

Doctorado en Informática

PKI de Próxima Generación: Estrategias de Migración Progresiva y Preparación Post-Cuántica para Entidades de Certificación

Lenin Alberto Vásquez González

Director: PHD. Rodrigo Cadena Martínez

Codirector: Dr. Jorge Hochstetter Diez

Quito, Ecuador, 27 de abril del 2026

Resumen

El presente proyecto de investigación abordó el problema de las Entidades de Certificación ecuatorianas con infraestructuras de clave pública - PKI basadas en RSA, que están poco preparadas frente a la amenaza cuántica, pero siguen siendo cada vez más costosas e ineficientes. Se propuso diseñar e implementar una estrategia integral de transición hacia una PKI de próxima generación basada en criptografía de curva elíptica - ECC, con preparación poscuántica - PQC en una Entidad de Certificación real del Ecuador. La investigación adoptó un enfoque mixto, crítico-hermenéutico y socio-técnico, combinando mediciones de desempeño en latencia, tamaño de certificados y cadenas, throughput, uso de CPU/RAM y compatibilidad con análisis normativo, organizacional y de gobernanza. Metodológicamente se enmarcó en Design Science Research, mediante el diseño y prueba de un artefacto compuesto por un modelo de migración por fases: piloto, emisión dual y convergencia, una matriz de riesgos, checklists de conformidad con estándares internacionales, indicadores de medición - KPIs técnicos y una guía de preparación PQC. En el entorno evaluado, los resultados indicaron que ECC presentó una reducción observable del tamaño de los certificados y mejoras en determinados indicadores de eficiencia operativa, creando margen para absorber el sobrecoste de algoritmos PQC. Asimismo, los resultados obtenidos en el entorno evaluado indican que una ruta de migración planificada, con criterios de paso y reversión, puede mantener altos niveles de continuidad del servicio, compatibilidad e interoperabilidad, al tiempo que fortalece la soberanía digital y la cripto-agilidad de la Entidad de Certificación en el caso institucional evaluado.

Palabras clave: PKI, criptografía de curva elíptica, criptografía poscuántica, cripto-agilidad, Entidad de Certificación.

Abstract

This research project addressed the challenges faced by Ecuadorian Certification Authorities operating Public Key Infrastructures (PKIs) based on RSA, which are insufficiently prepared to withstand the emerging quantum threat while becoming increasingly costly and inefficient. The study proposed the design and implementation of a comprehensive transition strategy toward a next-generation PKI based on Elliptic Curve Cryptography (ECC), with Post-Quantum Cryptography (PQC) readiness, within a real-world Certification Authority in Ecuador. The research adopted a mixed-methods, critical-hermeneutic, and socio-technical approach, combining performance measurements including latency, certificate and certificate-chain sizes, throughput, CPU/RAM utilization, and compatibility with regulatory, organizational, and governance analyses. Methodologically, the study was framed within Design Science Research (DSR) through the design and evaluation of an artifact comprising a phased migration model pilot, dual issuance, and convergence a risk matrix, compliance checklists aligned with international standards, technical Key Performance Indicators (KPIs), and a PQC readiness guide. Within the evaluated environment, the results indicated that ECC achieved an observable reduction in certificate sizes and improvements in selected operational efficiency indicators, thereby creating additional capacity to absorb the computational and operational overhead associated with PQC algorithms. Furthermore, the findings obtained in the evaluated environment suggest that a carefully planned migration roadmap, supported by clearly defined transition and rollback criteria, can maintain high levels of service continuity, compatibility, and interoperability while strengthening the Certification Authority's digital sovereignty and crypto-agility within the institutional case evaluated.

Keywords: PKI, elliptic-curve cryptography, postquantum cryptography, crypto-agility, Certification Authority.

Dedicatoria

A mi esposa,

Este proyecto de investigación está dedicado a ti, que has sido mi apoyo silencioso y mi fuerza en los momentos en que pensé que no podría continuar.

Gracias por tu paciencia por tu comprensión y por tu amor constante que me sostuvo incluso cuando el cansancio y las dudas querían ganar la batalla.

Cada página de este trabajo lleva algo de ti: tu sacrificio, tus palabras de ánimo, tus oraciones, tu confianza en mí. Tú me enseñaste que los sueños son más alcanzables cuando se caminan en equipo y con Dios como centro de nuestro hogar, y que el verdadero logro no es solo obtener un título, sino llegar hasta aquí sin perder lo más valioso nuestra unión, nuestra fe y nuestro amor.

Por todo lo que has dado, por todo lo que hemos pasado juntos y por todo lo que vendrá, este proyecto de investigación te lo dedico con todo mi corazón.

Agradecimientos

En primer lugar, agradezco a Dios, fuente de vida, sabiduría y fortaleza, por haberme permitido llegar hasta este momento, en los días de cansancio, de dudas y de silencio, sentí Su guía sosteniéndome y recordándome que cada esfuerzo tiene sentido cuando se ofrece con humildad y gratitud.

A mi esposa, compañera fiel de este camino, gracias por tu amor incondicional, tu paciencia ante mis ausencias, tus palabras de ánimo cuando el proyecto parecía no avanzar y por creer en mí, incluso cuando yo mismo no lo hacía. Este logro también es tuyo, porque detrás de cada página hay noches compartidas, sacrificios y renuncias que solo tú y yo conocemos.

A mis hijos, que son mi mayor motivo para seguir creciendo, gracias por enseñarme, con su sonrisa, que vale la pena luchar por un futuro mejor. Ustedes han sido mi inspiración constante para demostrar que, con disciplina, fe y perseverancia, los sueños se pueden alcanzar.

Extiendo también mi profundo agradecimiento a la empresa Security Data, por la confianza depositada en mí, por el apoyo brindado durante este proceso, su apertura, orientación y respaldo han sido fundamentales para que este trabajo no se quede solo en la teoría, sino que se proyecte como una contribución concreta al desarrollo tecnológico y a la seguridad digital.

A todos ellos, y a quienes de una u otra forma han estado presentes con su consejo, su tiempo o una palabra de aliento, muchas gracias. Este proyecto de investigación es un reflejo de un esfuerzo personal.

Contenido

Resumen ii

Abstract iii

Dedicatoria v

Agradecimientos vi

Lista de tablas y figuras xiv

Introducción 1

Capítulo 1. 4

1.1. Problema 4

1.2. Justificación 6

1.2.1. Justificación técnico-operativa 6

1.2.2. Relevancia académica y disciplinar 7

1.2.3. Relevancia normativa e interoperabilidad 7

1.2.4. Soberanía digital y contexto latinoamericano 7

1.3. Objetivo 8

1.3.1. Objetivo General 8

1.3.2. Objetivos Específicos 8

1.4. Hipótesis o supuesto hipotético 8

1.4.1. H1 – Comparativo técnico-operativo: 9

1.4.2. H2 – Factores condicionantes: 9

1.4.3. H3 – Escenarios por fases: 10

1.4.4 H4 – Preparación pos-cuántica: 10

1.5. Variables o Categoría de análisis 10

Capítulo 2. 17

2.1. Estado del Arte 17

2.1.1. Antecedentes 17

2.1.1.1. Origen de la criptografía de clave pública y surgimiento de la PKI 17

2.1.1.2. Consolidación de la WebPKI y expansión a servicios críticos 18

2.1.1.3. Incidentes históricos y limitaciones estructurales de la PKI 20

2.1.1.4. PKI en identidad digital, gobierno electrónico y contexto latinoamericano/ecuatoriano 21

2.1.1.5. Síntesis socio-técnica de los antecedentes 23

2.1.2. Fundamentos técnicos, estratégicos y normativos en la transición a PKI con ECC 24

2.1.2.1 Ventajas técnicas y operativas de ECC 24

2.1.2.2. Estrategias de adopción tecnológica: modelos híbridos y progresivos 25

2.1.2.3. Condicionamientos normativos y gobernanza técnica de la PKI 26

2.1.2.4. Consideraciones para entornos soberanos y latinoamericanos 28

2.1.2.5. Comparativa: RSA vs. ECC 28

2.1.3. Estudios de caso y experiencias internacionales en la adopción de ECC 30

2.1.3.1. Estonia, Corea del Sur y Emiratos Árabes Unidos como referencias de adopción 30

2.1.3.2. Lecciones para América Latina y el caso ecuatoriano 32

2.1.3.3. Síntesis comparativa 32

2.1.4. Descentralización de la confianza, identidad digital y tecnologías emergentes 34

2.1.5. Criptografía poscuántica, transición híbrida y preparación de la PKI 36

2.1.6. Interoperabilidad, sistemas legados y gestión del cambio 39

2.1.7. Síntesis: hacia una PKI de próxima generación 40

2.2. Trabajos relacionados 40

2.2.1. Hadan, Serrano & Camp (2021): Fallos reales vs. percepciones en la WebPKI 40

2.2.2. Girón et al. (2024): Emisión automatizada de certificados PQC 42

2.2.3. Sosnowski et al. (2023): desempeño de TLS 1.3 con algoritmos PQC 44

2.2.4. Astrizi & Custódio (2024): Transición híbrida a PQ-TLS 46

2.2.5. Hohm, Heinemann & Wiesmaier (2025): modelo de madurez CAMM 47

2.2.6. Cuadro comparativo de trabajos relacionados 49

2.2.7. Síntesis del estado del arte y brecha de investigación 52

2.3. Marco teórico-conceptual 54

2.3.1. Ejes conceptuales del modelo de PKI de próxima generación 55

2.3.2. Teorías fundamentales que sustentan el modelo 57

2.3.3. Relación entre los ejes teóricos y la propuesta de PKI de próxima generación 61

2.3.4. Marco histórico 63

2.3.5. Marco referencial 64

2.3.6. Marco legal 66

Capítulo 3. 70

3.1. Propuesta metodológica 70

3.1.1. Enfoque 70

3.1.2. Diseño de investigación 70

3.1.2.1. Diagnóstico y problematización 71

3.1.2.2. Diseño del artefacto: 71

3.1.2.3. Implementación piloto y evaluación experimental: 72

3.1.2.4. Refinamiento e integración: 72

3.2. Población y muestra 72

3.2.1. Descripción del Contexto: Escenario o lugar 72

3.2.2. Especificar el tipo de muestreo y cómo lo realizó 73

3.2.3. Criterios de selección y exclusión - no probabilístico 74

3.3. Instrumentos, método de validación y descripción del procedimiento de aplicación 75

3.3.1. Instrumento 75

3.3.2. Método de validación del Instrumento 76

3.3.3. Descripción del procedimiento de aplicación 77

3.3.4. Consideraciones éticas 78

3.4. Matriz de Variables 79

3.5. Establecimiento de Metodología por Objetivos 82

3.6. Implementación 84

3.6.1. Implementación del OE1: Estudio experimental RSA versus ECC 85

3.6.1.1. Planeación y preparación del entorno 85

3.6.1.2. Ejecución de pruebas 86

3.6.1.3. Estrategia de análisis de resultados 87

3.6.2. Implementación del OE2: Factores condicionantes y matriz de riesgos 88

3.6.2.1. Revisión documental y análisis hermenéutico 88

3.6.2.2. Elaboración de la matriz de riesgos 89

3.6.3. Implementación del OE3: Escenario progresivo de migración 90

3.6.3.1. Síntesis de requisitos y restricciones 90

3.6.3.2. Diseño de perfiles X.509 y políticas criptográficas 91

3.6.3.3. Modelado del escenario por fases 92

3.6.3.4. Checklists y validación iterativa 93

3.6.4. Implementación del OE4: Guía de preparación pos-cuántica 93

3.6.4.1. Marco conceptual PQC aplicado 94

3.6.4.2. Contenido de la guía PQC 94

3.6.4.3. Validación y cierre del ciclo de diseño 95

3.7. Pruebas 95

3.7.1. Escenarios de prueba simulados 96

3.8. Trazabilidad y reproducibilidad 96

Capítulo 4. 99

4.1. Resultados por Objetivo 99

4.1.1. Resultados del Objetivo Especifico 1 – OE1 99

4.1.1.1 Rendimiento por algoritmo y carga 99

4.1.1.2 Tamaño de certificados y cadenas 102

4.1.1.3. Uso de recursos 104

4.1.2 Resultados del Objetivo Especifico 2 – OE2 104

4.1.2.1 Principales hallazgos de la matriz de riesgos 105

4.1.3 Resultados del Objetivo Especifico 3 – OE3 106

4.1.4. Resultados del Objetivo Especifico 4 – OE4 109

4.2. Análisis 110

4.2.1. Análisis Objetivo Específico 1 – OE1 111

4.2.2. Análisis Objetivo Específico 2 – OE2 112

4.2.3. Análisis Objetivo Específico 3 – OE3 113

4.2.4. Análisis Objetivo Específico 4 – OE4 114

4.3. Discusión 116

4.3.1. Comparación con trabajos empíricos recientes 116

4.3.1.1. Hadan, Serrano & Camp (2021) – fallos reales vs percepciones en la WebPKI 116

4.3.1.2. Giron et al. (2024) – emisión automatizada de certificados PQC 117

4.3.1.3. Sosnowski et al. (2023) – desempeño de TLS 1.3 con algoritmos PQC 118

4.3.1.4. Astrizi & Custódio (2024) – transición híbrida a PQ-TLS 118

4.3.1.5. Hohm, Heinemann & Wiesmaier (2025) – modelo de madurez de cripto-agilidad (CAMM) 119

4.3.2. Relación con teorías fundamentales 120

4.3.3. Aporte original del estudio, implicaciones prácticas y futuras investigaciones 122

Capítulo 5. 125

5.1. Conclusiones 125

5.2. Recomendaciones 126

5.3. Limitaciones y desafíos 129

Referencias Bibliográficas 131

Anexos 139

Anexo A. Protocolo técnico de pruebas RSA-ECC/PQC 139

Anexo B. Matriz normativo-organizacional y de riesgos 141

Anexo C. Guion de entrevista semiestructurada 142

Anexo D. Ficha de validación por juicio experto 143

Anexo E. Modelo de consentimiento informado y confidencialidad 144

Anexo F. Plantilla de reproducibilidad y protocolo recomendado para nuevas réplicas 145

