> 2,000$ horas
 - Tiempo medio en arreglar. Mean Time To Repair (MTTR): < 4 horas
 - Proporción de personal cualificado. Personal qualification rate: 100% plantilla certificada
 - Incidentes de seguridad. Security incidents: Cero compromisos críticos.

- Financieras:
 - Cumplimiento del presupuesto. Budget adherence: $\pm 10\%$ del presupuesto aprobado
 - ROI de seguridad: Medición de riesgos mitigados
 - Coste Total de un activo a lo largo de su ciclo. Total Cost of Ownership: Tracking completo 5 años

5.7.3 Métricas de Seguridad

- Resistencia a Amenazas:
 - Nivel de preparación cuántica. Quantum readiness score: 95/100 según framework QUASAR
 - Evaluación de vulnerabilidades: Cero críticas, < 5 high-severity
 - Test de penetración. Penetration testing: Pasar nivel anual marcado
 - Nivel de cumplimiento. Compliance score: 100% con regulaciones aplicables
- Detección de Ataques:
 - Porcentaje de falsos positivos. False positive rate: $< 1\%$ en detección QKD
 - Tiempo de detección. Detection time: < 5 minutos para anomalías críticas
 - Tiempo de respuesta. Response time: < 30 minutos para incidentes de seguridad

6 CONCLUSIONES Y VALORACIONES

6.1 Síntesis de Resultados y Contribuciones

La investigación desarrollada en este trabajo confirma que las tecnologías de distribución de clave cuántica (QKD) han alcanzado un nivel de madurez suficiente para implementaciones especializadas en sectores críticos, aunque permanecen limitaciones significativas que restringen su adopción generalizada.

El análisis comparativo de protocolos revela que BB84 constituye la opción más viable para implementaciones inmediatas (TRL 7-8), mientras que protocolos avanzados como E91 y MDI-QKD ofrecen ventajas de seguridad específicas a costa de mayor complejidad tecnológica. La evaluación de madurez tecnológica indica que los sistemas QKD comerciales han superado la fase de prueba de concepto, pero requieren desarrollo adicional para alcanzar la robustez requerida en entornos operacionales exigentes.

La principal contribución del trabajo reside en la identificación de arquitecturas híbridas QKD+PQC como la aproximación más prometedora para superación de limitaciones individuales de cada tecnología. Esta hibridación resuelve específicamente el problema crítico de autenticación inicial en QKD mediante certificados post-cuánticos, mientras proporciona protección incondicional contra amenazas cuánticas futuras. La implementación híbrida recomendada optimiza la relación costo-beneficio mientras construye capacidades cuánticas estratégicas. El cronograma 2025-2030 coincide con las tendencias globales y permite una transición controlada que minimiza riesgos operacionales mientras maximiza la preparación ante la era cuántica.

La inversión total estimada de 4,1 M € durante 5 años se justifica por la criticidad de las comunicaciones seguras y la necesidad de adelantarse a la amenaza cuántica emergente HNDL. El retorno de inversión se materializa en continuidad operacional, cumplimiento normativo y ventaja competitiva estratégica.

Las organizaciones que retrasen esta preparación se enfrentan a riesgos de exposición extendida de datos sensibles y costes de migración de emergencia significativamente mayores.

El éxito en la transición cuántica dependerá fundamentalmente de inversión en capacidades humanas, establecimiento de arquitecturas adaptables y colaboración activa con el ecosistema de investigación e industria cuántica. Las organizaciones que adopten aproximaciones estratégicas

integrales estarán mejor posicionadas para aprovechar las oportunidades transformacionales que las tecnologías cuánticas proporcionarán en la próxima década.

En síntesis, la convergencia de la amenaza HNDL y el desarrollo acelerado de los CRQC sitúa a las organizaciones de Defensa ante un imperativo de actuación inmediato. El análisis realizado permite concluir:

- La **PQC es necesaria e inevitable**, constituyendo la primera línea de defensa escalable y de rápida implementación para la mayoría de sistemas IT.
- La **QKD es insustituible para la alta seguridad**, proporcionando la única garantía de confidencialidad a largo plazo basada en leyes físicas, crítica para secretos de estado.
- La **Hibridación es la estrategia ganadora**, combinando la robustez física de la QKD con la versatilidad y capacidad de autenticación de la PQC.

La adopción de la hoja de ruta propuesta permitirá a la organización transitar desde una postura de vulnerabilidad latente hacia una de **ciber-resiliencia cuántica**, garantizando la soberanía de la información en la era post-Shor.

6.2 Aplicaciones Presentes: Nichos de Alto Valor

6.2.1 Sector Defensa e Inteligencia

Las aplicaciones defensivas representan el sector de adopción más inmediata para tecnologías QKD, donde los requisitos de seguridad justifican las inversiones y complejidades operacionales involucradas.

- *Comunicaciones Estratégicas*: Enlaces entre centros de mando y control, donde la interceptación podría comprometer operaciones críticas. Los sistemas QKD proporcionan alertas inmediatas de interceptación mediante monitoreo de QBER, capacidad inexistente en sistemas clásicos.
- *Protección de Inteligencia*: Transmisión de información clasificada donde la amenaza HNDL representa un riesgo estratégico a largo plazo. La seguridad incondicional de QKD garantiza protección permanente independiente de avances tecnológicos adversarios.
- *Infraestructura Crítica*: Protección de sistemas de control SCADA (Control de Supervisión y Adquisición de Datos), es un sistema informático que permite monitorear y controlar procesos industriales en tiempo real en instalaciones nucleares, redes eléctricas y sistemas de transporte donde el compromiso criptográfico podría causar impactos catastróficos.

6.2.2 Sector Financiero y Sanitario

- *Transacciones de Alto Valor*: Instituciones financieras con necesidades de protección de transacciones superiores a 1M €, donde el costo de implementación QKD resulta proporcional al valor protegido.
- *Datos Médicos Longitudinales*: Protección de información genética y registros médicos con valor permanente, donde la confidencialidad debe mantenerse durante décadas.
- *Interconexión de Datacenters*: Enlaces seguros entre centros de datos geográficamente distribuidos, particularmente para organizaciones con requisitos de soberanía de datos.

6.3 Aplicaciones Futuras: Perspectivas de Evolución

6.3.1 Quantum Internet y Redes Globales (2030-2035)

La evolución hacia redes cuánticas globales representa la perspectiva más transformativa para tecnologías QKD, aunque requiere desarrollos tecnológicos sustanciales en repetidores cuánticos y memorias cuánticas.

- *Repetidores Cuánticos*: El desarrollo de repetidores basados en entrelazamiento permitirá extensión de QKD a distancias intercontinentales, superando las limitaciones actuales de ~400 km mediante repetidores confiables.
- *Protocolos de Internet Cuántico (Quantum Internet Protocols)*: La estandarización de protocolos de red cuántica (análogos a TCP/IP) facilitará interoperabilidad global y aplicaciones distribuidas que aprovechen correlaciones cuánticas.
- *Aplicaciones Distribuidas*: Computación cuántica distribuida, consenso cuántico en blockchain, y protocolos de votación verificable cuánticamente representan aplicaciones emergentes que requerirán infraestructura QKD.

6.3.2 Integración IoT y Edge Computing (2025-2030)

- *Dispositivos IoT Críticos*: Sensores y actuadores en infraestructura crítica que requieren autenticación cuántica para prevenir ataques de suplantación.
- *Edge Computing Seguro*: Procesamiento distribuido en el borde de red con garantías cuánticas de integridad computacional.
- *Vehículos Autónomos*: Comunicaciones entre vehículos (V2V (vehicle-to-vehicle)) con autenticación cuántica para prevenir ataques a sistemas de transporte autónomo.

6.4 Desafíos Tecnológicos Persistentes

6.4.1 Limitaciones Físicas Fundamentales

- *Pérdidas en Fibra Óptica*: La atenuación exponencial de señales cuánticas impone límites fundamentales en distancias de transmisión que solo pueden superarse mediante repetidores cuánticos, tecnología aún en desarrollo (TRL 2-3).
- *Ruido de Detectores*: Las tasas de recuento oscuro en detectores de fotón único limitan la sensibilidad y requieren refrigeración criogénica para aplicaciones de alta sensibilidad.
- *Decoherencia Ambiental*: La interacción inevitable con el entorno destruye gradualmente la coherencia cuántica, requiriendo protocolos de corrección de errores cuánticos para aplicaciones extendidas.

6.4.2 Desafíos de Ingeniería

- *Sincronización Temporal*: Los protocolos QKD requieren sincronización de nanosegundos que se degrada con la distancia y condiciones ambientales.
- *Estabilización de Componentes*: Las fluctuaciones térmicas y mecánicas afectan la estabilidad de interferómetros y moduladores ópticos, requiriendo sistemas de control activo sofisticados.
- *Integración de Sistemas*: La complejidad de integración con infraestructura de red existente introduce puntos de fallo adicionales y requisitos de mantenimiento especializados.

6.5 Recomendaciones Estratégicas

6.5.1 Para Organizaciones Implementadoras

- *Adopción Gradual*: Iniciar con proyectos piloto en enlaces críticos específicos antes de expansión sistémica, aprovechando curva de aprendizaje y evolución tecnológica.
- *Enfoque Híbrido*: Priorizar arquitecturas QKD+PQC que proporcionen flexibilidad operacional y protección robusta contra múltiples vectores de amenaza.
- *Desarrollo de Competencias*: Invertir en formación especializada y establecer alianzas con centros de investigación para acceso continuo a expertos (expertise) emergentes.

6.5.2 Para responsables de Política

- *Financiación de I+D*: Mantener inversión sostenida en investigación fundamental de tecnologías cuánticas, particularmente en repetidores cuánticos y memorias cuánticas.
- *Estandarización Proactiva*: Participar activamente en desarrollo de estándares internacionales para asegurar interoperabilidad y evitar fragmentación tecnológica.
- *Ecosistema Industrial*: Fomentar colaboraciones universidad-industria y apoyar el desarrollo de una cadena de suministro europea independiente en tecnologías cuánticas.

6.6 Perspectiva Temporal y Hoja de Ruta Tecnológica

La adopción masiva de tecnologías QKD seguirá un patrón de difusión tecnológica característica de innovaciones disruptivas, con adopción inicial en nichos especializados seguida de expansión gradual conforme se reduzcan costos y se simplifique operación. (Ver Figura 6.1. Cronograma de perspectivas)

- *Horizonte 2024-2027*: Consolidación de aplicaciones en defensa e infraestructura crítica, con mejoras en costo-efectividad y robustez operacional.
- *Horizonte 2027-2032*: Expansión a sectores comerciales de alto valor, desarrollo de servicios QKD-as-a-Service (QaaS), y primeras implementaciones de repetidores cuánticos.
- *Horizonte 2032-2040*: Integración en infraestructura de telecomunicaciones generalizada, desarrollo de aplicaciones Quantum Internet, y convergencia con ecosistemas de computación cuántica.

La transformación hacia un paradigma criptográfico cuántico *representa no solo una evolución tecnológica sino una revolución en los fundamentos mismos de la seguridad digital*, con implicaciones que trascienden el ámbito técnico para abarcar aspectos geopolíticos, económicos y sociales de la sociedad digital del siglo XXI. Las organizaciones que inicien su transición cuántica segura hoy se posicionarán con ventajas competitivas decisivas en el ecosistema digital de la próxima década.

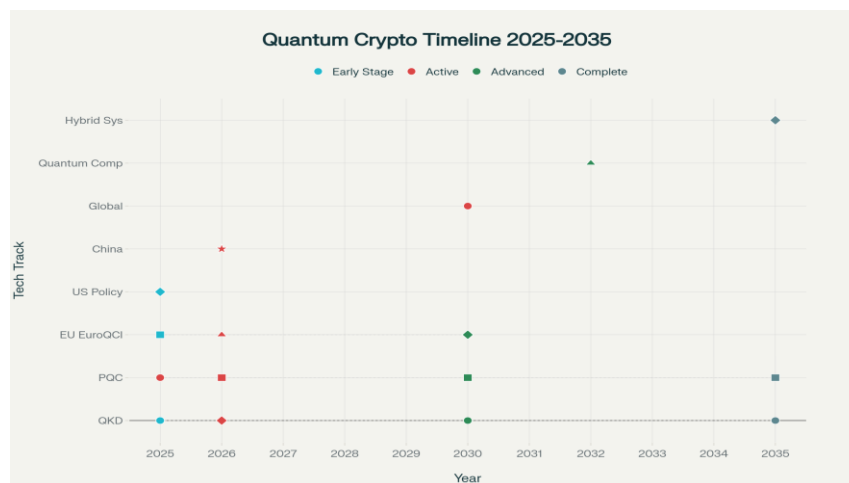


Figura 6-1. Cronograma de previsión de despliegue de tecnologías de criptografía cuántica (2025-2035)
(Adaptado de Perplexity)

7 BIBLIOGRAFÍA

- Acker, M. S. (2023). Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. *Journal of Cybersecurity Research*.
- Adnane, A., & Potortì, F. (2023). Measurements of Cross-Border Quantum Key Distribution Link. En *Proceedings of the 12th International Conference on Data Science, Technology and Applications* (pp. 472-479). SciTePress. <https://www.scitepress.org/Papers/2023/116472/116472.pdf>
- Aguado, A., Lopez, V., Martinez-Mateo, J., Szyrkowiec, T., Autenrieth, A., Slyne, F., ... & Martin, V. (2021). The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections. *Fifth PQC Standardization Conference*. <https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/the-impact-of-data-heavy-post-quantum.pdf>
- Ahmed, F. (2024). Quantum-resistant cryptography for national security: A policy and implementation roadmap. *International Journal of Multidisciplinary on Science and Management*, 1(4), 54-65. <https://doi.org/10.71141/30485037/V1I4P108>
- Barrero, D. J. (2014, enero). Quantum state tomography of polarization states: An exploration of quantum logic gates. [Tesis]. Universidad de Buenos Aires.
- Behera, B. K., Al-Kuwari, S., & Farouk, A. (2025). QNN-QRL: Quantum neural network integrated with quantum reinforcement learning for quantum key distribution. *Quantum Information Processing*.
- Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179.
- Campagna, M., LaMacchia, B., & Ott, D. (s.f.). Post quantum cryptography: Readiness challenges and the approaching storm. NIST Technical Report.
- Canada's National Quantum Strategy. (s.f.). Recuperado el 23 de diciembre de 2025, de <https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy>
- Canto, A. C., Sarker, A., Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R. (2022). Error detection schemes assessed on FPGA for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography. *IEEE Transactions on Emerging Topics in Computing*, 10(3), 3168-3175. <https://doi.org/10.1109/TETC.2022.3217006>

- Celi, S., & Wiggers, N. (2024). KEM-based Authentication for TLS 1.3 (Internet-Draft draft-celi-wiggers-tls-authkem-06). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-celi-wiggers-tls-authkem/>
- Choi, K.-H., Han, J., & Han, D.-G. (2024). Single trace analysis of visible vs. invisible leakage for comparison-operation-based CDT sampling. *Electronics*, 13(23), 4681. <https://doi.org/10.3390/electronics13234681>
- Cloudflare. (2020). KEMTLS: Post-quantum TLS without signatures. The Cloudflare Blog. <https://blog.cloudflare.com/kemtls-post-quantum-tls-without-signatures/>
- Currás-Lorenzo, R., García-Martínez, V., & Vázquez-Gallardo, F. (2025). Quantum network implementations: Recent advances and practical considerations. *Quantum Journal*.
- Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, 7(3), 40. <https://doi.org/10.3390/cryptography7030040>
- Darzi, S., Ahmadi, K., Aghapour, S., Yavuz, A. A., & Kermani, M. M. (2023). Envisioning the future of cyber security in post-quantum era: A survey on PQ standardization, applications, challenges and opportunities. *IEEE Security & Privacy Magazine*, 35.
- De Santis, E., & Mancini, M. (2025). Extending Quantum-Safe Communications to Real-World Networks: An Adaptive Security Framework. arXiv. <https://arxiv.org/html/2511.22416v1>
- Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., ... & Shields, A. J. (2009). High Speed Quantum Key Distribution Over Optical Fiber Network System. *Journal of Research of the National Institute of Standards and Technology*, 114(3), 167. <https://nvlpubs.nist.gov/nistpubs/jres/114/3/V114.N03.A02.pdf>
- Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661–663. <https://doi.org/10.1103/PhysRevLett.67.661>
- El Gobierno lanza la primera Estrategia de Tecnologías Cuánticas de España con una inversión de 800 millones de euros. (2025, abril). Recuperado el 23 de diciembre de 2025, de <https://www.ciencia.gob.es/Noticias/2025/abril/lanza-primera-estrategia-tecnologias-cuanticas.html>
- EMPIR. (2018). Best practice guide on characterisation of counter-measures to side-channel and Trojan-horse attacks (Deliverable D5-1). European Metrology Programme for Innovation and Research. https://empir.npl.co.uk/miqc2/wp-content/uploads/sites/9/2018/10/D5-1-Best_practice_guide_side-channel_Trojan-horse_attacks_redacted-for-publication.pdf
- European Telecommunications Standards Institute. (2019). Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API (ETSI GS QKD 014 V1.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
- European Telecommunications Standards Institute. (2020). Quantum Key Distribution (QKD); Application Interface (ETSI GS QKD 004 V2.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf
- European Telecommunications Standards Institute. (2021). Quantum Key Distribution (QKD); Control Interface for Software Defined Networks (ETSI GS QKD 015 V1.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/01.01.01_60/gs_qkd015v010101p.pdf
- European Telecommunications Standards Institute. (2022). Quantum Key Distribution (QKD); Control Interface for Software Defined Networks (ETSI GS QKD 015 V2.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf

- Fedorov, A. K. (2023). Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Frontiers in Quantum Science and Technology*. <https://doi.org/10.3389/frqst.2023.1164428>
- Galdo, G., Grover, A., & Martinez, P. (2024). Physical properties of qubits and their role in security. *Quantum Security Review*.
- García, C. R., Rommel, S., Takarab, S., Olmos, J. J. V., Guilley, S., Nguyen, P., & Monroy, I. T. (2024). Quantum-resistant transport layer security. *Computer Communications*, 213, 345-358. <https://doi.org/10.1016/j.comcom.2024.05.012>
- GÉANT. (s.f.). Quantum Standardisation. GÉANT Federated Confluence. Recuperado el 4 de enero de 2026, de <https://wiki.geant.org/display/NETDEV/Quantum+Standardisation>
- Gobierno de España. (2025). Estrategia de Tecnologías Cuánticas de España 2025-2030. Ministerio para la Transformación Digital y de la Función Pública.
- Government of Canada. (2023). Canada's National Quantum Strategy. Recuperado de <https://isde-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy>
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219.
- Hita, I. B., González, Ó. I., Álvarez, J. A., Roca, L. P., López, G. M. C., & Cao, M. F. (2023, septiembre). Investigación de la aplicabilidad de las tecnologías cuánticas a las telecomunicaciones. *Revista de Tecnología Cuántica*, 15(3), 234-256.
- HM Government. (2023). National Quantum Strategy. Department for Science, Innovation and Technology (UK).
- Hoque, S., Aydeger, A., & Zeydan, E. (2024). Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. *ACM Transactions on Network Security*, 2024. <https://doi.org/10.1145/3659997.3660033>
- Huttner, B. (2013). Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. En 2013 IEEE International Conference on Space Optical Systems and Applications (ICSOS) (pp. 1-7). IEEE. <https://ieeexplore.ieee.org/document/6459842/>
- Iberdrola. (2023). Quantum technologies and cryptography: Current limitations and future prospects. Technical Report, Iberdrola Innovation Lab.
- ID Quantique. (s.f.). ETSI releases world's first Protection Profile for QKD. Recuperado el 4 de enero de 2026, de <https://www.idquantique.com/etsi-releases-qkd-protection-profile/>
- IndustrialCyber. (2024). EU begins coordinated effort for member states to switch critical infrastructure to quantum-resistant encryption by 2030. Recuperado de <https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf>
- Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11), e1701491. <https://pmc.ncbi.nlm.nih.gov/articles/PMC5706749/>
- J, Karthika Sorna Ilakkia and Jebadurai, Immanuel Johnraja and Paulraj, Getzi Jeba Leelipushpam (2025). Demystifying Security Analysis of Intercept-and-Resend Attack Over Quantum Key Distribution (QKD) Protocols .3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). <https://ieeexplore.ieee.org/abstract/document/11167114/authors>

- Joint Research Centre (Comisión Europea). (2023). Quantum Key Distribution (QKD) Experimental Assessment. Publications Office of the European Union.
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC132426/JRC132426_01.pdf
- Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., & Diamanti, E. (2013). Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5), 378-381.
<https://eprints.whiterose.ac.uk/id/eprint/161908/1/1. Long distance continuous variable quantum key distribution over 202.81 km fiber.pdf>
- Juniper Networks. (2022). Validation of a Quantum Safe MACsec Implementation.
<https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2022/validation-of-quantum-safe-macsec-white-paper.pdf>
- Kabanov, D., Petrov, I., & Smirnov, Y. (2018). Early experiments in quantum key distribution: From theory to practice. *Journal of Quantum Computing*, 12(4), 445-467.
- Kiktenko, E. O., Trushechkin, A. S., Lim, C. C. W., Kurochkin, Y. V., & Fedorov, A. K. (2023). Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams. *Sensors*, 23(24), 9818. <https://www.mdpi.com/1424-8220/23/24/9818>
- Laudenbach, F., Pacher, C., Fung, C. H. F., Poppe, A., Peev, M., Schrenk, B., ... & Hübel, H. (2018). Continuous-variable quantum key distribution with Gaussian modulation: The theory of practical implementations. *Advanced Quantum Technologies*, 1(1), 1800011.
<https://pubs.aip.org/aip/apr/article/11/1/011318/3279669/Continuous-variable-quantum-key-distribution>
- Le, T. D., Do, P. H., Dinh, T. D., & Pham, V. D. (2025). Are enterprises ready for quantum-safe cybersecurity? *Cybersecurity Quarterly Review*.
- Li, X., & Xu, F. (2025). A Survey on Continuous Variable Quantum Key Distribution for Secure Data Transmission. *arXiv*. <https://arxiv.org/html/2506.21640v1>
- Lidbjörk, E., & Söderström Nylander, R. (2023, septiembre). Cost and efficiency comparison of quantum key distribution schemes. *IEEE Transactions on Quantum Engineering*, 4(2), 1-12.
- Liu, J., Wang, X., & Chen, Y. (2025). Twin-field quantum key distribution: Recent advances and practical implementation. *Nature Photonics*, 19(2), 123-135.
- Makris, K., Papadopoulos, N., & Stavrinos, S. (2024). Commercial quantum key distribution implementations: Status and trends. *Quantum Technology Market Report*.
- Matsuura, T., Maeda, K., Sasaki, T., & Koashi, M. (2023). Countering detector manipulation attacks in quantum communication through detector self-testing. *APL Photonics*, 10(1), 016106.
<https://pubs.aip.org/aip/app/article/10/1/016106/3330518/Countering-detector-manipulation-attacks-in>
- Mattsson, J. P., Smeets, B., & Thormarker, E. (2021). Quantum-resistant cryptography: A comprehensive overview. *ACM Computing Surveys*. <https://doi.org/10.48550/arXiv.2112.00399>
- Mehic, M., et al. (2025). Overview of Routing Approaches in Quantum Key Distribution Networks. *arXiv*. <https://arxiv.org/abs/2511.15465>
- Miloslavskaya, V. (2024). Comparison of Discrete Variable and Continuous Variable Quantum Key Distribution Protocols with Phase Noise in the Thermal-Loss Channel. *Quantum*, 8, 1382.
<https://quantum-journal.org/papers/q-2024-06-20-1382/>
- Ministerio de Defensa (España). (2024). Capacidades Militares en el Ámbito Europeo de la Defensa. Informe Estratégico.