Lista de tablas y figuras

Tablas

Tabla 1 Operacionalización de las Variables independientes 12

Tabla 2 Operacionalización de las Variables dependientes 13

Tabla 3 Operacionalización de las Variables de control 15

Tabla 4 Comparación técnica y operativa entre RSA y ECC en el contexto de Infraestructuras de Clave Pública 29

Tabla 5 Comparación de estrategias internacionales de adopción de criptografía de curva elíptica (ECC) en Infraestructuras de Clave Pública 33

Tabla 6 Cuadro comparativo de trabajos relacionados 50

Tabla 7 Teorías fundamentales 57

Tabla 8 Matriz de Variables 80

Tabla 9 Matriz de trazabilidad metodológica por objetivos específicos 83

Tabla 10 Desempeño bajo carga baja y alta 100

Tabla 11 Tamaño de certificados y cadenas por algoritmo 102

Tabla 12 KPIs por fase 107

Tabla 13 Contraste entre hipótesis y resultados de la investigación 123

Tabla 14 Registro de Información para las pruebas 139

Tabla 15 Matriz organizacional y de riesgos 141

Tabla 16 Ficha de validación por juicio de experto 143

Tabla 17 Plantilla de reproducibilidad 145

Figuras

Figura 1 Latencia media de validación bajo carga alta 101

Figura 2 Throughput de emisión bajo carga alta 101

Figura 3 Tamaño de certificados y cadenas por algoritmo 103

Figura 4 Distribución de riesgo residual tras mitigación 105

Figura 5 Latencia por fase 108

Figura 6 Throughput por fase 108

Figura 7 Compatibilidad, Conformidad y PQC readiness por fase 109

Introducción

Las Infraestructuras de Clave Pública - PKI[1] y Entidades de Certificación - EC sostienen servicios de confianza digital mediante certificados X.509[2], mecanismos de validación, revocación y políticas de certificación. La evidencia reciente muestra que la confiabilidad de una PKI depende tanto de la criptografía como de la operación, la gobernanza, la configuración y la auditoría de sus procesos (Dumitrescu & Pouwelse, 2024; Hadan et al., 2021).

En paralelo, el ecosistema criptográfico atraviesa dos cambios relevantes. Primero, la criptografía de curva elíptica - ECC[3] permite alcanzar niveles de seguridad equivalentes a RSA[4] con claves y objetos criptográficos de menor tamaño y, en determinados escenarios, con menor costo operativo (Certauri, 2023; Priya, 2024). Segundo, la estandarización pos-cuántica del Instituto Nacional de Estándares y Tecnología - NIST[5] obliga a preparar las infraestructuras para futuras sustituciones algorítmicas; ML-KEM[6], ML-DSA y SLH-DSA formalizan esta transición y hacen de la cripto-agilidad una capacidad organizacional necesaria (NIST, 2024a; NIST, 2024b).

El problema científico no consiste, por tanto, en decidir si ECC es criptográficamente válido ni en anticipar una migración productiva inmediata a PQC[7]. Consiste en determinar cómo una EC regulada puede transitar de RSA hacia ECC de manera progresiva, medible, reversible y auditable, preservando continuidad operativa, interoperabilidad y conformidad normativa mientras

[1] PKI: Public Key Infrastructure - Infraestructura de Claves Públicas
[2] X.509: Estándar internacional que define el formato de los certificados de clave pública.
[3] ECC: Elliptic Curve Cryptography – Criptografía de Curva Elíptica
[4] RSA: Rivest-Shamir-Adleman – Técnica de cifrado Asimétrico
[5] NIST: National Institute of Standards and Technology
[6] ML-KEM: Module-Lattice Key Encapsulation Mechanism - Mecanismo de Encapsulación de Claves Basado en Módulos
[7] PQC: Post-Quantum Cryptography – Criptografía postcuántica

desarrolla capacidades de preparación pos-cuántica.

La investigación se desarrolló en una Entidad de Certificación específica del Ecuador y delimitó su validación a laboratorio y entornos controlados o preproductivos. Esta delimitación evita proyectar los resultados a todas las EC y permite separar dos niveles de evidencia: tendencias generales sustentadas por la teoría y los estándares; y resultados empíricos correspondientes exclusivamente a la infraestructura evaluada.

Metodológicamente se adoptó un enfoque mixto articulado con una perspectiva crítico-hermenéutica y Design Science Research - DSR[8]. La dimensión cuantitativa midió desempeño y compatibilidad; la dimensión cualitativa interpretó requisitos normativos, riesgos y condiciones organizacionales; y DSR integró ambas evidencias en el diseño, evaluación y refinamiento de un artefacto de transición.

El aporte original del estudio es la integración, en un único artefacto aplicable a una EC regulada, de cinco componentes que se suele abordar por separado: comparación técnico-operativa RSA-ECC, matriz de riesgos, estrategia por fases con criterios de paso y reversión, checklists normativos con KPIs, y guía de preparación pos-cuántica. El valor científico no radica en generalizar una solución universal, sino en ofrecer una estructura trazable y replicable que pueda ser validada posteriormente en otras organizaciones.

La investigación se organiza en cinco capítulos. El primero delimita el problema, la justificación, los objetivos, las hipótesis y las variables. El segundo desarrolla el estado del arte, la brecha de investigación y el marco teórico-conceptual. El tercero presenta la metodología, los instrumentos, las condiciones experimentales y la lógica de construcción del artefacto. El cuarto

[8] DSR: Investigación basada en la ciencia del diseño

reporta resultados, análisis y discusión. El quinto responde a los objetivos mediante conclusiones, recomendaciones y limitaciones.

Capítulo 1.

1.1. Problema

Describe limitaciones operativas asociadas a infraestructuras que mantienen RSA como esquema dominante como claves y certificados de mayor tamaño, mayores costos de determinadas operaciones criptográficas y dificultades de evolución cuando existen dependencias de clientes, módulos HSM[9], bibliotecas y perfiles X.509 heredados (Certauri, 2023; Priya, 2024). Estas tendencias generales no se asumen automáticamente como fallas de todas las Entidades de Certificación, sino que constituyen el marco de contraste para estudiar un caso concreto.

En la Entidad de Certificación analizada, el diagnóstico técnico estableció una línea base RSA-2048/SHA-256 en entorno controlado. En las condiciones documentadas del banco de pruebas, la validación registró 60 ms de latencia media en carga baja y 120 ms en carga alta; el throughput de emisión fue de 40 y 180 certificados por segundo, respectivamente; el consumo de CPU pasó de 35 % a 75 % y la memoria registrada de 600 MB a 900 MB. Adicionalmente, el certificado RSA evaluado tuvo un tamaño de 1,6 KB y la cadena completa 4,0 KB. Estos valores son datos del caso estudiado y no deben interpretarse como características universales de RSA ni de otras EC.

La comparación posterior con ECC P-256, realizada sobre la misma lógica de evaluación, mostró diferencias suficientes para justificar científicamente el estudio de una ruta de transición: bajo carga alta la latencia media observada fue 90 ms, el throughput[10] de emisión 210 certificados por segundo, el uso de CPU 65 % y la cadena completa 2,5 KB. La existencia de estas diferencias

[9] HSM: Hardware Security Module – Módulo de Seguridad de Hardware
[10] Throughput: Es la tasa o cantidad de producción que se logra en un período de tiempo determinado y puede variar según el contexto

no implica que ECC deba reemplazar RSA de forma inmediata; plantea la necesidad de evaluar si tales ventajas pueden mantenerse sin introducir incompatibilidades, incumplimientos normativos o riesgos de continuidad.

El problema comprobado es más específico que la tendencia descrita, es decir, la EC mantiene dependencias operativas y documentales asociadas a RSA y carece de una estrategia integral, reproducible y auditada que conecte el cambio hacia ECC con criterios de compatibilidad, conformidad, riesgo, reversión y preparación pos-cuántica.

A esta brecha se suma la evolución del marco pos-cuántico, la normalización de ML-KEM, ML-DSA y SLH-DSA por el NIST no convierte a PQC en una obligación productiva inmediata para la EC, pero sí exige inventariar dependencias, actualizar políticas y preparar mecanismos de cambio algorítmico. En un entorno regulado, la transición debe coordinar perfiles X.509, OCSP[11]/CRL, HSM, CP/CPS, auditoría y al nivel de servicio - SLA[12], por lo que el problema no puede reducirse a sustituir una primitiva criptográfica.

En consecuencia, el problema principal que aborda esta investigación es la ausencia, en la Entidad de Certificación objeto de estudio, de una estrategia de migración progresiva desde RSA hacia ECC con preparación pos-cuántica, validada en laboratorio y entornos controlados o preproductivos, que articule evidencia de desempeño, interoperabilidad, conformidad normativa, gestión del riesgo y mecanismos de reversión.

La pregunta de investigación es: ¿Cómo diseñar y validar, en una Entidad de Certificación específica del Ecuador y en entornos controlados o preproductivos, una estrategia de transición

[11] OCSP: Online Certificate Status Protocol – Protocolo de estado de Certificados en línea
[12] SLA: Service Level Agreement – Acuerdo de Nivel de Servicio

progresiva de PKI desde RSA hacia ECC con preparación pos-cuántica, que permita evaluar su viabilidad técnico-operativa, interoperabilidad y conformidad normativa sin extrapolar los resultados fuera del caso estudiado?

1.2. Justificación

La investigación se justifica por una brecha aplicada, donde existen estudios sobre eficiencia criptográfica, transición pos-cuántica, automatización y cripto-agilidad, pero son escasos los trabajos que integran estas dimensiones en un artefacto validable para una Entidad de Certificación regulada. El estudio aporta una estructura de decisión que conecta evidencia técnica, riesgo, normativa y preparación futura, sin asumir que una ventaja algorítmica equivale por sí sola a viabilidad institucional.

1.2.1. Justificación técnico-operativa

Técnicamente, el estudio permite comparar RSA y ECC bajo condiciones controladas y transformar esa evidencia en criterios de paso, reversión y monitoreo. La utilidad no consiste en proclamar la superioridad absoluta de ECC, sino en identificar bajo qué condiciones la EC analizada puede obtener mejoras de latencia, tamaño y uso de recursos manteniendo compatibilidad y continuidad. Esta optimización es además relevante como preparación para el mayor peso de objetos y operaciones pos-cuánticas (Sosnowski et al., 2023; Astrizi & Custódio, 2024).

1.2.2. Relevancia académica y disciplinar

La aportación científica es integradora y metodológica. Frente a trabajos centrados en incidentes WebPKI, rendimiento de TLS[13]-PQC, automatización ACME[14] o madurez de cripto-agilidad, esta investigación diseña y evalúa un artefacto que relaciona benchmark RSA-ECC, riesgo, conformidad, fases de transición y readiness PQC en un mismo caso de estudio regulado. Su replicabilidad debe entenderse como posibilidad de repetir el método, no como transferencia automática de sus resultados (Dumitrescu & Pouwelse, 2024; Serrano et al., 2019).

1.2.3. Relevancia normativa e interoperabilidad

Normativamente, el estudio traduce requisitos de NIST, ETSI, RFC aplicables y regulación ecuatoriana en criterios verificables de transición. El aporte consiste en conectar la conformidad documental con evidencia operacional mediante checklists, perfiles X.509, OCSP/CRL y registros de cambio, de modo que la modernización criptográfica pueda ser auditada y no dependa de afirmaciones generales de cumplimiento.

1.2.4. Soberanía digital y contexto latinoamericano

La dimensión de soberanía digital se aborda como criterio contextual y no como conclusión generalizable. Mantener control institucional sobre claves, políticas y decisiones de transición puede reducir dependencias tecnológicas y fortalecer capacidades locales; sin embargo, la evidencia empírica de esta investigación corresponde a una sola EC ecuatoriana. Por ello, cualquier aplicación regional requiere validaciones adicionales y adaptación a cada marco legal, arquitectura y nivel de madurez.

---

[13] TLS: Transport Layer Security - Seguridad de la capa de transporte
[14] ACME: Automated Certificate Management Environment - protocolo para automatizar las comunicaciones

Para la presente investigación, ello refuerza el vínculo entre PKI, soberanía digital y autonomía tecnológica (Zuboff, 2019).

1.3. Objetivo

1.3.1. Objetivo General

- Diseñar y validar, en una Entidad de Certificación específica del Ecuador y en entornos controlados o preproductivos, una estrategia progresiva de transición de RSA hacia ECC con preparación pos-cuántica, evaluando desempeño, interoperabilidad y conformidad normativa.

1.3.2. Objetivos Específicos.

- OE1[15]: Comparar RSA y ECC mediante latencia, tamaño de certificados y cadenas, throughput, uso de CPU/RAM y compatibilidad en el entorno evaluado.
- OE2: Identificar y priorizar factores técnicos, normativos y organizacionales de la transición mediante una matriz de riesgos y medidas de mitigación.
- OE3: Diseñar y validar un escenario por fases piloto, emisión dual y convergencia, con perfiles X.509 ECC, flujos OCSP/CRL, KPIs, checklists y mecanismos de reversión.
- OE4: Integrar una guía de preparación pos-cuántica con inventario, criterios de adopción híbrida, rotación de claves y algoritmos, pruebas controladas y planes de reversión.

1.4. Hipótesis o supuesto hipotético

La hipótesis general de esta investigación sostiene que una estrategia de transición progresiva de PKI desde RSA hacia ECC con preparación pos-cuántica, validada en una Entidad de Certificación específica del Ecuador y en entornos controlados o preproductivos, permite

[15] OE: Objetivo Especifico

evidenciar mejoras técnico-operativas frente a infraestructuras jerárquicas tradicionales, expresadas en una reducción de la latencia de validación de al menos el 20 %, una disminución del tamaño de certificados de al menos un 30 %, una compatibilidad efectiva superior al 95 % y niveles de conformidad normativa superiores al 90 %, sin afectación significativa de los indicadores operativos asociados al SLA.

A partir de esta hipótesis general se derivan las siguientes hipótesis específicas alineadas con los objetivos de investigación.

1.4.1. H1 – Comparativo técnico-operativo:

En una Entidad de Certificación específica del Ecuador y bajo pruebas en entornos controlados o preproductivos, ECC presenta mejoras operativas frente a RSA, para niveles equivalentes de seguridad efectiva, reflejadas en una reducción de la latencia de validación OCSP/TLS de al menos el 20 %, una disminución del tamaño de certificados y cadenas de al menos el 30 % y un throughput estable o superior.

Medición: Bancos de prueba reproducibles; scripts/bitácoras; panel de clientes representativos y comparaciones emparejadas RSA vs. ECC en perfiles X.509.

1.4.2. H2 – Factores condicionantes:

La identificación y evaluación de factores técnicos, normativos y organizacionales, así como la aplicación de medidas de mitigación en la Entidad de Certificación analizada, permiten alcanzar un nivel de conformidad normativa igual o superior al 90 % y reducir el nivel de riesgo residual de la transición a categorías aceptables para su validación en entornos controlados o preproductivos.

Medición: matrices de conformidad al NIST, ETSI RFC y normativa aplicable a la Entidad de Certificación, matriz de riesgos con probabilidad e impacto, y evidencias de capacitación de roles críticos.

1.4.3. H3 – Escenarios por fases:

La validación de un esquema progresivo de transición, estructurado en fases de piloto, emisión dual y convergencia, con criterios de paso y reversión definidos, permite mantener niveles de compatibilidad efectiva iguales o superiores al 95 % y niveles de conformidad normativa iguales o superiores al 90 %, con trazabilidad operativa y evidencia auditable en los entornos controlados o preproductivos evaluados.

Medición: KPIs por fase, auditorías internas, evidencia en OCSP/CRL y registro de control de cambios.

1.4.4 H4 – Preparación pos-cuántica:

La formulación e integración de una guía de preparación pos-cuántica para la Entidad de Certificación objeto de estudio, incrementa el grado de preparación pos-cuántica de la infraestructura, medido mediante la existencia de políticas, pruebas, planes de migración y criterios para la futura incorporación de esquemas híbridos ECC-PQC, rotación de claves y mecanismos de reversión.

Medición: Validación de prueba de concepto híbrida, plan PQC versionado, y evaluación comparativa del riesgo antes y después.

1.5. Variables o Categoría de análisis

La selección de variables e indicadores se sustenta en tres aspectos:

- Primero, la comparativa RSA-ECC justifica medir latencia, throughput, tamaño de objetos y consumo de recursos como manifestaciones observables del desempeño criptográfico (Certauri, 2023; Priya, 2024).

- Segundo, los lineamientos de transición y cripto-agilidad del NIST justifican incorporar fase de migración, riesgo residual, inventario y readiness como indicadores de capacidad de cambio (NIST, 2019; NIST, 2024c).

- Tercero, los marcos ETSI y los perfiles X.509 justifican medir compatibilidad y conformidad como condiciones de interoperabilidad. En consecuencia, los indicadores no se definieron únicamente por conveniencia instrumental, sino por su relación con desempeño, gobernanza y validez normativa.

En esta investigación, las variables permiten operacionalizar el problema de estudio y establecer una relación analítica entre la estrategia de transición criptográfica y sus efectos observables en la Entidad de Certificación analizada. Su uso hace posible medir, comparar e interpretar el comportamiento de la infraestructura frente al cambio de RSA hacia ECC con preparación pos-cuántica, proporcionando una base empírica para valorar la viabilidad técnico-operativa, la interoperabilidad y la conformidad normativa de la propuesta.

La Tabla 1 presenta las variables independientes, es decir, aquellos factores que definen las condiciones de análisis de la transición criptográfica, tales como el algoritmo utilizado, la fase de migración y el tipo de servicio PKI evaluado.

Tabla 1
Operacionalización de las Variables independientes

Variable	Tipo	Definición operacional	Indicador	Unidad de medida	Fuente de datos
Algoritmo criptográfico utilizado en la PKI	Cualitativa nominal	Algoritmo asimétrico configurado para emisión y validación de certificados en la Entidad de Certificación.	Algoritmo activo en CA: RSA, ECC, ECC+PQC (en laboratorio).	Categoría RSA/ECC/ECC+PQC)	Configuración de la CA, HSM, servidores; scripts de prueba
Fase de la estrategia de transición criptográfica	Cualitativa ordinal	Etapa del plan de transición RSA→ECC→PQC definida en la hoja de ruta de la EC.	Fase activa: 0 = solo RSA; 1 = piloto ECC; 2 = emisión dual; 3 = convergencia ECC (y pruebas PQC).	Niveles 0–3	Plan de migración, cronograma de proyecto, actas de cambio.
Tipo de servicio PKI evaluado	Cualitativa nominal	Servicio específico de la PKI evaluado en las pruebas.	Clasificación: emisión de certificados de firma, certificados de servidor TLS, validación OCSP/CRL	Categoría	Documentación de servicios, diagramas de arquitectura.

Nota. Elaboración propia.

La Tabla 2 reúne las variables dependientes, que corresponden a los efectos observables y medibles de la transición, expresados en indicadores de desempeño técnico-operativo, interoperabilidad, conformidad normativa, riesgo residual y preparación poscuántica.

Tabla 2
Operacionalización de las Variables dependientes

Variable	**Tipo**	**Definición operacional**	**Indicador**	**Unidad de medida**	**Fuente de datos**
Latencia de operación o transacción	Cuantitativa continua	Tiempo desde que se inicia una operación (OCSP, handshake TLS, descarga de CRL) hasta que se recibe una respuesta válida.	Tiempo promedio y máximo por tipo de operación y por algoritmo/fase.	Milisegundos (ms) / segundos	Herramientas de medición (scripts, logs de servidor, capturas de red).
Throughput de la Entidad de Certificación	Cuantitativa continua	Capacidad de la EC para procesar operaciones criptográficas bajo carga.	Número de certificados emitidos/segundo, respuestas OCSP/segundo o transacciones válidas por unidad de tiempo.	Operaciones por segundo / minuto	Benchmarks, generadores de carga, métricas de servidor.
Uso de recursos de infraestructura (CPU, RAM e IO)	Cuantitativa continua	Recursos de infraestructura consumidos por la EC durante la operación con distintos algoritmos y fases.	% de uso de CPU promedio y pico, memoria RAM utilizada, IOPS o uso de disco durante las pruebas.	%, MB, IOPS	Monitor de sistema, herramientas APM, logs de rendimiento.

Tamaño de certificados y cadenas de certificación	Cuantitativa continua	Tamaño en bytes de certificados X.509 y cadenas de certificación generadas en cada escenario.	Tamaño promedio de certificado y de cadena completa por algoritmo.	Bytes / KB	Exportación de certificados y cadenas, comandos de inspección.
Compatibilidad efectiva	Cuantitativa continua	Porcentaje de clientes/navegadores/dispositivos que validan correctamente certificados y cadenas emitidas bajo las nuevas configuraciones.	Número de plataformas que funcionan sin error / total de plataformas probadas × 100.	Porcentaje (%)	Matriz de pruebas de compatibilidad, reportes de testing funcional.
Nivel de conformidad normativa	Cuantitativa (índice)	Grado de cumplimiento de la EC con requisitos de NIST, ETSI, normativa local y otros relevantes para PKI y PQC.	% de requisitos cumplidos en checklists (ítems cumplidos / ítems totales × 100).	Porcentaje (%)	Checklists de cumplimiento, matrices de mapeo normativo, informes de auditoría.
Nivel de riesgo residual de la transición	Cuantitativa / ordinal	Riesgo que permanece después de aplicar controles y mitigaciones en la migración RSA→ECC→PQC.	Valor de riesgo resultante por matriz (probabilidad × impacto) y clasificación (bajo/medio/alto).	Índice / Bajo-Medio-Alto	Matriz de riesgos, talleres con expertos, actas de gestión de riesgos.
Grado de preparación pos-	Cuantitativa / ordinal	Preparación de la EC para adoptar algoritmos	Índice de preparación (0–100 %) o niveles	% o niveles	Guía PQC, planes de migración,

cuántica (PQC readiness)		poscuánticos y esquemas híbridos en su PKI.	(básico/intermedio/avanzado) según existencia de políticas, pruebas y planes PQC.		pruebas de laboratorio, entrevistas.

Nota. Elaboración propia.

La Tabla 3 muestra las variables de control, cuya función es mantener condiciones de prueba comparables en aspectos como hardware, red, software y carga de trabajo, con el fin de reducir sesgos y fortalecer la validez de los resultados obtenidos.

Tabla 3

Operacionalización de las Variables de control

Variable de control	**Tipo**	**Definición operacional**	**Forma de control**
Plataforma de hardware de servidores	Cualitativa nominal	Características de CPU, RAM y almacenamiento de los servidores usados en las pruebas.	Mantener la misma plataforma para pruebas con RSA y ECC/ECC+PQC; documentar especificaciones de hardware.
Condiciones de red en las pruebas	Cuantitativa continua	Latencia, ancho de banda y pérdida de paquetes durante las mediciones.	Usar el mismo escenario de red o una emulación controlada para todos los algoritmos; registrar parámetros de red.
Versión de software y sistema operativo	Cualitativa nominal	Versión de la CA, servicio OCSP, librerías criptográficas y sistema operativo.	Congelar versiones durante las comparaciones; documentar versiones exactas.