- Molano, K. A. S. (2020, agosto). Fundamentos y avances en criptografía cuántica. [Trabajo de Grado]. Universidad de los Andes.
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16(5), 38-41. <https://doi.org/10.1109/MSP.2018.3761723>
- National Institute of Standards and Technology. (2024). NIST IR 8547: Post-Quantum Cryptography Standardization. Recuperado de <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>
- National Institute of Standards and Technology. (2024, 13 de agosto). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. U.S. Department of Commerce. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
- National Institute of Standards and Technology. (s.f.). FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard. Recuperado el 23 de diciembre de 2025, de <https://csrc.nist.gov/pubs/fips/203/final>
- National Institute of Standards and Technology. (s.f.). Module-Lattice-Based Digital Signature Standard. Recuperado el 23 de diciembre de 2025, de <https://www.nist.gov/publications/module-lattice-based-digital-signature-standard>
- National Institute of Standards and Technology. (s.f.). On the practical cost of Grover for AES key recovery. Recuperado el 23 de diciembre de 2025, de <https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf>
- National Institute of Standards and Technology. (s.f.). Stateless Hash-Based Digital Signature Standard. Recuperado el 23 de diciembre de 2025, de <https://www.nist.gov/publications/stateless-hash-based-digital-signature-standard>
- National Institutes of Health. (2026). Real-Time Diagnostics on a QKD Link via QBER Time-Series. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11593268/>
- Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.
- Organization for Economic Cooperation and Development. (2025, febrero). A quantum technologies policy primer. <https://doi.org/10.1787/fd1153c3-en>
- Palo Alto Networks. (s.f.). What Is Post-Quantum Cryptography (PQC)? A Complete Guide. Recuperado el 4 de enero de 2026, de <https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc>
- Paredes López, M., Meneses Viveros, A., & Morales-Luna, G. (2018). Algoritmo cuántico de Deutsch y Jozsa en GAMA. Revista Mexicana de Física E, 64(2), 181-189.
- PennyLane Demos. (s.f.). Grover's Algorithm. Recuperado el 23 de diciembre de 2025, de https://pennylane.ai/qml/demos/tutorial_grovers_algorithm
- Popa, A.-B., & Popescu, P. G. (2021). CEF: Connecting elaborate federal QKD networks. Journal of Latex Class Files, 14(8), 1-15.
- PostQuantum. (2024). EU PQC Roadmap: European Union post-quantum cryptography adoption strategy. Recuperado de <https://postquantum.com/industry-news/eu-pqc-roadmap>
- PQShield. (s.f.). Post-quantum cryptography for defence and governmental applications: Overview and use cases. Recuperado de <https://pqshield.com/publications/post-quantum-cryptography-for-defence-and-governmental-applications-overview-and-use-cases>

- Primaatmaja, I. W., Goh, K. T., Tan, E. Y.-Z., Khoo, J. T.-F., Ghorai, S., & Lim, C. (2023). Security of device-independent quantum key distribution protocols: A review. *Quantum*, 7, 1026. <https://doi.org/10.22331/q-2023-02-16-5326458>
- Reyes Rosado, A. R., Rifà Coma, J., Arjona Fernández, M., & Rifà Pous, H. (2018, diciembre). Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos. *Proceedings of XXXIV Congreso de la Sociedad de Estadística e Investigación Operativa*.
- Saganová, R. (2024). Quantum key distribution protocols and their implementation challenges. [Tesis de Grado]. Brno University of Technology.
- Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics*, 12, 1456491. <https://doi.org/10.3389/fphy.2024.1456491>
- Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), 1301–1350. <https://doi.org/10.1103/RevModPhys.81.1301>
- Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Recuperado el 23 de diciembre de 2025, de <https://www.semanticscholar.org/paper/Algorithms-for-quantum-computation%3A-discrete-and-Shor/2273d9829cdf7fc9d3be3cbecb961c7a6e4a34ea>
- Shamshad, S., Riaz, F., Riaz, R., Rizvi, S. S., & Abdulla, S. (2022). An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. *Sensors*, 22(8), 8151. <https://doi.org/10.3390/s22218151>
- Shokrivahed, S., & Verticale, G. (2023). Integration of QKD at the application layer vs network layer: A Markov-chain model. *IEEE Communications Magazine*, 61(5), 1-7.
- Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. <https://doi.org/10.1109/sfcs.1994.365700>
- Shu, H. (2022). Quantum key distribution based on orthogonal state encoding. *arXiv Preprint arXiv:2107.01964v6*. <https://arxiv.org/abs/2107.01964v6>
- Suarez Molano, K. A., & Botero Mejía, A. (2020). Fundamentos y avances en criptografía cuántica. [Trabajo de Grado]. Universidad de los Andes.
- Toshiba Europe. (s.f.). The importance of quantum-safe communication: Post-quantum cryptography (PQC) and quantum key distribution (QKD). Recuperado de <https://www.toshiba.eu/quantum/insights/the-importance-of-qkd-and-pqc-for-quantum-security>
- UK Government. (2023). National Quantum Strategy. Recuperado de <https://www.gov.uk/government/publications/national-quantum-strategy>
- Villafruela, J. M. (s.f.). Estudio del protocolo BB84 de criptografía cuántica. Technical Report.
- Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., ... & Zbinden, H. (2013). A fast and versatile QKD system with hardware key distillation and wavelength multiplexing. *Journal of Quantum Communications*, 2(3), 1-18. <https://arxiv.org/abs/1309.2583v2>
- Wang, L. L. (2025, junio). Introducción a la criptografía post-cuántica: Métodos y conceptos para su validación. Springer Nature, *Quantum Computing Reviews*.
- Wang, Y., & Ismail, E. S. (2025). A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT. *IEEE Access*, 13, 1-45. <https://doi.org/10.1109/ACCESS.2025.3584473>

- Wang, Y., Zhang, Z., & Wang, X. (2024). Research on QKD network routing algorithm based on key consumption. En Proceedings of SPIE 13968, International Conference on Optical Communications and Networks (p. 1396817). <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/13968/1396817/Research-on-QKD-network-routing-algorithm-based-on-key-consumption/10.1117/12.3090949.full>
- Weger, V., Gassner, N., & Rosenthal, J. (2024, julio). A survey on code-based cryptography. arXiv Preprint arXiv:2201.07119v5. <https://arxiv.org/abs/2201.07119v5>
- Wiedijk, E. (2022, junio). Comparison of post-quantum cryptography and quantum key distribution. [Tesis de Máster]. University of Amsterdam.
- Wikipedia. (s.f.). Michele Mosca. Recuperado el 23 de diciembre de 2025, de https://en.wikipedia.org/wiki/Michele_Mosca
- Wikipedia. (s.f.). Quantum key distribution. Recuperado el 4 de enero de 2026, de https://en.wikipedia.org/wiki/Quantum_key_distribution
- World Journal of Advanced Research and Reviews. (2025). [Título del artículo]. World Journal of Advanced Research and Reviews, 25(1), 1–15.
- Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Di Pietro, R., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. IEEE Transactions on Quantum Engineering, 5, 1-22.
- Zeng, P., Bandyopadhyay, D., Méndez, J. A. M., Bitner, N., Kolar, A., Solomon, M. T., ... & Liu, J. (2024). Practical hybrid PQC-QKD protocols with enhanced security and performance. arXiv Preprint arXiv:2411.01086. <https://arxiv.org/abs/2411.01086>
- Zhang, L., Li, W., Pan, J., Lu, Y., Li, W., Li, Z.-P., ... & Pan, J.-W. (2025). Experimental mode-pairing quantum key distribution surpassing the repeaterless bound. Physical Review X, 15(2), 021037. <https://doi.org/10.1103/PhysRevX.15.021037>
- Zhang, Y., Li, Z., & Zhao, Y. (2024). Enhancing Performance of Continuous-Variable Quantum Key Distribution (CV-QKD) and Gaussian Modulation of Coherent States (GMCS) in Free-Space Channels under Individual Attacks with Phase-Sensitive Amplifier (PSA) and Homodyne Detection (HD). Sensors, 24(16), 5201. <https://www.mdpi.com/1424-8220/24/16/5201>
- Zhou, R.-G., Zhang, X.-X., & Du, L.-T. (s.f.). Design and analysis of secure quantum communication schemes. Journal of Quantum Information Technology.

7.1 Referencias utilizadas para obtener las Figuras:

- [1] Figura 1-1: <https://www.hashicorp.com/en/blog/harvest-now-decrypt-later-why-today-s-encrypted-data-isn-t-safe-forever>.
- [2] Figura 1-2: <https://medium.com/mit-6-s089-intro-to-quantum-computing/a-general-implementation-of-shors-algorithm-da1595694430>
- [3] Figura 1-3: <https://indexedev.com/post/grovers-algorithm-unveiling-quantum-computings-search-superpower/>
- [4] Figura 1-4: https://en.wikipedia.org/wiki/Deutsch%E2%80%93Jozsa_algorithm#
- [5] Figura 1-5: https://www.researchgate.net/figure/Figura-32-Ilustracao-da-esfera-de-Bloch-KETTERER-2016_fig1_352898890.
- [6] Figura 1-6: <https://www.heraldo.es/noticias/sociedad/2011/06/21/superposicion-cuantica-medida-cuantica-145441-310.html>.