Carga de trabajo de prueba	Cuantitativa continua	Número de solicitudes concurrentes y volumen de transacciones generadas en los escenarios de benchmark.	Utilizar el mismo patrón de carga (scripts, número de usuarios virtuales, duración) para todos los algoritmos evaluados.

Nota. Elaboración propia.

En conjunto, estas variables permiten estructurar el análisis empírico de la transición de PKI desde RSA hacia ECC con preparación poscuántica, vinculando las condiciones del cambio criptográfico con sus efectos observables en términos de desempeño, interoperabilidad, conformidad normativa y preparación institucional.

Capítulo 2.

2.1. Estado del Arte

2.1.1. Antecedentes

2.1.1.1. Origen de la criptografía de clave pública y surgimiento de la PKI

La PKI tuvo su origen en el desarrollo de la criptografía de clave pública durante la década de 1970. La propuesta de Diffie y Hellman introdujo la posibilidad de establecer secretos compartidos sin intercambio previo de claves privadas, mientras que el algoritmo RSA consolidó el uso práctico de mecanismos asimétricos para cifrado y firma digital (Diffie & Hellman, 1976; Rivest, 1978).

Sobre esa base se desarrollaron los certificados digitales X.509 y las jerarquías de certificación que posteriormente estructuraron la PKI moderna. Con la expansión de Internet y la adopción de SSL/TLS, esta arquitectura pasó a convertirse en un mecanismo central de confianza para la Web y para múltiples servicios de gobierno electrónico (Sectigo, 2021).

En ese proceso, la evolución hacia los certificados X.509 versión 3 fue especialmente importante, porque permitió incorporar extensiones que vinculan identidad, uso de clave, políticas y restricciones de validación dentro del propio certificado. Para esta investigación, este punto es relevante porque muestra que la PKI no solo evolucionó mediante mejores algoritmos, sino también mediante estructuras de certificación más expresivas y aptas para sostener interoperabilidad y control (Curry, 1996).

Desde sus primeras implementaciones, la PKI no dependió únicamente de la solidez matemática de sus algoritmos. También quedó condicionada por políticas de certificación, resguardo de claves raíz, disciplina operativa y gobernanza institucional. Este aspecto es

importante para la presente investigación porque muestra, desde el origen mismo de la PKI, que la confianza digital siempre tuvo una dimensión técnica y otra organizacional.

2.1.1.2. Consolidación de la WebPKI y expansión a servicios críticos

Con la expansión masiva de la Web a partir de la década de 1990, la PKI se consolidó como base de la denominada WebPKI, es decir, del conjunto de autoridades raíz integradas en navegadores y sistemas operativos de las que dependieron millones de certificados TLS, de firma de código y de firma documental. En ese proceso, diversas autoridades comerciales ampliaron la emisión de certificados públicos, mientras los programas de raíz exigieron controles cada vez más estrictos en materia de auditoría y seguridad.

De manera paralela, varios países desarrollaron infraestructuras PKI propias para habilitar servicios de gobierno electrónico, identidad digital y firma electrónica con validez jurídica. En América Latina, uno de los casos más relevantes fue ICP-Brasil, que consolidó un ecosistema jerárquico de certificación con sustento legal e institucional específico (ICP, 2017).

Este antecedente resulta importante porque muestra que la expansión de la PKI no ocurrió únicamente en el ámbito comercial o técnico, sino también como parte de procesos estatales de institucionalización de la confianza digital.

En esa misma línea, la evolución de dicho modelo también se sostuvo en mecanismos formales de acreditación, fiscalización y auditoría de autoridades certificadoras y de registro, lo que fortaleció su papel como infraestructura de confianza con efectos jurídicos y administrativos concretos (ANCD, 2025).

Desde la perspectiva de esta investigación, ello confirma que una PKI madura no depende solo de la emisión de certificados, sino también de la existencia de estructuras de supervisión y control capaces de sostener la legitimidad del ecosistema.

La importancia de la PKI también apareció en estudios recientes sobre gobierno digital e infraestructura pública digital en América Latina y el Caribe. En estos trabajos, la identidad, la autenticación y la confianza digital se reconocieron como componentes básicos para avanzar hacia servicios públicos más resilientes e interoperables (OECD, 2024).

A partir de ello, puede sostenerse que la PKI ya no debe entenderse como una herramienta auxiliar, sino como una infraestructura habilitante para la transformación digital del Estado y para la provisión de servicios públicos con mayores niveles de integración.

Otros informes destacaron que la consolidación de infraestructura pública digital en la región requiere articular capacidades de identidad, autenticación y confianza como parte de una estrategia más amplia de modernización institucional (UNDP, 2025).

Dentro de la investigación es importante, porque permite ubicar a la PKI dentro de una agenda más amplia de fortalecimiento estatal, interoperabilidad y desarrollo tecnológico, y no solo dentro del campo restringido de la criptografía aplicada. Asimismo, se ha señalado que la infraestructura pública digital depende de componentes básicos que permitan sostener relaciones de confianza, intercambio seguro de datos y prestación continua de servicios, especialmente en entornos donde el Estado busca ampliar su capacidad digital (Appaya et al., 2024).

En conclusión, la consolidación de la WebPKI y de las infraestructuras nacionales de certificación muestra que las Entidades de Certificación pasaron de ser actores puramente técnicos para convertirse en componentes estratégicos de la confianza institucional y digital. Por ello,

cualquier transición criptográfica en este ámbito impacta no solo en el plano técnico, sino también en la continuidad de servicios públicos, financieros y jurídicos.

2.1.1.3. Incidentes históricos y limitaciones estructurales de la PKI

Aunque durante varios años la PKI fue presentada como una infraestructura relativamente consolidada, los estudios sobre incidentes mostraron un panorama más complejo. Un metaanálisis reciente documentó fallos recurrentes tanto en la WebPKI como en sistemas de identidad digital basados en certificados, identificando problemas persistentes de emisión, revocación, supervisión regulatoria, gobernanza y error humano (Dumitrescu & Pouwelse, 2024).

Este antecedente es relevante para la presente investigación porque desplaza la discusión desde la supuesta solidez de la infraestructura hacia sus debilidades operativas y organizacionales. En otras palabras, la PKI no aparece como un sistema plenamente resuelto, sino como un entorno donde la confianza puede verse comprometida por múltiples factores no estrictamente criptográficos.

Como complemento, otro estudio basado en entrevistas a expertos y en el análisis de alrededor de 1.800 incidentes documentados evidenció una brecha entre lo que los especialistas consideran como principales causas de fallo y lo que efectivamente se observa en los casos reales. Mientras la percepción experta suele enfatizar vulnerabilidades criptográficas, muchos incidentes se relacionan con errores de emisión, configuraciones deficientes, incumplimientos de políticas y problemas de gobernanza (Hadan et al., 2021). Desde la perspectiva de esta investigación, este hallazgo es relevante porque confirma que la discusión sobre modernización criptográfica no puede centrarse únicamente en la fortaleza del algoritmo. También debe considerar la forma en que la infraestructura es administrada, auditada y controlada en la práctica.

A partir de estos antecedentes, pueden identificarse varias limitaciones estructurales que siguen afectando a la PKI. Entre ellas destacan la fragilidad de la cadena de confianza, las debilidades en los mecanismos de revocación, la dependencia de procesos manuales y el desfase entre las exigencias normativas y la capacidad real de implementación institucional.

Estas limitaciones permiten comprender que una transición desde RSA hacia ECC, e incluso hacia esquemas poscuánticos, no resolverá por sí sola los problemas de fondo si no se acompañan de mejoras en procesos, gobernanza, monitoreo y trazabilidad. Por ello, la presente investigación asume que la evolución de la PKI debe abordarse como un proceso integral de transformación y no únicamente como una sustitución tecnológica.

2.1.1.4. PKI en identidad digital, gobierno electrónico y contexto latinoamericano/ecuatoriano

El avance de las identidades digitales soberanas, las credenciales verificables y las firmas electrónicas avanzadas volvió a situar a la PKI en el centro de la transformación digital del Estado. En distintos escenarios, estas infraestructuras pasaron a sustentar procesos de autenticación, validación jurídica y prestación de servicios digitales de creciente complejidad (Prego, 2020). Este antecedente es importante para la presente investigación porque muestra que la PKI ya no puede considerarse una herramienta técnica externa. Su función se vincula directamente con la capacidad del Estado y de las instituciones para sostener confianza digital, identidad y validez transaccional.

En América Latina, varios países adoptaron modelos basados en PKI para soportar firmas con validez jurídica, trámites electrónicos y sistemas tributarios digitales, lo que confirma su papel como infraestructura habilitante en procesos de modernización administrativa y documental

(CEPALSTAT, 2024). De la misma forma, se ha advertido que el despliegue de mecanismos de identidad y confianza debe acompañarse de transparencia, protección de datos y garantías de seguridad, especialmente cuando la PKI forma parte de sistemas de identificación y validación de derechos en entornos digitales (Alimonti, 2025).

En la región, las trayectorias de adopción de PKI fueron heterogéneas. Brasil consolidó una infraestructura jerárquica robusta bajo ICP-Brasil, con soporte legal e institucional para la fiscalización y auditoría de autoridades certificadoras y de registro (ICP, 2017).

La consolidación de ese ecosistema también se apoyó en estructuras formales de acreditación y control que fortalecieron su papel como infraestructura de confianza con efectos jurídicos y administrativos concretos (ANCD, 2025).

En el caso ecuatoriano, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, junto con su normativa complementaria, estableció el marco para la acreditación de Entidades de Certificación y la emisión de certificados con validez jurídica. Más recientemente, ARCOTEL actualizó los requisitos técnicos, de seguridad e interoperabilidad aplicables al sector (Arcotel, 2024).

Asimismo, el ecosistema ecuatoriano incluye entidades públicas y privadas acreditadas, sujetas a obligaciones regulatorias expresas, lo que evidencia la existencia de una estructura formal de certificación digital en funcionamiento (Arcotel, 2025).

No obstante, la mayor parte de estas implementaciones continúa apoyándose en RSA, mientras la adopción de ECC sigue siendo limitada y la incorporación de PQC prácticamente inexistente. Entre los principales obstáculos se encuentran la dependencia de HSM con soporte

restringido, la permanencia de sistemas legados, la ausencia de guías específicas de migración y la escasez de métricas sistemáticas sobre impacto operativo.

Por ello, el contexto latinoamericano y ecuatoriano no se incorpora en esta investigación como un marco meramente descriptivo, sino como el espacio donde se manifiesta de forma concreta la necesidad de una estrategia progresiva, validada y metodológicamente estructurada para la transición hacia ECC con preparación poscuántica.

2.1.1.5. Síntesis socio-técnica de los antecedentes

La revisión de antecedentes muestra que la PKI debe entenderse como un sistema socio-técnico, en el que la seguridad no depende exclusivamente de la robustez criptográfica, sino también de factores como la cultura organizacional, la gestión del riesgo, la calidad del talento humano y la existencia de procesos auditables (Dumitrescu & Pouwelse, 2024).

Este punto resulta central para la presente investigación porque desplaza el análisis desde la sola discusión algorítmica hacia una comprensión más amplia de la infraestructura de confianza. En consecuencia, la modernización de la PKI exige considerar simultáneamente componentes técnicos, organizacionales y regulatorios.

De igual manera, la evidencia revisada indica que muchos incidentes en PKI no se originan principalmente en la debilidad matemática de los algoritmos, sino en errores de emisión, revocación, control y cumplimiento. Por ello, la transición de algoritmos no puede asumirse como una actualización puramente técnica, sino como un proceso que debe planificarse y ejecutarse dentro de una estrategia de gestión del riesgo y del ciclo de vida criptográfico (NIST, 2024c).

Desde esta perspectiva, la adopción de ECC y la preparación para PQC requieren algo más que soporte tecnológico. También demandan criterios de trazabilidad, políticas actualizadas,

control del cambio y mecanismos formales de validación que permitan sostener la continuidad del servicio y la confianza institucional.