- [7] Figura 1-7: <https://www.cambio16.com/nuevo-chip-cuatico-de-google-tiene-potencia-de-calculo-alucinante/>
- [8] Figura 1-8: <https://www.elespectador.com/ciencia/en-fotos-asi-se-ven-dos-particulas-de-luz-entrelazadas-cuanticamente/>
- [9] Figura 1-9: <https://how-to-understand-physics.site123.me/my-blog/principio-de-incertidumbre-de-heisenberg>.
- [10] Figura 1-10: <https://www.monografias.com/trabajos107/informacion-cuantica/informacion-cuantica>.
- [11] Figura 1-11: <https://divulgando-ciencia.blog/el-reino-cuatico-y-su-interpretacion/>
- [12] Figura 1-12: <https://francis.naukas.com/2013/07/08/francis-en-trending-ciencia-el-problema-del-colapso-de-la-funcion-de-onda/>
- [13] Figura 2-1:
https://www.researchgate.net/publication/282821048_Development_of_a_simulator_for_the_quantum_cryptography_protocol_E91_in_a_distributed_environment.
- [14] Figura 2-2: <https://www.semanticscholar.org/paper/Is-Quantum-State-in-BB84-Protocol-Really-Unclonable-Lee-Kim/1d0e2facfd2c79db6f100c4b2c8a81153475a940>

8 ANEXO I: ACRÓNIMOS

ACL	Ataques de Canal Lateral (Side-Channel Attacks)
AES	Advanced Encryption Standard (Estándar de Cifrado Avanzado)
ANSSI	Agence nationale de la sécurité des systèmes d'information (Agencia Nacional de Seguridad de Sistemas de Información - Francia)
APD	Avalanche Photodiode (Fotodiodo de Avalancha)
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
BB84	Bennett & Brassard 1984 (Protocolo QKD)
CAPEX	Capital Expenditure (Gasto de Capital)
CC	Computación Clásica
CCN-STIC	Centro Criptológico Nacional - Sistemas y Tecnologías de la Información y las Comunicaciones
CCNOT	Controlled-Controlled-NOT (Puerta cuántica, equivalente a Toffoli)
CHSH	Clauser, Horne, Shimony y Holt (Desigualdad Bell)
CNOT	Controlled-NOT (No-Controlada)
COTS	Commercial Off-The-Shelf (Componentes comerciales listos para usar)
CP	Controlled-P (Fase Controlada)
CRQC	Cryptographically Relevant Quantum Computer (Ordenador Cuántico Criptográficamente Relevante)
CV-QKD	Continuous-Variable Quantum Key Distribution (Distribución de Clave Cuántica de Variable Continua)
CZ	Controlled-Z (Z Controlada)
DCI	Data Center Interconnect (Interconexión de Centros de Datos)
DCR	Dark Count Rate (Tasa de Cuentas Oscuras)
DH	Diffie-Hellman
DV-QKD	Discrete-Variable Quantum Key Distribution (Distribución de Clave Cuántica de Variable Discreta)
DWDM	Dense Wavelength Division Multiplexing (Multiplexación por División de Longitud de Onda Densa)
E91	Ekert 1991 (Protocolo QKD)
EAL4+	Evaluation Assurance Level 4+ (Nivel de Garantía de Evaluación 4+)
ECC	Elliptic Curve Cryptography (Criptografía de Curva Elíptica)
ENM	Escuela Naval Militar (Marín, España)
ENS	Esquema Nacional de Seguridad (España)
ETSI	European Telecommunications Standards Institute (Instituto Europeo de Normas de Telecomunicaciones)
FIPS	Federal Information Processing Standards (Estándares Federales de Procesamiento de Información)
FTE	Full Time Equivalent (Equivalente a Tiempo Completo)

GCM	Galois/Counter Mode (Modo Galis/Contador)
GDPR	General Data Protection Regulation (Reglamento General de Protección de Datos)
GPS	Global Positioning System (Sistema de Posicionamiento Global)
H	Hadamard (Puerta cuántica)
HFT	High Frequency Trading (Negociación de Alta Frecuencia)
HMAC	Hash-based Message Authentication Code (Código de Autenticación de Mensajes basado en Hash)
HN DL	Harvest Now, Decrypt Later (Cosechar Ahora, Descifrar Después)
HSM	Hardware Security Module (Módulo de Seguridad de Hardware)
I+D	Investigación y Desarrollo (R&D)
IETF	Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)
IKEv2	Internet Key Exchange versión 2 (Intercambio de Claves de Internet v2)
IoT	Internet of Things (Internet de las Cosas)
IP	Internet Protocol (Protocolo de Internet)
IPsec	Internet Protocol Security (Seguridad del Protocolo de Internet)
ISO	International Organization for Standardization (Organización Internacional de Normalización)
IT	Information Technology (Tecnologías de la Información)
ITS	Information-Theoretic Security (Seguridad Teórica de la Información)
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
KDF	Key Derivation Function (Función de Derivación de Clave)
KEM	Key Encapsulation Mechanism (Mecanismo de Encapsulamiento de Claves)
KMS	Key Management System (Sistema de Gestión de Claves)
KPI	Key Performance Indicator (Indicador Clave de Rendimiento)
LCoS	Liquid Crystal on Silicon (Cristal Líquido sobre Silicio)
LDPC	Low-Density Parity-Check (Comprobación de Paridad de Baja Densidad)
LKMS	Local Key Management System (Sistema de Gestión de Claves Local)
LWE	Learning With Errors (Aprendizaje con Errores)
MAN	Metropolitan Area Network (Red de Área Metropolitana)
MDI-QKD	Measurement-Device-Independent QKD (QKD Independiente del Dispositivo de Medición)
MEMS	Micro-Electro-Mechanical Systems (Sistemas Microelectromecánicos)
MITM	Man-In-The-Middle (Ataque de Intermediario)
ML-DSA	Module-Lattice Digital Signature Algorithm (Algoritmo de Firma Digital basado en Retículos de Módulos)
ML-KEM	Module-Lattice Key Encapsulation Mechanism (Mecanismo de Encapsulamiento de Claves basado en Retículos)
MLWE	Module Learning With Errors (Aprendizaje con Errores en Módulos)
MTBF	Mean Time Between Failures (Tiempo Medio Entre Fallos)

MTTR	Mean Time To Repair (Tiempo Medio de Reparación)
MTU	Maximum Transmission Unit (Unidad Máxima de Transmisión)
NATO	North Atlantic Treaty Organization (OTAN)
NIS2	Network and Information Security Directive 2 (Directiva de la UE)
NISQ	Noisy Intermediate-Scale Quantum (Cuántica de Escala Intermedia Ruidosa)
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología - EE.UU.)
NOC	Network Operations Center (Centro de Operaciones de Red)
NTB LM	IA de Gemini (Notebook LM)
O&M	Operation and Maintenance (Operación y Mantenimiento)
ODF	Optical Distribution Frame (Repartidor Óptico)
OPEX	Operational Expenditure (Gastos Operacionales)
OTN	Optical Transport Network (Red de Transporte Óptico)
OTP	One-Time Pad (Libreta de un Solo Uso)
P&M	Prepare and Measure (Preparación y Medida)
PCS	Post-Compromise Security (Seguridad Post-Compromiso)
PIC	Photonic Integrated Circuit (Circuito Integrado Fotónico)
PKE	Public Key Encryption (Cifrado de Clave Pública)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PLOB	Pirandola-Laurenza-Ottaviani-Banchi (Límite fundamental de capacidad cuántica)
PNS	Photon Number Splitting (Ataque de División del Número de Fotones)
PoC	Proof of Concept (Prueba de Concepto)
PQC	Post-Quantum Cryptography (Criptografía Post-Cuántica)
PQCS	Post-Quantum Cryptography Specialist (Especialista en Criptografía Post-Cuántica)
QBER	Quantum Bit Error Rate (Tasa de Error de Bit Cuántico)
QC	Quantum Computing (Computación Cuántica)
QDS	Quantum Digital Signature (Firma Digital Cuántica)
QKD	Quantum Key Distribution (Distribución de Clave Cuántica)
QKD-KMS	QKD Key Management System (Sistema de Gestión de Claves QKD)
QKDN	QKD Network (Red de Distribución Cuántica de Claves)
QNP	Certified Quantum Network Professional
QoS	Quality of Service (Calidad de Servicio)
QRNG	Quantum Random Number Generator (Generador Cuántico de Números Aleatorios)
QSA	Quantum Security Analyst
Qubit	Quantum Bit (Bit Cuántico)
RFP	Request For Proposal (Solicitud de Propuesta)
ROI	Return on Investment (Retorno de la Inversión)
RRHH	Recursos Humanos

COMUNICACIONES CUÁNTICAS SEGURAS: HOJA DE RUTA DE APLICACIONES HÍBRIDAS:
QKD+PQC

RSA	Rivest, Shamir, Adleman (Algoritmo de cifrado)
SA	Security Association (Asociación de Seguridad - IPsec)
SAE	Secure Application Entity (Entidad de Aplicación Segura)
SCA	Side-Channel Attacks (Ataques de Canal Lateral)
SCADA	Supervisory Control and Data Acquisition (Control de Supervisión y Adquisición de Datos)
SDN	Software Defined Networks (Redes Definidas por Software)
SHA	Secure Hash Algorithm (Algoritmo de Hash Seguro)
SKR	Secret Key Rate (Tasa de Clave Secreta)
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio)
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (Firma Digital basada en Hash sin estado)
SLI	Service Level Indicator (Indicador de Nivel de Servicio)
SLO	Service Level Objective (Objetivo de Nivel de Servicio)
SME	Small and Medium-sized Enterprises (PYMES)
SMF	Single Mode Fiber (Fibra Óptica Monomodo)
SNR	Signal-to-Noise Ratio (Relación Señal-Ruido)
SNSPD	Superconducting Nanowire Single-Photon Detector (Detector de Fotón Único de Nanocable Superconductor)
SOP	Standard Operating Procedure (Procedimiento Operativo Estándar)
SPAD	Single Photon Avalanche Diode (Fotodiodo de Avalancha de Fotón Único)
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión)
TF-QKD	Twin-Field QKD (QKD de Campo Gemelo)
TFM	Trabajo Fin de Máster
TIC	Tecnologías de la Información y Comunicación (ICT)
TLS	Transport Layer Security (Seguridad de la Capa de Transporte)
TN	Trusted Node (Nodo de Confianza)
TRL	Technology Readiness Level (Nivel de Madurez Tecnológica)
TTLB	Time-To-Last-Byte (Tiempo hasta el último byte)
UPS	Uninterruptible Power Supply (Sistema de Alimentación Ininterrumpida)
V2V	Vehicle-to-Vehicle (Vehículo a Vehículo)
VHL	Variables Ocultas Locales
VPN	Virtual Private Network (Red Privada Virtual)
WAN	Wide Area Network (Red de Área Amplia)
WDM	Wavelength Division Multiplexing (Multiplexación por División de Longitud de Onda)
XOR	Exclusive OR (O Exclusivo)

9 ANEXO II: PARADIGMA MOSCA

9.1 Paradigma MOSCA: Riesgo Cuántico y Migración Segura

El paradigma MOSCA (a menudo referido como el Teorema de Mosca por Michele Mosca) es un referente que se utiliza para cuantificar la urgencia y el riesgo que representa la Computación Cuántica Criptológicamente Relevante (CRQC), especialmente en el contexto de la amenaza Harvest Now, Decrypt Later (HNDL).

Este paradigma se aplica directamente para justificar la implementación temprana de soluciones de seguridad cuántica, como la QKD o PQC, al confrontar el tiempo necesario para la migración con el valor a largo plazo de los datos a proteger.

9.1.1 Definición del Teorema MOSCA

El modelo MOSCA se utiliza para estimar la línea de tiempo hasta que los activos de una organización se vuelven vulnerables a los ataques post-cuánticos. Este modelo establece una comparación de tiempos cruciales para determinar si la organización está en riesgo. Se tiene un problema grave si:

Tiempo de Migración (x)+Vida Útil de los Datos (y)>Tiempo hasta el CRQC (z) (Mosca, 2018)

Donde los componentes se definen de la siguiente manera en la tabla 9.1:

Componente	Definición	Relevancia en el Contexto Cuántico
x	Tiempo necesario para migrar y equipar la infraestructura con una solución cuánticamente segura (preparación post-cuántica).	La migración a criptografía cuántica/post-cuántica lleva años (se estima al menos cinco años).
y	Vida útil de los datos (o el período que los datos deben permanecer confidenciales después de la migración) / Tiempo necesario para que los datos sean seguros.	Datos como la propiedad intelectual, registros médicos, o secretos de seguridad nacional tienen una vida útil de décadas.
z	Tiempo hasta que el CRQC (Ordenador Cuántico Criptológicamente Relevante) esté disponible.	Se espera que el CRQC que puede romper la criptografía actual (RSA/ECC) esté disponible alrededor del año 2030.

Tabla 9-1. Explicación componentes formula MOSCA (Adaptado de NTB LM)

Si la suma del tiempo que se tarda en asegurar los datos (x) más el tiempo que esos datos deben mantenerse seguros (y) excede el momento en que se espera que el CRQC esté disponible (z), la información ya está en riesgo de ser comprometida. Este modelo es fundamental para justificar inversiones inmediatas en PQC y QKD para datos de larga duración.

9.1.2 La Urgencia Impulsada por HNDL y el CRQC

La necesidad de implementar soluciones de seguridad cuántica, como QKD, cuanto antes, se basa en la convergencia de dos amenazas temporales críticas

- La Amenaza Inminente del CRQC. El Algoritmo de Shor puede romper la criptografía asimétrica actual (RSA, ECC, DH) en tiempo polinomial si se ejecuta en un CRQC. La aparición de un CRQC hará que los cifrados clásicos ya no puedan evitar que los atacantes descifren los datos.
- La Realidad del Ataque HNDL. El ataque HNDL (también conocido como Store Now, Decrypt Later o descifrado retrospectivo) no es una amenaza futura, sino una amenaza activa e inmediata. Los atacantes roban y almacenan datos cifrados hoy (datos de larga duración) con la intención de descifrarlos más tarde cuando dispongan de un CRQC.
- Riesgo Amplificado por MOSCA. El riesgo es particularmente alto para los datos de larga duración (y grande), como los secretos de defensa, historiales médicos o propiedad intelectual. Si estos datos tienen una vida útil que se extiende más allá de la llegada del CRQC (principios de la década de 2030), el cumplimiento de la ecuación de Mosca ($x+y>z$) indica un problema grave, forzando a las organizaciones a empezar la migración de inmediato.

La aplicación del Paradigma MOSCA subraya la necesidad de una defensa inmediata y robusta. Aunque la PQC es la solución más escalable y se implementa por software (minimizando x , el tiempo de migración), la QKD se justifica como la solución definitiva contra HNDL debido a su fundamento físico, siendo la respuesta más fuerte para la amenaza HNDL según el marco MOSCA por las siguientes razones:

- Seguridad Incondicional: La QKD ofrece seguridad teóricamente incondicional (o perfecta), basada en las leyes inmutables de la mecánica cuántica (como el principio de incertidumbre y el teorema de no clonación). A diferencia de PQC, cuya seguridad es condicional (depende de supuestos matemáticos que podrían romperse en el futuro), la seguridad de QKD no se ve comprometida, sin importar el poder computacional futuro del atacante.
- Neutralización de la Amenaza HNDL: Dado que la QKD detecta inmediatamente cualquier intento de interceptación o medición del fotón (qubit) mediante la introducción de errores detectables (QBER), cualquier clave cuántica generada se descarta si ha sido espiada. Esto garantiza que el material de clave robado hoy carecerá del secreto incondicional necesario para el descifrado futuro, neutralizando el ataque HNDL para la información cifrada con esa clave.

Por lo tanto, si la vida útil de los datos críticos (y) se extiende significativamente más allá de la llegada estimada del CRQC (z), la implementación de QKD, a pesar de su mayor coste y complejidad de hardware, es crucial para proporcionar el blindaje físico incondicional que la PQC no puede garantizar a largo plazo, satisfaciendo la urgencia que impone el Teorema de Mosca.

Estableciendo una analogía: El paradigma MOSCA es como una fecha límite para almacenar provisiones críticas (y) antes de una tormenta (z). La PQC es una solución de almacenamiento rápida y barata (bajo x) pero con cerraduras matemáticas que podrían romperse más tarde. La QKD, aunque es un almacén caro y lento de construir (alto x), ofrece un blindaje físico inviolable, garantizando que las provisiones cruciales robadas hoy no serán utilizables cuando llegue la tormenta cuántica.

10 ANEXO III: COMPARATIVA CC & CQ: MATEMÁTICA Y FÍSICA

Análisis detallados de las diferencias matemáticas entre espacios vectoriales clásicos y espacios de Hilbert complejos, enfatizando cómo la unitariedad de las puertas cuánticas preserva la información (reversibilidad) frente a las puertas lógicas clásicas disipativas.

Mientras que la representación matemática del bit clásico es un valor discreto binario, la del qubit requiere el formalismo del álgebra lineal. El qubit se representa como un vector de estado en un espacio de Hilbert complejo de dos dimensiones, $\mathbb{C}^2$. Los estados base $|0\rangle$ y $|1\rangle$ forman la base computacional canónica.

La Esfera de Bloch

La representación geométrica del estado de un único qubit se realiza mediante la **Esfera de Bloch**. Cualquier estado de superposición puro $|\psi\rangle$ puede mapearse a un punto sobre la superficie de esta esfera unitaria tridimensional. La posición de este punto está definida por dos ángulos esféricos:

El estado se expresa, en coordenadas esféricas, como:

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\phi} \sin(\theta/2) |1\rangle$$

Donde la explicación de los componentes:

- $|\psi\rangle$ (Ket de psi): Representa el estado cuántico del sistema (un qubit, en este caso).
- $|0\rangle$ y $|1\rangle$: Son los estados base del qubit (el "arriba" y el "abajo", por ejemplo).
- $\cos(\theta/2)$ y $\sin(\theta/2)$: Son amplitudes de probabilidad (números reales) que indican la "cantidad" de cada estado base.
- $e^{i\phi}$: Es un factor de fase complejo, que añade información sobre la fase relativa entre los dos estados base.
- θ (ángulo polar), que va de 0 a π y ϕ (ángulo azimutal), que va de 0 a 2π : Son ángulos (coordenadas esféricas) que definen el punto exacto en la esfera de Bloch donde se encuentra el estado $|\psi\rangle$.

Esta representación no es solo una ayuda visual, sino una herramienta operacional. Las transformaciones de estados (la aplicación de puertas cuánticas) corresponden a rotaciones en la Esfera de Bloch, y estas rotaciones son implementadas por matrices de Pauli y otras matrices unitarias.

Característica	Bit Clásico (c-bit)	Qubit (q-bit)
Estado Fundamental	Determinista: 0 o 1	Superposición: $ \psi\rangle$
Capacidad (N unidades)	N estados posibles (Lineal)	2^N estados representados simultáneamente (Exponencial). (Nielsen & Chuang, 2010)
Representación Matemática	Valor discreto (0 o 1)	Vector en el Espacio de Hilbert $\mathbb{C}^2$ (Esfera de Bloch). (Nielsen & Chuang, 2010)
Transformación (Puertas)	Puertas Booleanas (No reversibles, excepto NOT)	Puertas Unitarias (Reversibles).

Tabla 10-1. Comparación Dimensional y Funcional del Bit y el Qubit (Adaptado de NTB LM)

11 ANEXO IV: PUERTAS CUÁNTICAS

11.1 Puertas cuánticas

La computación clásica y la computación cuántica, aunque ambas utilizan compuertas (o puertas) lógicas como bloques fundamentales para procesar información, operan bajo paradigmas físicos y matemáticos fundamentalmente diferentes.

Las compuertas clásicas manipulan bits basados en la lógica booleana y la física clásica, mientras que las compuertas cuánticas manipulan cúbits basándose en las leyes de la mecánica cuántica (superposición, entrelazamiento e interferencia).

A continuación, se presenta una comparativa detallada entre ambos tipos de compuertas.

Característica	Compuertas Clásicas	Compuertas Cuánticas
Unidad de Información	<i>Bit</i> (Binary Digit), que solo puede ser 0 o 1.	<i>Qubit</i> (Quantum Bit), que puede existir en superposición de 0 y 1
Fundamento de Operación	<i>Lógica Booleana</i> (Álgebra de Boole). Las operaciones se basan en la conmutación de transistores que siguen leyes de la física clásica.	<i>Mecánica Cuántica</i> (Álgebra Lineal Compleja). Manipulan cúbits mediante operaciones unitarias.
Reversibilidad	<i>Generalmente Irreversible</i> (ej. AND, OR), ya que se pierde información sobre las entradas.	<i>Reversible</i> (Unitaria e Invertible). La unitariedad ($U^\dagger U = I$) asegura que no se pierde información ni se destruye la superposición.
Representación	<i>Tablas de verdad</i> que definen la salida binaria. Circuitos que manipulan 0s y 1s.	<i>Matrices unitarias</i> que operan sobre vectores de estado en el espacio de Hilbert. Las entradas y salidas son estados cuánticos (<i>amplitudes complejas</i>).
Tipos Comunes	NOT, AND, OR, XOR, NAND. Compuertas reversibles (Fredkin, Toffoli).	Hadamard (H), Pauli-X (NOT cuántico), Pauli-Z, CNOT (control-NOT), Rotacionales (RX, RY, RZ), Tofoli (cuántico).
Conjunto Universal	Ejemplos: {NOT, AND} o {NAND}. También {Toffoli, NOT} es universal y reversible.	Compuertas de un solo cúbit + CNOT. También {Hadamard, Phase, CNOT, $\pi/8$ gate}

Tabla 11-1. Comparativa de Compuertas: Clásicas & Cuánticas (Adaptado de Perplexity)

11.2 El Fundamento Físico de la Información

11.2.1 Bits Clásicos y Compuertas Irreversibles

En la computación clásica, la unidad mínima de información es el bit, que se materializa mediante estados discretos y bien definidos, como el paso o no de corriente eléctrica a través de un transistor.

- **Estados Definidos:** Un bit solo puede ser 0 o 1 en un momento dado.
- **Irreversibilidad:** Las compuertas clásicas fundamentales (como AND y OR) son funciones booleanas que típicamente pierden información sobre la entrada cuando se calcula la salida. Por ejemplo, si una compuerta AND emite un 0, no se puede saber si las entradas fueron (0, 0), (0, 1) o (1, 0). Esta pérdida de información hace que la operación sea irreversible.
- **Cálculo = Física Clásica:** El cálculo en la computación clásica se reduce al uso de las leyes que controlan a los electrones en los transistores.

11.2.2 Qúbits Cuánticos y Compuertas Unitarias

El cúbit es la unidad fundamental de la computación cuántica. A diferencia del bit, el cúbit puede existir en una superposición lineal de $|0\rangle$ y $|1\rangle$ a la vez, con amplitudes complejas (α y β) que determinan la probabilidad de obtener cada estado al medir.