De esta manera, el enfoque de cripto-agilidad muestra que las Entidades de Certificación deben desarrollar capacidades para gestionar algoritmos y parámetros de manera controlada y repetible, lo que supone inventarios de activos, gestión formal del cambio, actualización de políticas y mecanismos de auditoría consistentes (NIST, 2024c). A partir de ello, esta investigación asume que una PKI de próxima generación no se define únicamente por los algoritmos que incorpora, sino por la forma en que una Entidad de Certificación planifica, gobierna, valida y audita su transición criptográfica. Bajo esta lógica, los antecedentes no solo describen una evolución histórica, sino que también justifican el enfoque metodológico adoptado en la investigación.

2.1.2. Fundamentos técnicos, estratégicos y normativos en la transición a PKI con ECC

2.1.2.1 Ventajas técnicas y operativas de ECC

La ECC se fundamenta en las propiedades algebraicas de las curvas elípticas sobre cuerpos finitos, su principal ventaja frente a RSA es la eficiencia criptográfica donde logra niveles de seguridad equivalentes con tamaños de clave significativamente menores. Por ejemplo, una clave ECC de 256 bits proporciona un nivel de seguridad comparable al de una clave RSA de 3072 bits (Koblitz & Menezes, 2000). Esto reduce drásticamente los requerimientos de cómputo, el uso de memoria y la latencia en operaciones criptográficas, haciéndola ideal para entornos de alta demanda y dispositivos con recursos limitados.

Desde una perspectiva operativa, ECC presenta ventajas para firmas digitales, establecimiento de claves y autenticación mutua, su menor tamaño de clave se traduce en certificados más pequeños y operaciones de verificación más rápidas, facilitando despliegues en entornos IoT, móviles y plataformas en la nube (Bos et al., 2014; Laassiri et al., 2022).

Además, ECC permite una mejor escalabilidad en sistemas donde se emiten miles o millones de certificados por día, lo cual es especialmente relevante para Entidades de Certificación nacionales, gubernamentales o de gran escala.

2.1.2.2. Estrategias de adopción tecnológica: modelos híbridos y progresivos

Estudios coinciden en que la transición hacia ECC no debe plantearse como un reemplazo abrupto de RSA, sino como un proceso gradual. En entornos donde coexisten infraestructuras críticas, aplicaciones heredadas y marcos regulatorios restrictivos, se han propuesto modelos híbridos que permiten la convivencia temporal entre ambos esquemas criptográficos mediante firma dual, certificados multiclave, túneles criptográficos o autoridades de certificación paralelas para pilotos controlados (Springer & Haindl, 2024).

Este enfoque resulta relevante para la presente investigación porque permite comprender que la transición criptográfica no depende únicamente de la superioridad técnica del nuevo algoritmo, sino de la capacidad institucional para introducirlo sin comprometer la continuidad del servicio. En ese sentido, la adopción progresiva aparece como una condición de viabilidad y no solo como una opción metodológica.

En términos operativos, los modelos híbridos permiten mitigar riesgos durante la migración, preservar compatibilidad con sistemas externos que aún utilizan RSA y validar el

comportamiento de ECC en condiciones reales antes de una adopción más amplia (Springer & Haindl, 2024).

Desde esta perspectiva, la estrategia gradual adquiere valor porque transforma la transición en un proceso verificable y gobernable. Para esta investigación, ello justifica la necesidad de fases, criterios de paso, pilotos controlados y mecanismos de reversión, en lugar de una sustitución total e inmediata del algoritmo base.

2.1.2.3. Condicionamientos normativos y gobernanza técnica de la PKI

La adopción de ECC también está condicionada por el marco normativo y por la estructura de gobernanza técnica de la PKI. En muchos contextos regulatorios, los perfiles, certificaciones de software y prácticas operativas siguen fuertemente asociados a RSA, lo que dificulta la actualización de algoritmos y genera riesgos de dependencia tecnológica y obsolescencia.

Diversos organismos impulsaron la estandarización de ECC mediante curvas y perfiles interoperables. Entre ellos, NIST, SECG[16] y ETSI promovieron lineamientos que facilitaron su incorporación en entornos regulados y comerciales. De forma complementaria, el IETF formalizó el uso de ECC en certificados X.509 a través del RFC 5480, habilitando su integración en TLS y en infraestructuras PKIX[17].

La complejidad histórica de X.509 también muestra que la interoperabilidad de una PKI no depende solo de adherirse formalmente a un estándar, sino de definir perfiles consistentes, extensiones comprensibles y prácticas de implementación suficientemente disciplinadas. Esta observación resulta útil para la investigación porque refuerza la idea de que la transición hacia

[16] SECG: Standards for Efficient Cryptography Group - Grupo de estándares para eficiencia Criptográfica
[17] PKIX: Public Key Infrastructure x509 - infraestructura de clave pública para el estándar X.509

ECC exige gobernanza técnica sobre perfiles, políticas y validaciones, y no únicamente soporte algorítmico (Gutmann, 2000).

De forma complementaria, el RFC 5280 establece el perfil operativo más ampliamente aceptado para certificados X.509 y listas de revocación, definiendo campos, extensiones y criterios de validación que resultan esenciales para la interoperabilidad entre autoridades certificadoras, clientes y servicios de confianza. Para esta investigación, este referente es importante porque permite entender que la transición hacia ECC no depende únicamente del soporte del algoritmo, sino también de la preservación de perfiles compatibles y de reglas de validación consistentes dentro del ecosistema PKI (Cooper et al., 2008).

Este antecedente es importante porque muestra que la transición no puede evaluarse únicamente en términos de rendimiento. También debe examinarse desde su compatibilidad con estándares, perfiles de certificado y exigencias de validación que hacen posible el reconocimiento de confianza en ecosistemas más amplios.

En términos de gobernanza técnica, la migración hacia ECC ha sugerido considerar modelos complementarios apoyados en blockchain[18], DLT[19] como referentes para discutir nuevas formas de estructuración de la confianza, aunque no necesariamente como sustitutos directos del modelo jerárquico tradicional.

Desde este marco, la presente investigación asume que la gobernanza de la transición es tan importante como el algoritmo que se adopta. Por ello, el análisis no se limita a la comparación

[18] Blockchain: Es una Bases de datos descentralizada y compartida
[19] DLT: Distributed Ledger Technology - Tecnología de Contabilidad Distribuida

técnica RSA-ECC, sino que incorpora también la relación entre estandarización, jerarquía de confianza, control institucional e interoperabilidad.

2.1.2.4. Consideraciones para entornos soberanos y latinoamericanos

El uso de ECC también ha sido defendido desde una perspectiva de soberanía tecnológica. En distintos contextos, su adopción se ha vinculado con la reducción de dependencia respecto de proveedores externos, el fortalecimiento de infraestructura criptográfica propia y la mejora de la resiliencia cibernética nacional. Sin embargo, en América Latina se muestra una adopción todavía limitada y una institucionalización incompleta de este cambio, asociadas a la falta de políticas públicas claras y a capacidades técnicas restringidas (Quiroz et al., 2020).

Es importante para la presente investigación porque permite situar la transición criptográfica en un plano más amplio que el puramente técnico. En contextos latinoamericanos, migrar hacia ECC también implica fortalecer autonomía tecnológica, capacidad regulatoria y madurez institucional.

Desde esta perspectiva, el caso ecuatoriano puede leerse como una oportunidad de innovación regional, siempre que la transición se articule mediante una estrategia integral que combine aspectos técnicos, organizacionales y normativos.

2.1.2.5. Comparativa: RSA vs. ECC

La comparación entre RSA y ECC permite observar con mayor claridad la conveniencia de una transición progresiva en infraestructuras de clave pública. Mientras RSA mantiene ventajas ligadas a su amplia estandarización e integración histórica en sistemas legados, ECC alcanza niveles equivalentes de seguridad con tamaños de clave considerablemente menores y con menores requerimientos de procesamiento.

En términos operativos, esta diferencia tiene efectos directos sobre el tamaño de certificados y cadenas, la latencia de validación, el consumo de memoria, el tráfico de red y la viabilidad de despliegue en dispositivos de borde e IoT. Por ello, la comparación entre ambos algoritmos no solo tiene valor teórico, sino también relevancia práctica para el análisis de desempeño de una Entidad de Certificación.

La comparación RSA con ECC no se utiliza para justificar una sustitución inmediata y total, sino para fundamentar una transición ordenada basada en eficiencia, compatibilidad y preparación para escenarios criptográficos más exigentes. En este sentido, la Tabla 4 sintetiza las diferencias técnicas y operativas entre ambos algoritmos.

Tabla 4
Comparación técnica y operativa entre RSA y ECC en el contexto de Infraestructuras de Clave Pública

Criterio	**RSA**	**ECC (Criptografía de Curva Elíptica)**
Nivel de seguridad	Requiere claves largas para alta seguridad.	Logra igual o mayor seguridad con claves más cortas.
Tamaño de clave (seguridad ~112 bits)	2048 bits	224 bits
Tamaño de clave (seguridad ~256 bits)	15360 bits	512 bits
Eficiencia en procesamiento	Alto consumo computacional.	Requiere menos potencia de cálculo.
Velocidad de generación de claves	Más lenta	Más rápida
Velocidad de firma digital	Moderada	Rápida
Velocidad de verificación de firma	Alta	Moderada
Uso de memoria y ancho de banda	Elevado	Bajo
Adecuado para dispositivos IoT	Poco recomendable	Ideal por su bajo consumo
Estado de estandarización	Altamente estandarizado (PKCS, X.509, TLS)	Estándares bien definidos (SECG, RFC 5480, NIST)

Vulnerabilidad frente a computación cuántica	Quebrantable mediante algoritmo de Shor	Igualmente, vulnerable, aunque más resistente en el corto plazo
Aplicación práctica actual	Uso extendido en CA tradicionales y sistemas legacy	En aumento, especialmente en sistemas móviles y blockchain

Nota. Elaboración propia con base en (Koblitz & Menezes, 2000; Bos et al., 2014; Gutmann, 2000; Shor, 1997).

2.1.3. Estudios de caso y experiencias internacionales en la adopción de ECC

La adopción de ECC en infraestructuras de clave pública avanzó de forma desigual en distintas regiones, dependiendo de factores normativos, capacidades técnicas y prioridades de política digital. El análisis comparado de experiencias internacionales permite identificar patrones de implementación, condiciones de éxito y desafíos que resultan útiles para interpretar el caso ecuatoriano.

2.1.3.1. Estonia, Corea del Sur y Emiratos Árabes Unidos como referencias de adopción

Estonia es uno de los casos de adopción temprana de ECC en servicios públicos digitales. Desde 2014 integró algoritmos como Curve25519 y EdDSA[20] en parte de su infraestructura nacional de firma digital, incluyendo identidad electrónica, servicios móviles y trámites con efectos jurídicos, dentro de una estrategia más amplia de gobierno digital (Kattel, 2025).

El éxito estonio se asoció con una combinación de legislación habilitante, arquitectura modular e interoperable y una cultura institucional favorable a la innovación. Además, la apertura a validación pública y auditoría externa reforzó la confianza en la actualización de sus mecanismos criptográficos (Vassil, 2016).

[20] EdDSA: Edwards-curve Digital Signature Algorithm – Algoritmo de Firma Digital con curvas elípticas de Edwards

Desde la perspectiva de esta investigación, el caso estonio muestra que la adopción de ECC no depende únicamente de la disponibilidad del algoritmo, sino de una capacidad estatal para integrarlo dentro de un ecosistema coherente de identidad, regulación e interoperabilidad.

Corea del Sur siguió una trayectoria distinta, más vinculada al sector financiero y a la modernización de servicios móviles. Desde 2017 varios bancos incorporaron ECC en esquemas de autenticación digital y aplicaciones fintech, apoyados por pilotos controlados, certificación de software local y ajustes regulatorios progresivos (Kim & Lee, 2019).

A diferencia de Estonia, Corea del Sur enfrentó mayores restricciones derivadas de sistemas heredados y tecnologías propietarias, lo que obligó a rediseñar componentes completos para sostener compatibilidad. Sin embargo, la presión competitiva y la necesidad de eficiencia aceleraron la transición.

En esta investigación es útil porque evidencia que la migración hacia ECC puede surgir no solo desde agendas estatales, sino también desde demandas sectoriales concretas, siempre que exista capacidad para gestionar la compatibilidad con infraestructura heredada.

En Emiratos Árabes Unidos, ECC fue integrada de manera ambiciosa en programas nacionales de identidad digital. En UAE Pass se utilizó tanto para firmas digitales como para autenticación multifactor en entornos gubernamentales y empresariales, con énfasis en mejorar tiempos de validación y eficiencia operativa en redes distribuidas (Dumitrescu & Pouwelse, 2024).