- **Superposición y Entrelazamiento:** El cúbit aprovecha las leyes de la mecánica cuántica, como la superposición y el entrelazamiento. La capacidad de un sistema de n cúbits de representar 2^n estados simultáneamente es la base del paralelismo cuántico.
- **Unitariedad y Reversibilidad:** Las compuertas cuánticas deben ser operadores unitarios ($U^\dagger U = I$), lo que significa que son reversibles. Esta reversibilidad es clave, ya que la evolución de un sistema cuántico debe ser unitaria para preservar la superposición y las probabilidades (la suma de probabilidades debe ser igual a 1 en cualquier momento). Una operación irreversible resultaría en la pérdida de información y causaría el colapso de la superposición.
- **Medición vs. Operación:** En la computación cuántica, el cálculo se realiza aplicando transformaciones unitarias al cúbit. Es crucial que estas transformaciones sean unitarias para evitar la decoherencia (pérdida de la coherencia cuántica), que ocurre cuando el cúbit interactúa con el entorno o es medido, obligando al estado a colapsar a un valor clásico definido (0 o 1).
- **Equivalentes Cuánticos de Compuertas Clásicas.** Existen compuertas cuánticas que son el análogo directo de las compuertas clásicas, así como compuertas puramente cuánticas, como la Hadamard.
 - **Compuertas Sencillas (Análogos al NOT).** Estas actúan sobre un solo qubit y realizan rotaciones en la Esfera de Bloch.
 - **Puerta Hadamard (H):** Es la puerta más importante para la inicialización, ya que convierte un estado base (e.g., $|0\rangle$) en una superposición equidistribuida: $H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$
 - **Puerta NOT Cuántica (X):** Se representa por la matriz de Pauli X y es el análogo cuántico del NOT clásico, invirtiendo los estados base.
 - **Puertas de Fase (S, T, Z, R):** Estas puertas aplican desplazamientos de fase a los estados, esenciales para la universalidad de la computación cuántica. Por ejemplo, la puerta Z invierte la fase del estado $|1\rangle$, y las puertas S y T aplican rotaciones de fase específicas ($S^2=Z$ y $T^2=S$) necesarias para construir cualquier operación cuántica compleja.
 - **Compuertas Multiqubit y Universales**

Concepto Clásico	Concepto Cuántico	Función/Rol
AND, OR, XOR	Compuertas reversibles	Las compuertas clásicas AND y OR son irreversibles. Sin embargo, la compuerta Toffoli (CCNOT) es una compuerta clásica

	(Toffoli, Fredkin, CNOT)	reversible universal que puede usarse para simular puertas AND, OR y NOT. Según Nielsen & Chuang (2010).
Universalidad Clásica	Universalidad Cuántica	El conjunto {Compuertas de un solo cúbit + CNOT} es universal, lo que significa que cualquier operación unitaria arbitraria puede implementarse con estas compuertas. El conjunto de compuertas cuánticas subsume a los circuitos clásicos.

Tabla 11-2. Compuertas Multicúbit y Universales (Adaptado de Perplexity)

- Compuertas Clave para el Paradigma Cuántico. Existen compuertas que son esenciales para el funcionamiento de la computación cuántica y no tienen un análogo funcional simple en el mundo clásico (aparte de la Hadamard, que no es un análogo de una compuerta clásica, sino que crea un fenómeno cuántico):
 - Hadamard (H): Es una compuerta fundamental de un solo cúbit que transforma los estados base en *superposiciones equiprobables*. Es crucial para crear *el paralelismo cuántico al inicio de un algoritmo*.
 - Controlled-NOT (CNOT): Es la compuerta multicúbit prototípica, *esencial para introducir el entrelazamiento*. La CNOT aplica una operación X (NOT) al cúbit objetivo si, y solo si, el cúbit de control está en $|1\rangle$.
 - Compuertas de Rotación (R_x , R_y , R_z): *Permiten rotaciones continuas del estado del cúbit en la esfera de Bloch*. Esto es posible porque los operadores cuánticos no están restringidos a tener elementos discretos (0s y 1s), sino que pueden ser continuos y versátiles.

11.3 Implicaciones en Criptografía y Seguridad

Las diferencias entre las compuertas clásicas y cuánticas tienen consecuencias directas en la seguridad de la información:

- Clonación: En la criptografía clásica, la información (bits) puede copiarse y reenviarse perfectamente sin modificar el mensaje original. En contraste, el *Teorema de No Clonación* (que se deriva de la linealidad de la evolución unitaria cuántica) establece que es *imposible clonar un estado cuántico arbitrario desconocido*. Esta imposibilidad es la *base de la seguridad en la Criptografía Cuántica* (QKD), ya que cualquier intento de espionaje (medir o copiar los cúbits) perturba el estado y se detecta inmediatamente.
- Vulnerabilidad: Los métodos de criptografía tradicionales (clásica) se basan en algoritmos matemáticos que pueden romperse con suficiente poder informático. Los ordenadores cuánticos, al explotar el paralelismo cuántico (logrado mediante superposición creada por compuertas como Hadamard) e interferencia, pueden ejecutar algoritmos como el de Shor, que rompe el cifrado asimétrico clásico (RSA, Diffie-Hellman) en tiempo polinómico, una tarea que a las máquinas clásicas les tomaría cientos o miles de años.
- Seguridad Incondicional: Mientras que la seguridad clásica es condicional (depende de la dificultad matemática y el poder computacional del atacante), la criptografía cuántica ofrece seguridad incondicional o perfecta, ya que se basa en principios físicos inviolables como el principio de incertidumbre y el teorema de no clonación.

Las compuertas cuánticas son los bloques de construcción (building blocks) fundamentales de los algoritmos y circuitos cuánticos. A diferencia de las puertas lógicas clásicas (como AND, OR), las compuertas cuánticas operan sobre cúbits mediante operaciones unitarias y reversibles, lo que significa que modifican el vector de estado sin pérdida de información y preservan la coherencia global del estado cuántico.

Una compuerta cuántica que actúa sobre n cúbits puede representarse mediante una matriz unitaria de grado 2^n . El conjunto de compuertas que afectan a un solo cúbit, junto con las compuertas de dos cúbits (como la CNOT), forman un conjunto universal con el que se puede construir cualquier programa cuántico.

A continuación, se presenta un cuadro detallado con los tipos de compuertas cuánticas clasificadas según si operan sobre un único cúbit (uniquubit) o sobre múltiples cúbits (multiqubit).

11.3.1 Cuadro de Compuertas Cuánticas (Uniquubit y Multiqubit)

Tipo de Compuerta	Qúbits Requeridos	Notación Común	Función Principal / Descripción
Hadamard	1 (Uniquubit)	H	Transforma los estados base computacionales
Pauli-X (NOT)	1 (Uniquubit)	X	Es el análogo cuántico de la puerta NOT clásica. Intercambia los estados base
Pauli-Z (Phase Flip)	1 (Uniquubit)	Z	Conocida como la compuerta de inversión de fase. Preserva
Pauli-Y	1 (Uniquubit)	Y	Combina la permutación y el cambio de fase con un factor imaginario. Es una rotación discreta alrededor del eje Y.
Rotación (General)	1 (Uniquubit)	$RX(\phi)$, $RY(\phi)$, $RZ(\phi)$	Compuertas que implementan rotaciones continuas sobre el cúbit alrededor de los ejes X, Y o Z de la esfera de Bloch con un ángulo ϕ .
Phase Gate	1 (Uniquubit)	S	Compuerta que introduce un cambio de fase específico. Parte de conjuntos para construir compuertas arbitrarias.
$\pi/8$ Gate	1 (Uniquubit)	T	Compuerta de fase con $e^{i\pi/4}$. Es crucial para la descomposición de compuertas más complejas.
Controlled-NOT	2 (Multiqubit)	CNOT	Compuerta entrelazadora fundamental. Aplica una operación Pauli-X (NOT) al cúbit objetivo si, y solo si, el cúbit de control está en el estado
Toffoli	3 (Multiqubit)	CCNOT	Compuerta universal reversible clásica que utiliza dos cúbits de control para invertir condicionalmente un tercer cúbit objetivo (solo si ambos controles son 1).
Controlled-P (General)	≥ 2 (Multiqubit)	CP	Se pasa como parámetro la función de la puerta a aplicar. Realiza una operación P en un cúbit objetivo condicionado por el estado de uno o más cúbits de control.
SWAP	2 (Multiqubit)	SWAP	Intercambia completamente los estados cuánticos entre dos cúbits. Puede

			descomponerse en tres compuertas CNOT aplicadas secuencialmente.
Controlled-Z	2 (Multiqubit)	CZ	Aplica la matriz Pauli-Z al cúbit objetivo solo si el cúbit de control está en 1
Fredkin	3 (Multiqubit)	Controlled-SWAP	Intercambia dos cúbits si el cúbit de control es 0

Tabla 11-3. Compuertas Cuánticas (Uniqubit y Multiqubit) (Adaptada de Perplexity)

11.3.2 Información Adicional y Fundamentos

- Compuertas Uniqubit

Las compuertas de un solo cúbit se describen mediante matrices unitarias de 2×2 . La restricción de que la matriz sea unitaria ($U^\dagger U = I$) es la única limitación para que una matriz represente una compuerta cuántica válida.

- Puertas de Pauli (X, Y, Z): Estas matrices, al ser unitarias de 2×2 , son compuertas de un solo cúbit válidas. Por ejemplo, en la terminología de cúbits, el punto (0,0,1) en la Esfera de Bloch corresponde al autovector con autovalor positivo de la matriz de Pauli Z, y el punto opuesto (0,0,-1) corresponde al autovector con autovalor negativo. La Esfera de Bloch se utiliza para visualizar la acción de estas puertas lógicas.
- Hadamard (H): La aplicación de la compuerta Hadamard a un cúbit en el estado $|0\rangle$ o $|1\rangle$ es fundamental para crear la superposición inicial, permitiendo que un solo paso de computación se ejecute para múltiples valores a la vez (paralelismo cuántico).

- Compuertas Multiqubit

Las operaciones multiqubit, que actúan sobre dos o más cúbits, son esenciales porque son las responsables de introducir el entrelazamiento, un recurso cuántico sin equivalente clásico. Una compuerta de dos cúbits se puede implementar con una matriz de 4×4 .

- CNOT (Controlled-NOT): Esta compuerta es el prototipo de compuerta multiqubit. Su capacidad condicional es lo que permite construir estados de entrelazamiento como los estados Bell y es un ingrediente crucial para la teleportación cuántica y la corrección de errores.
- Toffoli (CCNOT): Es una compuerta multicontrol que utiliza dos cúbits como control para invertir condicionalmente un tercero. Es imprescindible para implementar operaciones lógicas reversibles clásicas dentro del marco cuántico. Su matriz de transición es una matriz de 8×8 .

El poder de una computadora cuántica radica en el procesamiento paralelo de superposiciones, lo que se logra manipulando los cúbits mediante secuencias de estas compuertas unitarias. Los cálculos cuánticos se definen como una secuencia de transformaciones unitarias seguidas de una medición.

12 ANEXO V: QRNG Y ORQUESTADOR SDN

12.1 Integración QRNG con HSM y KSM

La integración de un Generador Cuántico de Números Aleatorios (QRNG) con Módulos de Seguridad de Hardware (HSM) y Sistemas de Gestión de Claves (KMS) mejora significativamente la entropía y, por lo tanto, la seguridad de la generación de claves criptográficas.

- El funcionamiento de los ordenadores tradicionales utiliza generadores de números pseudoaleatorios (PRNG) que, aunque eficaces, se basan en algoritmos predecibles si se conoce la semilla inicial. Un QRNG, por el contrario, aprovecha fenómenos de la mecánica cuántica (como la medición de estados cuánticos o el ruido inherente de los fotones láser) para producir números verdaderamente aleatorios e inherentemente impredecibles.
- Al integrar un QRNG, los HSM y KMS pueden utilizar esta fuente de aleatoriedad genuina como una potente fuente de entropía para la creación de semillas y claves criptográficas, lo que hace que las claves sean mucho más robustas y resistentes a ataques de adivinación o fuerza bruta.
- La seguridad de los sistemas criptográficos modernos reside en la imposibilidad computacional de romper una clave secreta si esta es verdaderamente aleatoria y lo suficientemente larga. El QRNG asegura que el eslabón más débil, la aleatoriedad inicial, sea lo más fuerte posible.

Beneficios que aporta QRNG frente a PRNG:

- *Seguridad Reforzada:* Proporciona una base sólida para la seguridad criptográfica, garantizando que las claves generadas dentro del entorno seguro del HSM sean de la máxima calidad y aleatoriedad.
- *Cumplimiento Normativo:* Ayuda a las organizaciones a cumplir con estándares de seguridad rigurosos (como las directrices del NIST y FIPS 140-2) que exigen fuentes de entropía fuertes para la gestión de claves.
- *Casos de Uso Críticos:* Es especialmente valioso para aplicaciones que requieren un nivel extremadamente alto de confianza en la aleatoriedad, como la generación de claves para infraestructura de clave pública (PKI), transacciones financieras y seguridad de datos críticos.
- *Integración Sencilla:* La implementación se simplifica mediante el uso de APIs abiertas que permiten la integración de QRNG en arquitecturas de múltiples proveedores, eliminando la dependencia de soluciones propietarias.

En síntesis, la combinación de la seguridad física y lógica que ofrecen los HSM/KMS con la aleatoriedad genuina de los QRNG crea un sistema de gestión de claves altamente seguro y preparado para los desafíos criptográficos futuros.

12.2 SDN-QKD. El orquestador

La escalabilidad más allá de un enlace punto a punto requiere una gestión inteligente de la red, definida en el estándar ETSI GS QKD 015.

12.2.1 Arquitectura SDN-QKD

En una Red QKD (QKDN), el Controlador SDN no gestiona paquetes de datos, sino Recursos de Claves.

- **Modelo YANG:** La red se modela utilizando estructuras de datos YANG que definen parámetros como `link_id`, `max_absorption`, `qkdi_status` (estado de la interfaz) y `key_rate` disponible (ETSI, 2022).
- **Interfaz Norte (Orquestación):** El Controlador SDN expone una API hacia el Orquestador de Servicios. Cuando se provisiona un nuevo servicio crítico (ej. Conexión Sucursal Bancaria), el orquestador solicita un Flujo de Claves con un QoS específico.

12.2.2 Algoritmos de Enrutamiento de Claves

El enrutamiento en QKDN difiere fundamentalmente del enrutamiento IP.

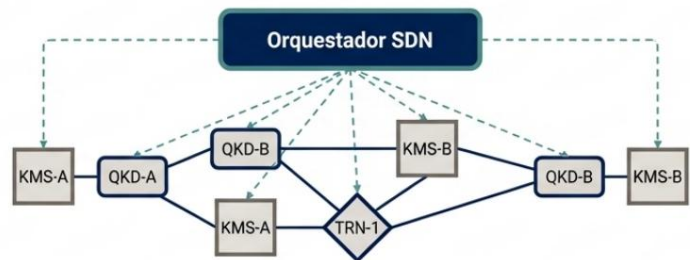
- **Métrica de Costo:** No es solo ancho de banda o latencia, sino *Disponibilidad de Claves*. El algoritmo de enrutamiento debe calcular si una ruta compuesta A-B-C tiene suficiente generación de claves en *ambos* saltos para sostener el servicio solicitado.
- **Balanceo de Carga:** Si el enlace directo A-B tiene alta atenuación y bajo SKR, el controlador SDN puede desviar la petición de claves por una ruta alternativa A-D-B que, aunque tenga más saltos, posea buffers de claves más llenos o enlaces de mejor calidad óptica (Wang et al., 2024).

El Cerebro de la Red: Orquestación SDN y Gestión del KMS

SDN-QKD (Software-Defined Networking para QKD)

Este paradigma desacopla el plano de control (lógica de red) del plano de datos cuánticos (transmisión de fotones), permitiendo la gestión centralizada y programable de la red QKD. (Fuente: SDN Orchestration...).

El Rol del Orquestador SDN (Ref: ETSI GS QKD 018)



El orquestador actúa como una capa de gestión superior. Sus funciones clave son:

1. **Enrutamiento de Claves:** Determina la ruta óptima para establecer un VQKP (Virtual Quantum Key Pool), seleccionando una cadena de nodos de confianza.
2. **Gestión de Nodos de Confianza:** Monitorea la salud y seguridad de los relés y puede re-enrutar dinámicamente el flujo de claves.
3. **Aplicación de Políticas (QoS):** Impone políticas de calidad de servicio como tasa de clave mínima ('min_bandwidth'), latencia máxima ('jitter'), y tiempo de vida de la clave ('ttl'). (Fuente: SDN Orchestration...).

Integración con el KMS

El orquestador instruye a los KMS sobre qué claves generar, a través de qué ruta y para qué aplicación, asegurando la sincronización de la política de claves de extremo a extremo.

Figura 12-1. SDN-QKD (Adaptado de NTB LM)

13 ANEXO VI: LOS SLA EN LA QKD

La seguridad teórica incondicional de QKD asume dispositivos ideales. La realidad física introduce imperfecciones que pueden ser explotadas mediante ataques de canal lateral (Side-Channel Attacks - SCA) (Matsuura et al., 2023).

13.1 Vulnerabilidades Críticas

13.1.1 Ataque de Cegado de Detectores (Detector Blinding):

- **Mecanismo:** El atacante (Eva) inyecta luz brillante continua en los detectores de Bob. Esto satura los fotodiodos de avalancha (APD), forzándolos a operar en modo lineal clásico en lugar de modo Geiger. Eva puede entonces controlar cuándo el detector genera un "click" enviando pulsos brillantes sincronizados, dictando efectivamente la clave.
- **Impacto:** Compromiso total de la seguridad sin aumentar el QBER.

13.1.2 Ataque de Caballo de Troya (Trojan Horse):

- **Mecanismo:** Eva envía pulsos de luz *hacia* el transmisor de Alice a través de la fibra cuántica y analiza la reflexión (back-reflection). Si los moduladores de fase o intensidad de Alice reflejan parte de la luz, Eva puede leer el estado cuántico que Alice acaba de preparar.

13.1.3 Ataque de Desplazamiento Temporal (Time-Shift):

- **Mecanismo:** Se explota la diferencia en las eficiencias de detección de los distintos detectores de Bob en función del tiempo. Eva desplaza temporalmente el fotón para que llegue en un momento donde un detector específico es más sensible que el otro, sesgando la probabilidad de detección y revelando la base de medición.

13.2 Contramedidas y Seguridad por Diseño

13.2.1 Monitor de Potencia (Watchdog):

- **Mecanismo:** Instalar fotodetectores clásicos a la entrada de Bob para monitorizar la potencia óptica media. Si supera el nivel de fotón único, se detecta el intento de cegado y se corta la conexión (EMPIR, 2018).

13.2.2 Aisladores Ópticos:

- **Mecanismo:** Implementar múltiples etapas de aisladores ópticos y circuladores en la salida de Alice para atenuar cualquier señal entrante (ataque troyano) por debajo del nivel de ruido detectable (> 60-70 dB de aislamiento).

13.2.3 MDI-QKD (Measurement-Device-Independent):

- **Mecanismo:** Una arquitectura avanzada donde los detectores se colocan en un nodo central "Charlie" que no necesita ser confiable. Alice y Bob envían fotones a Charlie, quien realiza una medición de estado de Bell. Esto elimina todos los canales laterales relacionados con la detección, aunque aumenta la complejidad de implementación.

14 ANEXO VII: QKD CON TN EN SEDE-DELEGACIÓN

Se analiza a continuación un caso práctico de alta relevancia para el TFM como es la conexión segura entre una Sede Central (Madrid) y una Delegación Regional (Toledo), separadas por una distancia geográfica de 70 km, lo que se traduce en una longitud de fibra física de aproximadamente 85 km debido al trazado de infraestructura.

14.1 Presupuesto de Enlace Óptico (Link Budget)

La viabilidad física es el primer filtro.

- *Pérdida por Fibra*: $85 \text{ km} \times 0.22 \text{ dB/km} = 18.7 \text{ dB}$. (Se usa 0.22 para ser conservador por envejecimiento de fibra).
- *Pérdidas por Conectores*: Se asumen 6 puntos de parcheo (ODF) en la ruta. $6 \times 0.5 \text{ dB} = 3.0 \text{ dB}$.
- *Pérdida Total del Canal*: 21.7 dB.

14.2 Selección Tecnológica y Análisis de Rendimiento

- *CV-QKD*: A 21.7 dB, la mayoría de los sistemas CV-QKD comerciales operan cerca de su límite de ruido. La tasa de clave secreta (SKR) caería drásticamente o el sistema sería inestable debido a la sensibilidad al ruido de fase y térmico (Miloslavskaya, 2024).
- *DV-QKD*: Un sistema basado en el protocolo BB84 con Estados Señuelo (Decoy States) es la opción viable.
- *Rendimiento Esperado*: Según especificaciones de sistemas comerciales (ej. ID Quantique Cerberis XGR o Toshiba), a 21.7 dB se puede esperar un SKR de aproximadamente 1.5 kbps a 3 kbps (Huttner, 2013).

14.3 Modelo de Consumo y Buffer de Claves

- *Demanda de Seguridad*: La política de seguridad exige rotar la clave AES-256 cada 60 segundos.
- *Tasa de Consumo*: $256 \text{ bits} / 60 \text{ s} \sim 4.3 \text{ bps}$.
- *Balance*: La generación (1500 bps) supera ampliamente el consumo (4.3 bps).
- *Estrategia de Buffer*: El excedente de claves se almacena en el KMS. Esto es crucial para la resiliencia. Si el enlace QKD sufre una interrupción temporal (ej. mantenimiento de fibra), el KMS puede servir claves desde el buffer durante horas antes de agotarse.
- *Cálculo de Reserva*: En 1 hora de operación normal, se generan $1500 \times 3600 = 5.4 \text{ Mbits}$. Se consumen $4.3 \times 3600 = 15.4 \text{ kbits}$. El sistema acumula un remanente masivo, permitiendo incluso soportar múltiples túneles paralelos o ráfagas de consumo.

14.4 Análisis de Nodos de Confianza (Trusted Nodes)

Si la **delegación estuviera a 150 km**, la pérdida sería $>33 \text{ dB}$, haciendo inviable un enlace directo (el SKR sería cercano a 0 o inestable).

- *Solución*: Implementar un Trusted Node (TN) intermedio.
- *Arquitectura*: Sede Central en Madrid-TN (75km)- Delegación Regional en Toledo (75km).
- *Implicaciones de Seguridad*: El TN es un punto de vulnerabilidad clásica. En él, las claves cuánticas se descifran a texto plano en la memoria del KMS para ser re-cifradas hacia el siguiente salto.

- *Requisito Físico:* El TN debe estar alojado en un búnker de seguridad física (Certificación UNE-EN 1143-1 Grado 4, jaula de Faraday, control biométrico) para evitar acceso físico o ataques de canal lateral electromagnético (TEMPEST). *Esta es la principal limitación de escalabilidad de las redes QKD actuales frente a la promesa futura de los repetidores cuánticos.*

15 ANEXO VIII: DIAGRAMAS DE ARQUITECTURA Y SECUENCIAS DE PROTOCOLO

La integración práctica requiere modificar los flujos de comunicación tradicionales. A continuación, se detallan las secuencias operativas para la fase de autenticación (PQC) y la fase de cifrado de transporte (QKD).