Lo distintivo del caso emiratí fue que la adopción de ECC se conformó con objetivos de sostenibilidad, soberanía tecnológica y transformación digital. Además, se promovió el uso complementario de blockchain, configurando un ecosistema híbrido de seguridad y confianza.

Para la presente investigación, este caso demuestra que ECC puede integrarse como parte de una estrategia nacional más amplia, en la que eficiencia criptográfica, innovación institucional y soberanía digital se refuerzan mutuamente.

2.1.3.2. Lecciones para América Latina y el caso ecuatoriano

Aunque cada experiencia estuvo condicionada por su propio contexto geopolítico, tecnológico y normativo, de estos casos se desprenden varios patrones comunes: la transición hacia ECC requiere liderazgo institucional, actualización regulatoria, pilotos controlados, garantía de interoperabilidad y formación especializada de talento técnico.

Sin embargo, en América Latina la evidencia revisada muestra un escenario todavía dividido. Existen iniciativas parciales y discusiones sobre modernización, pero no una estrategia regional consolidada de adopción de ECC en infraestructuras PKI con alcance amplio (Quiroz et al., 2020).

Este vacío regional no debe leerse solo como demora, sino también como una oportunidad. En el caso ecuatoriano, la ausencia de una estrategia consolidada abre espacio para proponer una ruta metodológicamente estructurada, compatible con el marco regulatorio nacional y orientada a construir capacidad local de transición criptográfica.

2.1.3.3. Síntesis comparativa

La comparación entre Estonia, Corea del Sur y Emiratos Árabes Unidos muestra que la adopción de ECC no responde a una única lógica de implementación. En algunos casos predominó el liderazgo estatal, en otros, la presión del sector financiero o la articulación con programas de identidad nacional. No obstante, en todos ellos la transición se sostuvo sobre una combinación de visión estratégica, adecuación normativa, pruebas progresivas e interoperabilidad.

La Tabla 5 detalla de manera resumida la comparación de estrategias respecto a la adopción de una PKI con RSA a ECC.

Tabla 5
Comparación de estrategias internacionales de adopción de criptografía de curva elíptica (ECC) en Infraestructuras de Clave Pública

País / Región	Estrategia de Adopción	Factores Facilitadores	Principales Desafíos	Aplicabilidad en Ecuador
Estonia	Migración temprana y progresiva a ECC en e-ID y servicios digitales (X-Road)	Legislación avanzada, interoperabilidad, cultura digital, auditoría abierta	Actualizar algoritmos certificados y mantener compatibilidad	Modelo de referencia por modularidad y soberanía tecnológica
Corea del Sur	Pilotos en sector bancario, con adaptación a servicios móviles y fintech	Presión del sector privado, modernización regulatoria	Superar sistemas heredados como ActiveX	Viable para sector bancario y móvil si se modernizan plataformas
Emiratos Árabes Unidos	Integración total de ECC en sistema de identidad nacional UAE Pass	Enfoque gubernamental integral, eficiencia energética, soberanía digital	Escalar tecnologías complementarias (blockchain, biometría)	Ejemplo de integración institucional a gran escala
Latinoamérica (general)	Iniciativas dispersas; aún sin política pública regional consolidada	Conciencia académica emergente; interés institucional inicial en algunos países	Falta de marcos normativos, capacidades técnicas y planificación estratégica	Oportunidad de liderazgo regional mediante adopción estratégica

Nota. Elaboración propia con base en (Kattel, 2025; Vassil, 2016; Kim & Lee, 2019; Dumitrescu & Pouwelse, 2024; Quiroz et al., 2020).

En consecuencia, la principal lección para el Ecuador no es replicar mecánicamente un modelo extranjero, sino reconocer que la adopción de ECC debe plantearse como parte de una

estrategia nacional de modernización criptográfica, con fases, validación controlada y alineación entre capacidad técnica, regulación e interoperabilidad.

2.1.4. Descentralización de la confianza, identidad digital y tecnologías emergentes

La evolución de la PKI también se ha vinculado con tecnologías orientadas a descentralizar la confianza. Los estudios han señalado que el modelo jerárquico tradicional, basado en una autoridad de certificación central que emite, valida y revoca certificados, presenta vulnerabilidades estructurales como puntos únicos de fallo, dependencia institucional y limitaciones de auditoría pública (Dumitrescu & Pouwelse, 2024).

En respuesta a esas limitaciones, blockchain y otros modelos de gobernanza distribuida han sido propuestos como mecanismos complementarios para registrar certificados, revocaciones y eventos de confianza en redes abiertas y verificables. En este contexto, ECC se integra de forma natural porque múltiples plataformas distribuidas utilizan firmas basadas en curvas elípticas para sostener autenticación, integridad y eficiencia operativa (Springer & Haindl, 2024).

De forma más específica, propuestas como CertLedger y OpenPKI plantean almacenar certificados X.509 y sus estados de revocación directamente en blockchain, reduciendo dependencia de una autoridad única y favoreciendo auditoría pública en tiempo real (Kubilay et al., 2018). Estas alternativas buscan aumentar transparencia y trazabilidad, aunque también exigen nuevos criterios de interoperabilidad, regulación y auditoría.

Desde la perspectiva de esta investigación, estos desarrollos no sustituyen el objeto central de estudio, que sigue siendo una Entidad de Certificación regulada, pero sí amplían el horizonte conceptual de la transición criptográfica. En otras palabras, muestran que la evolución de la PKI

no solo implica cambiar algoritmos, sino también revisar cómo se organiza la confianza y cómo se verifican sus evidencias.

La misma tendencia aparece en los modelos de Identidad Descentralizada - DID, que permiten a los usuarios generar y controlar sus propios identificadores criptográficos sin depender por completo de una autoridad central. Estos sistemas se apoyan en claves ECC y han sido desarrollados en proyectos como Sovrin, uPort y Veres One, además de contar con respaldo de estandarización desde el W3C (Reijers et al., 2021; W3C, 2022).

Las pruebas de conocimiento cero - ZKP[21] se han incorporado como un componente relevante en escenarios de autenticación avanzada, ya que permiten demostrar información sin revelar su contenido. Muchas de sus implementaciones utilizan ECC por su compatibilidad con funciones de compromiso y estructuras criptográficas eficientes (Aranha et al., 2023).

La automatización mediante contratos inteligentes ha sido considerada una vía para ejecutar lógicas de emisión, renovación y revocación de certificados de forma más transparente y escalable en redes distribuidas (Ali et al., 2016).

En conjunto, estas tecnologías muestran que la PKI está dejando de entenderse únicamente como una jerarquía cerrada de certificación para convertirse en un campo de experimentación sobre nuevas formas de confianza, identidad y control criptográfico. Para esta investigación, su relevancia radicó en que permiten contextualizar la transición hacia ECC dentro de una transformación más amplia del ecosistema de confianza digital.

[21] ZKP: Zero Knowledge Proofs - Prueba de conocimiento cero

2.1.5. Criptografía poscuántica, transición híbrida y preparación de la PKI

Tanto RSA como ECC se basan en problemas matemáticos que podrían resolverse eficientemente mediante computación cuántica a gran escala. En particular, el algoritmo de Shor mostró que tanto la factorización como el logaritmo discreto podrían verse comprometidos en un escenario cuántico suficientemente avanzado (Shor, 1997).

Este riesgo no se limita a un escenario futuro abstracto. Se señala que un adversario puede capturar hoy tráfico cifrado y almacenarlo para descifrarlo más adelante, lo que vuelve necesaria una planificación anticipada de la transición criptográfica (NIST, 2024a; NIST, 2024b).

La teoría inicial sobre criptografía poscuántica ya había planteado que la transición hacia nuevos esquemas no debía entenderse únicamente como un cambio de algoritmo, sino como una transformación más amplia de supuestos de seguridad, formatos, interoperabilidad y ciclo de vida criptográfico. Esta observación permite ubicar la preparación PQC dentro de una lógica de anticipación estratégica y no solo como una reacción posterior a la estandarización formal (Bernstein et al., 2009).

En respuesta a este desafío, el NIST lideró un proceso de estandarización de algoritmos resistentes a la computación cuántica, del cual surgieron estándares como FIPS 203, FIPS 204 y FIPS 205, orientados a encapsulación de claves y firmas digitales poscuánticas (NIST, 2024b).

No obstante, la incorporación de PQC trae consigo costos operativos relevantes. Se muestra que muchos algoritmos poscuánticos incrementan el tamaño de claves, certificados y mensajes, así como la latencia y el consumo de recursos, lo que plantea desafíos de implementación e interoperabilidad en infraestructuras reales. Por ello, diversos autores recomiendan ECC como una solución de transición estratégica. Aunque ECC también es

vulnerable frente a la computación cuántica, mantiene ventajas claras sobre RSA en eficiencia computacional, tamaño de clave y consumo energético, especialmente en dispositivos con recursos limitados (Bos et al., 2014).

Otros trabajos destacaron que ECC es particularmente viable en entornos IoT, móviles y sistemas embebidos, donde las restricciones de energía, memoria y procesamiento vuelven poco eficientes el uso de RSA con claves largas (Kumar & Matho, 2017; Priya, 2024; Vahdati et al., 2019). Además, mediciones recientes reforzaron esta ventaja práctica al mostrar reducciones relevantes en tamaño de certificados y carga operativa (SoftwareCosmos, 2025; Maletsky, 2020).

Desde la perspectiva de esta investigación, este punto es central: ECC no se plantea como destino final, sino como una fase intermedia que permite optimizar la PKI actual y generar margen para una futura incorporación de mecanismos poscuánticos más costosos.

Una de las respuestas más sólidas frente a esta transición es el uso de esquemas híbridos, que combinan algoritmos clásicos como ECC con algoritmos PQC en certificados o protocolos. Esta aproximación busca mantener compatibilidad con el ecosistema actual y, al mismo tiempo, añadir una capa de preparación frente al riesgo cuántico (Bindel et al., 2019).

Desde el punto de vista terminológico, la coexistencia de mecanismos criptográficos tradicionales y poscuánticos requiere distinguir con precisión los esquemas híbridos utilizados durante la transición. La terminología propuesta en el ámbito de IETF permite describir estas combinaciones como esquemas en los que mecanismos tradicionales y poscuánticos se emplean conjuntamente para preservar propiedades de seguridad y facilitar una transición progresiva entre ambos paradigmas (Driscoll, 2024). En esta investigación, dicha terminología resulta útil para

delimitar los escenarios híbridos ECC-PQC considerados dentro de la estrategia de preparación pos-cuántica.

Se observa implementaciones de certificados X.509 híbridos y propuestas de transición incremental en protocolos como TLS, SSH y VPN, mostrando que la convivencia temporal entre esquemas clásicos y poscuánticos puede ser una vía viable para reducir riesgos de ruptura tecnológica (Bindel et al., 2019; Astrizi & Custódio, 2024). Estudios más aplicados añadieron que estos certificados pueden servir como instrumento de prueba, gestión del cambio y comunicación con usuarios y reguladores durante la transición (Pravin, 2025).

En esa misma línea, los estudios sobre desempeño de TLS 1.3 con algoritmos PQC mostraron incrementos significativos en latencia, tamaño de mensajes y consumo de recursos, especialmente bajo condiciones de red desfavorables o en dispositivos con restricciones de capacidad (Sosnowski et al., 2023).

Otro aspecto relevante de esta evolución es la automatización. Trabajos recientes sobre emisión de certificados poscuánticos mediante ACME demostraron que el rediseño de los flujos de emisión puede compensar parte del sobrecoste introducido por PQC, lo que confirma que la transición no depende solo del algoritmo, sino también de la arquitectura de automatización y orquestación (Giron et al., 2024).

La investigación no se basa en la PKI de próxima generación como una mera actualización técnica. La concibe como una evolución estratégica que integra transición gradual de RSA a ECC, preparación poscuántica basada en esquemas híbridos, automatización de procesos, métricas de desempeño y gobernanza del cambio. Esta lógica se organiza con los lineamientos de transición

del NIST y con la necesidad de inventarios, coexistencia temporal de algoritmos, políticas actualizadas y mecanismos de madurez organizacional (NIST, 2019; NIST, 2024c).

2.1.6. Interoperabilidad, sistemas legados y gestión del cambio

Uno de los principales desafíos de la transición criptográfica es la interoperabilidad con sistemas legados. En muchas instituciones, la infraestructura sigue basada en RSA y depende de HSM, lectores biométricos, navegadores, plataformas de firma y software heredado que no siempre soportan curvas modernas ni perfiles criptográficos recientes. A ello se suman los desafíos regulatorios. En varios países latinoamericanos, las normas sobre firma digital aún formulan referencias generales a algoritmos “seguros”, sin especificar con claridad curvas aceptadas o condiciones de validez para nuevos esquemas, lo que genera incertidumbre jurídica en la adopción de ECC y PQC (Quiroz et al., 2020).

Desde una perspectiva organizativa, cualquier transición PKI exige además coordinación interinstitucional, capacitación de personal, redefinición de procedimientos operativos y establecimiento de ambientes de prueba. Se visualizó que el liderazgo institucional y la colaboración entre Estado, academia y sector privado son factores decisivos para una migración exitosa (Karippacheril et al., 2016; Tammpuu & Masso, 2019).

Por otra parte, una PKI moderna debe sostener interoperabilidad internacional. Ello implica cumplir con estándares como RFC 5480, ETSI EN 319 y marcos asociados a WebPKI, así como mantener vigilancia técnica permanente y actualización continua de políticas de certificación. Esto justifica que la metodología no se limite a medir desempeño, sino que también incorpore conformidad normativa, compatibilidad y trazabilidad como dimensiones de validación.

2.1.7. Síntesis: hacia una PKI de próxima generación

La revisión del estado del arte muestra que la PKI de próxima generación no puede definirse por un único elemento aislado. No depende solo de adoptar ECC, ni solo de prepararse para PQC, ni solo de incorporar automatización o descentralización. Se configura más bien como la convergencia de varios componentes: eficiencia operativa, transición gradual, interoperabilidad normativa, esquemas híbridos, automatización de emisión y revocación, y gobernanza del cambio.

En este marco, RSA aparece como un esquema que todavía mantiene presencia por razones de compatibilidad e inercia del ecosistema, pero con limitaciones crecientes en costo operativo y escalabilidad. ECC se presenta como una alternativa más eficiente y viable en el corto y mediano plazo, mientras PQC introduce una exigencia estratégica de preparación a largo plazo.

Por ello, la investigación asume que la evolución hacia una PKI de próxima generación debe concebirse como un proceso estratégico, no como una simple sustitución algorítmica. Esa es precisamente la lógica que sustenta la propuesta de una transición progresiva, medible y validable en una Entidad de Certificación real del Ecuador.

2.2. Trabajos relacionados

En esta sección se revisan trabajos directamente relacionados con el problema de investigación, con el fin de identificar sus aportes, limitaciones y su pertinencia para la construcción de la propuesta planteada en el presente proyecto.

2.2.1. Hadan, Serrano & Camp (2021): Fallos reales vs. percepciones en la WebPKI

Hadan, Serrano y Camp desarrollaron un estudio mixto sobre la WebPKI en el que combinaron entrevistas semiestructuradas a expertos en seguridad y políticas públicas con un análisis cuantitativo de aproximadamente 1.800 incidentes reportados desde 2001 en programas

de raíz de navegadores, foros técnicos, blogs especializados y documentación de autoridades certificadoras. Su propósito fue contrastar lo que los especialistas consideraban como principales causas de fallo en la PKI con los incidentes que efectivamente aparecían documentados en la práctica (Hadan et al., 2021).

Los resultados mostraron una brecha significativa entre percepción y realidad. Mientras buena parte del discurso experto se concentró en vulnerabilidades criptográficas y debilidades de protocolo, los incidentes analizados se asociaron con mayor frecuencia a errores operativos de emisión, fallas en revocación, configuraciones incorrectas y problemas de gobernanza y cumplimiento de políticas. A partir de ello, los autores propusieron una taxonomía de causas de fallo organizada por tipo, origen y contexto, lo que permitió mostrar que las debilidades más frecuentes de la PKI no se ubicaban en ataques criptográficos sofisticados, sino en procesos cotidianos de gestión y control (Hadan et al., 2021).

Este trabajo resulta relevante para la presente investigación porque confirma que la transición criptográfica no puede diseñarse únicamente desde la comparación entre algoritmos. También debe considerar procedimientos de emisión, trazabilidad operativa, controles de auditoría y mecanismos de reversión. Desde esta perspectiva, el valor del artículo no radica solo en su diagnóstico de fallos, sino en que desplaza el análisis desde la criptografía aislada hacia la gobernanza efectiva de la infraestructura de confianza.

Uno de los principales aportes metodológicos del estudio fue precisamente su enfoque mixto, ya que permitió articular percepción experta y evidencia efectiva en una sola lectura analítica. Esto le dio mayor solidez a la conclusión de que la PKI falla con más frecuencia por debilidades de proceso que por quiebres matemáticos del algoritmo. Para esta investigación, ese

hallazgo es importante porque refuerza la necesidad de evaluar la migración RSA-ECC-PQC como un proceso socio-técnico, en el que el desempeño criptográfico debe ir acompañado de criterios de control, monitoreo y documentación verificable.

No obstante, el estudio también presenta limitaciones. Su foco principal está en la WebPKI y en programas de raíz de navegadores, por lo que no examina con igual profundidad PKI nacionales reguladas ni infraestructuras de certificación asociadas a firma electrónica con validez jurídica. Además, la base de incidentes depende de fuentes públicas y reportes voluntarios, lo que puede introducir sesgos de visibilidad o subregistro. Finalmente, aunque el artículo ofrece una lectura sólida sobre fallos reales, no desarrolla en detalle estrategias de migración algorítmica ni modelos de cripto-agilidad aplicados a una Entidad de Certificación concreta (Hadan et al., 2021).

En consecuencia, este trabajo aporta una base importante para la investigación, pero no resuelve directamente el problema que aquí se aborda. Su utilidad radica en que justifica la inclusión de fases de transición, bitácoras de cambio, pruebas de regresión, criterios de paso y mecanismos de reversión dentro de la estrategia propuesta. Es decir, aporta una comprensión rigurosa de por qué una PKI de próxima generación no puede construirse solo sobre mejores algoritmos, sino sobre mejores procesos de gestión del cambio.

2.2.2. Girón et al. (2024): Emisión automatizada de certificados PQC

Girón et al. analizaron la emisión automatizada de certificados poscuánticos en el contexto del protocolo ACME, partiendo del hecho de que en la WebPKI actual la emisión y renovación de certificados depende en gran medida de flujos automatizados. Su estudio se centró en evaluar qué ocurre cuando los algoritmos clásicos son reemplazados por alternativas poscuánticas o híbridas dentro de ese proceso (Giron et al., 2024).

Para ello, los autores diseñaron un entorno de simulación en el que compararon distintos tipos de desafío ACME, incluyendo el esquema tradicional y una variante adaptada a PQC. Las métricas principales fueron el tiempo de emisión, la cantidad de datos intercambiados y el impacto en la carga de los servidores. Sus resultados mostraron que el nuevo desafío propuesto podía reducir de forma significativa tanto el tiempo promedio de emisión como el tamaño de la comunicación, incluso en escenarios donde los algoritmos poscuánticos incrementaban el costo criptográfico (Giron et al., 2024).

El aporte central del trabajo consiste en demostrar que, en un escenario poscuántico, el principal cuello de botella no se ubica únicamente en el algoritmo, sino también en la automatización y en la orquestación del ciclo de emisión de certificados. Desde esta perspectiva, el artículo amplía la discusión habitual sobre PQC, porque desplaza parte del problema desde la criptografía pura hacia la arquitectura operativa que sostiene la emisión masiva.

Para la presente investigación, este hallazgo resulta útil porque refuerza la necesidad de no limitar la transición RSA-ECC-PQC a una comparación entre algoritmos. También obliga a revisar procesos de emisión, renovación y revocación, así como a definir indicadores de desempeño vinculados con tiempo de emisión, tamaño de mensajes y capacidad de escalamiento. En otras palabras, el estudio aporta un antecedente claro para justificar que una hoja de ruta poscuántica debe ir acompañada de cambios en automatización y no solo en perfiles criptográficos.

No obstante, el artículo también presenta límites importantes. Su análisis se sitúa en el ámbito de la WebPKI y de entornos cercanos a ACME, por lo que no aborda directamente las particularidades de una Entidad de Certificación regulada que emite certificados con validez

jurídica. Además, el estudio se desarrolla en condiciones controladas de simulación y no profundiza en restricciones normativas, gobernanza institucional o exigencias de auditoría propias de contextos regulatorios más estrictos (Giron et al., 2024).

En consecuencia, este trabajo no resuelve por sí solo el problema de transición que aborda la investigación, pero sí aporta un insumo metodológico relevante. Su principal valor radica en mostrar que la preparación poscuántica exige pensar la PKI también desde la eficiencia de sus flujos operativos. Por ello, su incorporación en este capítulo no se justifica por afinidad temática general, sino porque ayuda a sustentar la inclusión de KPIs operativos y de criterios de escalabilidad dentro de la estrategia propuesta.

2.2.3. Sosnowski et al. (2023): desempeño de TLS 1.3 con algoritmos PQC

Sosnowski et al. realizaron un estudio experimental sobre el desempeño de TLS 1.3 cuando se integran algoritmos poscuánticos y configuraciones híbridas, utilizando herramientas del proyecto Open Quantum Safe. El experimento evaluó distintos escenarios de red con variaciones en latencia y pérdida de paquetes, y comparó algoritmos clásicos, poscuánticos e híbridos en términos de comportamiento operativo (Sosnowski et al., 2023).

El trabajo midió de manera sistemática la latencia del handshake, incluyendo percentiles p95 y p99, el tamaño de los mensajes intercambiados, el uso de CPU y memoria, así como el efecto de distintos algoritmos y parámetros sobre la experiencia de conexión. Sus resultados mostraron que muchos algoritmos PQC generaron handshakes más pesados y lentos, y que ese impacto se intensificó en redes con mayor latencia o en condiciones operativas adversas (Sosnowski et al., 2023).

El principal aporte del estudio radica en la solidez de su metodología de medición. Más allá de los resultados puntuales para cada algoritmo, el artículo ofrece un marco reproducible para comparar esquemas clásicos, poscuánticos e híbridos bajo diferentes perfiles de red, lo que lo convierte en una referencia útil para evaluar el costo operativo real de una transición criptográfica (Sosnowski et al., 2023).

Para la presente investigación, este trabajo refuerza la necesidad de evaluar la migración no solo desde la seguridad teórica, sino también desde métricas observables de desempeño. Aporta criterios útiles para justificar el uso de latencia, tamaño de certificados y cadenas, y comportamiento bajo distintos escenarios de red como indicadores relevantes dentro del banco de pruebas de la investigación.

El estudio también presenta límites claros para el problema específico que aquí se aborda. Su enfoque principal está en TLS como protocolo y no en la gestión integral de certificados X.509 dentro de una Entidad de Certificación. Además, se desarrolla en entornos experimentales y no profundiza en aspectos normativos, de gobernanza ni de cumplimiento, que resultan decisivos en una infraestructura PKI regulada (Sosnowski et al., 2023).

En consecuencia, el valor de este artículo para la investigación no consiste en ofrecer una estrategia completa de transición, sino en proporcionar una base metodológica rigurosa para medir el impacto operativo de la incorporación de algoritmos poscuánticos. Desde una perspectiva metodológica, su aporte resulta especialmente valioso porque permite sustentar que la preparación PQC debe ser gradual, empíricamente validada y limitada a escenarios controlados mientras no existan condiciones suficientes de interoperabilidad y desempeño en producción.

2.2.4. Astrizi & Custódio (2024): Transición híbrida a PQ-TLS

Astrizi y Custódio propusieron una estrategia de transición hacia TLS 1.3 poscuántico basada en un enfoque híbrido, en el que se combinan algoritmos clásicos con algoritmos poscuánticos para evitar que todos los componentes del ecosistema deban migrar de forma simultánea. El objetivo central de su trabajo fue mostrar que la incorporación progresiva de PQC puede realizarse sin exigir una ruptura inmediata con la infraestructura existente (Astrizi & Custódio, 2024).

El artículo presentó una prueba de concepto en la que se integró un esquema híbrido en TLS 1.3 y se evaluó su comportamiento en términos de latencia, consumo de memoria y complejidad de implementación. Los resultados mostraron que, aunque el uso combinado de algoritmos incrementa el consumo de recursos, ese aumento puede mantenerse en rangos manejables cuando la selección de algoritmos y parámetros se diseña de forma cuidadosa (Astrizi & Custódio, 2024).