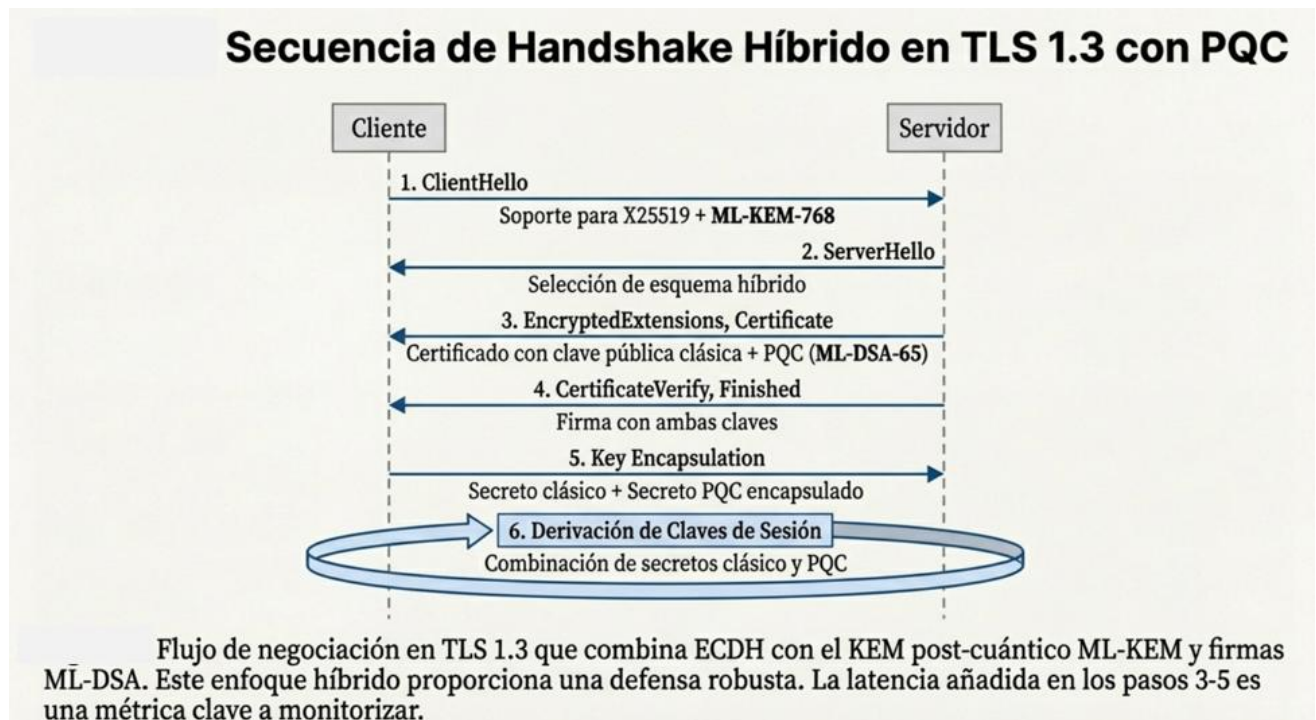


Figura 15-1. Secuencia TLS 1.3 con ML-KEM y ML-DSA (Adaptada de NTB LM)

15.1 Secuencia TLS 1.3 con ML-KEM y ML-DSA

La introducción de algoritmos PQC en TLS 1.3 altera significativamente el tamaño de los mensajes de handshake, lo que puede impactar en la latencia, especialmente en redes con pérdida de paquetes o congestión TCP.

15.1.1 Análisis del Flujo de Mensajes:

- Paso 1: Client Hello. El cliente envía el ClientHello. Además de proponer suites de cifrado, incluye la extensión key_share.
 - Impacto PQC: En un esquema híbrido (ej. X25519 + ML-KEM-768), el cliente debe enviar su clave pública ML-KEM. Para Kyber-768, esto añade 1,184 bytes. Esto puede empujar el tamaño del ClientHello por encima de la MTU estándar de Ethernet (1500 bytes), causando fragmentación IP o requiriendo múltiples segmentos TCP, lo que aumenta la probabilidad de retransmisiones (Aguado et al., 2021).

- Paso 2: Server Hello. El servidor responde con ServerHello, seleccionando la suite PQC y devolviendo su `key_share`.
 - Impacto PQC: El servidor realiza la operación de encapsulamiento y devuelve el Ciphertext de ML-KEM (aprox. 1,088 bytes).
- Paso 3: Autenticación (Certificate & Verify): Este es el punto más crítico. El servidor envía su cadena de certificados (Certificate) y la firma de la transcripción del handshake (CertificateVerify).
 - Impacto PQC: Si se utiliza ML-DSA (Dilithium-3), la clave pública en el certificado ocupa 1,952 bytes y la firma digital 3,293 bytes. Una cadena de confianza completa puede exceder fácilmente los 10 KB (Aguado et al., 2021).
 - La consecuencia es que, en *redes estables* de alto ancho de banda, el impacto en el Time-to-Last-Byte (TTLB) es menor al 5%. Sin embargo, en *redes congestionadas o con alta latencia*, el aumento de ventanas de congestión TCP puede degradar el tiempo de establecimiento de conexión en más del 30% (Aguado et al., 2021).
- Como alternativa se utiliza KEMTLS para mitigar el peso de las firmas ML-DSA, se investiga la arquitectura KEMTLS, donde la autenticación se realiza mediante encapsulamiento de claves (KEM) en lugar de firmas. El cliente encapsula un secreto hacia la clave pública de largo plazo del servidor (contenida en el certificado). Esto reduce el overhead, pero requiere que el cliente envíe datos cifrados antes de confirmar la identidad del servidor, cambiando el modelo de confianza (Cloudflare, 2020).

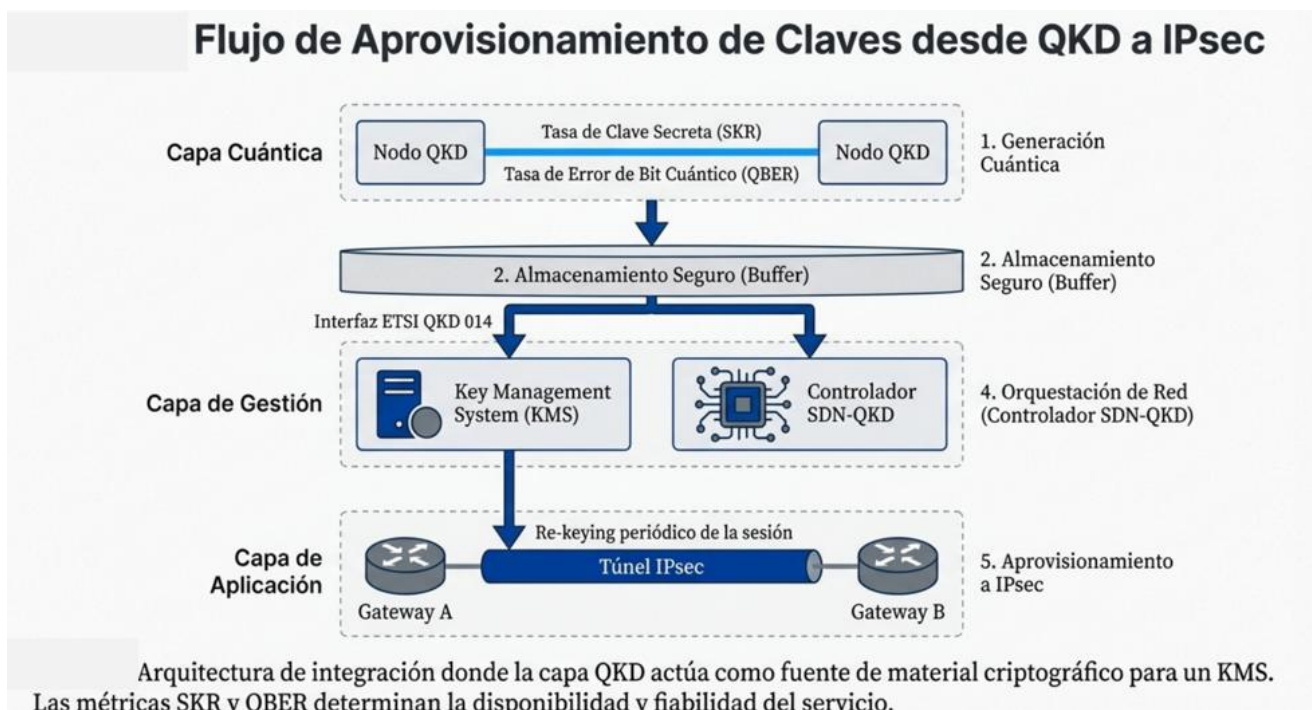


Figura 15-2. Flujo QKD-KMS-IPsec (ETSI GS QKD 014) (Adaptada de NTB LM)

15.2 Flujo QKD-KMS-IPsec (ETSI GS QKD 014)

Para el cifrado de la carga útil (Data Plane), se utiliza QKD para inyectar claves en túneles IPsec. Este proceso desacopla la generación de claves (Física) de su consumo (Red).

15.2.1 Diagrama de Secuencia Operativa:

- Fase de Generación y Sincronización (Capa Física):
 - Los dispositivos QKD (Alice y Bob) generan continuamente claves cuánticas en bruto (Raw Keys). Tras la reconciliación y amplificación de privacidad, las claves seguras se empujan a sus respectivos nodos KMS locales.
 - Los nodos KMS sincronizan los Key IDs (identificadores únicos UUID) y metadatos (calidad, tiempo de vida), pero nunca transmiten las claves reales por la red clásica.
- Fase de Solicitud de Claves (ETSI 014 API):
 - Paso A: La Entidad de Aplicación Segura maestra (SAE-A, ej. Firewall en Sede) determina que necesita rotar la clave IPsec. Envía una petición GET_STATUS a su KMS local para verificar disponibilidad de claves para el destino SAE-B.
 - Paso B: SAE-A envía una petición GET_KEY vía HTTPS (autenticado con mTLS). Payload JSON: {"number": 1, "size": 256, "slave_SAE_ID": "SAE-B-UUID"}.
 - Paso C: El KMS-A responde con un objeto JSON que contiene la clave (en Base64) y su key_ID.
- Fase de Negociación IKEv2 (Capa de Red):
 - Paso D: SAE-A inicia o actualiza el túnel IPsec con SAE-B. En lugar de realizar un intercambio Diffie-Hellman, SAE-A incluye el key_ID recibido en una carga útil de notificación o vendedor específica dentro del paquete IKE_AUTH o CREATE_CHILD_SA.
- Fase de Recuperación Esclava:
 - Paso E: SAE-B recibe el key_ID. Envía una petición GET_KEY_WITH_ID a su KMS local (KMS-B). Payload JSON: {"key_IDs": ["..."]}.
 - Paso F: KMS-B busca en su base de datos local segura, recupera la clave cuántica idéntica y la entrega a SAE-B.
- Fase de Cifrado:
 - Ambos extremos instalan la clave cuántica en la Security Association (SA) de IPsec y el tráfico comienza a fluir cifrado con AES-256-GCM.