El principal aporte del estudio consiste en demostrar que una transición híbrida no solo es conceptualmente deseable, sino técnicamente viable. A diferencia de enfoques que suponen un reemplazo total e inmediato, el trabajo de Astrizi y Custódio introduce una lógica de compatibilidad incremental, despliegue gradual y reducción de cambios disruptivos, lo que lo convierte en una referencia importante para escenarios donde la continuidad operativa es prioritaria (Astrizi & Custódio, 2024).

Para la presente investigación, este aporte se alinea con la lógica de transición por fases. No se trata de trasladar mecánicamente una propuesta pensada para TLS a una PKI completa, sino de aprovechar su principio central: la preparación poscuántica es más viable cuando se

implementa de manera progresiva, medible y compatible con el ecosistema vigente. Desde esta lectura, el artículo respalda conceptualmente la decisión de incorporar esquemas híbridos como etapa intermedia y no como estado final definitivo.

El trabajo también presenta límites claros, su ámbito directo es TLS 1.3, por lo que no desarrolla en detalle la incorporación del enfoque híbrido en perfiles X.509, políticas de certificación, HSM ni procesos de auditoría propios de una Entidad de Certificación regulada. Del mismo modo, no profundiza en restricciones normativas como las derivadas de ETSI, NIST, eIDAS[22] o del marco ecuatoriano, que son determinantes cuando la transición afecta servicios de confianza con validez jurídica (Astrizi & Custódio, 2024).

Para la presente investigación, este artículo refuerza una idea metodológica central: la introducción de PQC debe realizarse mediante rutas de coexistencia y validación controlada, no mediante sustituciones abruptas.

2.2.5. Hohm, Heinemann & Wiesmaier (2025): modelo de madurez CAMM[23]

Hohm, Heinemann y Wiesmaier propusieron el Crypto-Agility Maturity Model - CAMM como un marco para evaluar el grado en que una organización está preparada para cambiar algoritmos criptográficos de manera controlada, repetible y gobernada. El modelo define cinco niveles de madurez, desde un estado inicial y reactivo hasta un nivel avanzado en el que la cripto-agilidad se integra de forma sistemática a la gestión de tecnologías de información (Hohm et al., 2025).

[22] eIDAS: electronic IDentification, Authentication and trust Services- Reglamento de la Unión Europea
[23] CAMM: Crypto-Agility Maturity Model – Modelo de Madurez Cripto-agile

Cada nivel del modelo se describe a partir de requisitos agrupados en dimensiones técnicas, organizativas y de gobernanza. Entre los criterios considerados se encuentran la existencia de inventarios de algoritmos y dependencias, procesos formales de gestión de cambios criptográficos, automatización del despliegue, monitoreo continuo de estándares y alineación de políticas internas con recomendaciones externas como las del NIST (Hohm et al., 2025)

El principal aporte de este trabajo está en que traslada la discusión sobre criptografía desde el plano estrictamente técnico hacia el de la gestión institucional. En lugar de limitarse a recomendar que una organización sea cripto-ágil, CAMM proporciona niveles observables, criterios comparables y una ruta de evolución organizacional. Esto lo convierte en una referencia útil para investigaciones que no solo buscan describir una transición algorítmica, sino evaluar la capacidad real de una entidad para sostenerla (Hohm et al., 2025).

Para esta investigación, el valor de CAMM es particularmente alto porque ofrece una estructura conceptual adecuada para interpretar la transición de RSA a ECC y, posteriormente, la preparación para PQC, como un proceso de madurez organizacional y no únicamente como una actualización tecnológica. Desde esta perspectiva, la propuesta de la investigación es factible al vincular cada fase de migración con capacidades institucionales concretas, tales como inventario criptográfico, actualización de políticas, automatización y monitoreo.

No obstante, el modelo también presenta limitaciones para el problema específico que aborda este trabajo. CAMM no fue diseñado de forma exclusiva para Entidades de Certificación reguladas, por lo que requiere adaptación al contexto de una PKI sujeta a exigencias normativas, auditorías formales y validez jurídica de certificados. Además, no prescribe algoritmos concretos ni rutas técnicas específicas, sino que opera como un marco general de evaluación de madurez. Su

validación empírica, asimismo, se apoya en un conjunto todavía acotado de organizaciones y expertos (Hohm et al., 2025).

En consecuencia, este artículo no proporciona por sí mismo una estrategia de transición aplicable a una Entidad de Certificación ecuatoriana, pero sí aporta un marco analítico de gran utilidad para la investigación. Su principal contribución consiste en permitir que la propuesta no se interprete solo como un proyecto de cambio tecnológico, sino como una trayectoria de fortalecimiento institucional, en la que la cripto-agilidad se convierte en una capacidad medible y progresiva.

2.2.6. Cuadro comparativo de trabajos relacionados

Con el fin de sintetizar de manera comparativa los principales aportes de los estudios revisados, se presenta a continuación la Tabla 6, la cual resume sus objetivos, contribuciones, limitaciones y su relación con la presente investigación. Su incorporación permite observar de forma integrada qué dimensiones del problema han sido abordadas y cuáles permanecen escasamente desarrolladas.

Desde la perspectiva de esta investigación, la utilidad de la tabla no es solo descriptiva, sino también analítica, ya que permite identificar con mayor claridad los vacíos que la investigación busca atender, especialmente la ausencia de estudios centrados en una Entidad de Certificación regulada del contexto ecuatoriano, la falta de rutas integradas de transición progresiva y la escasa articulación entre desempeño técnico, conformidad normativa y madurez organizacional.

Tabla 6
Cuadro comparativo de trabajos relacionados

Autor(es) / Año	Tipo de estudio / Resumen breve	Aporte principal	Qué destaca del artículo	Limitaciones	Relación con el proyecto de investigación
Hadan, Serrano & Camp (2021)	Estudio mixto, Compara lo que los expertos creen que falla con las causas reales de los incidentes.	Propone una taxonomía de causas de fallo en PKI y demuestra una brecha entre percepciones expertas y fallos reales.	Enfoque mixto poco habitual en PKI, evidencia sólida de que la mayoría de incidentes provienen de procesos y gobernanza.	Se centra en WebPKI, no en PKI nacionales reguladas, depende de incidentes reportados públicamente, no aborda directamente migraciones de algoritmos ni cripto-agilidad.	Justifica que la estrategia de migración RSA a ECC y a PQC incluya criterios de paso, bitácoras de cambio, evidencias auditables, pruebas de regresión y planes de reversión. Refuerza el enfoque socio-técnico.
Giron et al. (2024)	Estudio experimental sobre emisión automatizada de certificados PQC usando ACME.	Muestra que el cuello de botella de certificados PQC no es sólo criptográfico, rediseñar ACME puede reducir el tiempo de emisión, el tamaño de comunicación, manteniendo la viabilidad	Automatización ACME con PQC, introduce un nuevo tipo de desafío ACME, resultados cuantitativos claros para tiempo y tráfico de red en emisión de certificados PQC.	Contexto centrado en WebPKI (Let's Encrypt, ACME); entorno de pruebas controlado, no una EC regulada; no aborda restricciones regulatorias ni procesos legales de firma/certificación.	Permite incluir KPIs de desempeño como tiempo de emisión, tamaño de mensajes, tasas de error y replantear los flujos de emisión/renovación/revocación en ECC y PQC. Reforzando la hoja de ruta PQC, esta debe ir acompañada de cambios en automatización y orquestación.

		de emisión masiva.			
Sosnowski et al. (2023)	Estudio experimental del desempeño de TLS 1.3 con algoritmos PQC y combinaciones híbridas	Proporciona una metodología robusta para evaluar el impacto de algoritmos PQC en TLS 1.3 y compararlos con algoritmos clásicos e híbridos en condiciones de red variadas.	Uso de métricas de percentiles (p95/p99), atención explícita a la interacción entre criptografía y condiciones de red reales.	Enfocado en TLS como protocolo, no analiza en detalle la gestión de certificados X.509 ni procesos internos de CAs, no discute marco legal.	Aporta un marco de medición para adaptar como banco de pruebas en la EC.
Astrizi & Custódio (2024)	Transición híbrida a TLS 1.3 poscuántico. Combina algoritmos clásicos y PQC para permitir una migración gradual sin necesidad de actualización simultánea de todos los	Demuestra que un enfoque híbrido en TLS 1.3 es técnicamente viable, con incrementos moderados de latencia y memoria, facilitando una transición fluida hacia seguridad	Énfasis en la transición, no sólo en el rendimiento de un algoritmo, principios claros de compatibilidad incremental, despliegue gradual y minimización de cambios disruptivos.	El ámbito directo es TLS, no toda la PKI; no da al detalle de perfiles X.509 ni de políticas de certificación; no considera en profundidad HSM, cumplimiento regulatorio ni marcos como eIDAS/NIST/ARC OTEL.	Respalda esquemas híbridos y fases de migración: primero RSA a ECC, luego emisión dual ECC y PQC. Aunque trata TLS.

	componentes.	poscuántica.			
Hohm, Heinemann & Wiesmaier (2025)	Proponen CAMM, de cinco niveles para evaluar la cripto-agilidad de una organización. Define requisitos por nivel en dimensiones técnicas, organizativas y de gobernanza.	Ofrece un marco estructurado para medir y planificar la cripto-agilidad, pasando de una situación reactiva a una gestión sistemática de cambios criptográficos.	Lleva la discusión de la criptografía al plano de la gestión y la gobernanza, integra normas, buenas prácticas y opinión de expertos.	Modelo general, no específico de Entidades de Certificación. Requiere adaptación a PKI reguladas, la validación empírica está limitada a un conjunto acotado de organizaciones, no prescribe algoritmos concretos.	Es la base para situar a la EC en un nivel inicial de madurez, definir el nivel objetivo y vincular cada fase de la ruta RSA a ECC a PQC. Refuerza una estrategia de evolución organizacional, no solo un cambio técnico.

Nota. Elaboración propia con base en (Hadan et al., 2021; Giron et al., 2024; Sosnowski et al., 2023; Astrizi & Custódio, 2024; Hohm et al., 2025).

2.2.7. Síntesis del estado del arte y brecha de investigación

La comparación crítica de los trabajos revisados muestra una convergencia parcial, pero no una solución integrada al problema de esta investigación. Hadan et al. (2021) explican fallos reales de gobernanza en WebPKI, pero no desarrollan una ruta de migración algorítmica para una EC regulada. Girón et al. (2024) estudian automatización de emisión con PQC en un contexto cercano a ACME, sin integrar requisitos regulatorios nacionales. Sosnowski et al. (2023) y Astrizi y Custódio (2024) cuantifican costos y alternativas híbridas en TLS, pero su unidad de análisis es el protocolo, no la infraestructura completa de certificación. Hohm et al. (2025) aportan un

modelo de madurez de cripto-agilidad, aunque no prescriben perfiles X.509, fases operativas ni criterios de conformidad para una EC ecuatoriana.

De forma complementaria, Ricchizzi et al. (2025) trasladan la discusión hacia un plano aplicado al presentar un enfoque práctico para la generación de certificados poscuánticos en entornos industriales (Ricchizzi et al., 2025). Este antecedente resulta particularmente relevante para la presente investigación porque evidencia la necesidad de estudiar PQC no solo desde la estandarización algorítmica, sino también desde su integración concreta en procesos de emisión y gestión de certificados. Su incorporación al estado del arte fortalece la orientación aplicada de la investigación y la necesidad de validar experimentalmente los componentes criptográficos antes de una adopción productiva.

Estas diferencias permiten precisar la brecha en cuatro niveles. Existe una brecha empírica, porque son limitados los estudios en EC reguladas latinoamericanas con evidencia de laboratorio y preproducción. Existe una brecha metodológica, porque desempeño, riesgo, conformidad y gobernanza suelen evaluarse por separado. Existe una brecha operacional, porque faltan rutas con criterios explícitos de paso, reversión y coexistencia RSA-ECC. Y existe una brecha prospectiva, porque la preparación PQC suele tratarse como recomendación general y no como componente medible de un artefacto de transición.

La investigación responde a esas brechas mediante un artefacto DSR integrado por banco de pruebas RSA-ECC, matriz de riesgos, fases de piloto-emisión dual-convergencia, KPIs, checklists normativos y guía PQC. Su originalidad no reside en proponer un algoritmo nuevo ni en afirmar validez universal, sino en vincular esos componentes en una secuencia reproducible de decisión y evaluación aplicada a una Entidad de Certificación específica del Ecuador.

La transferibilidad del aporte es, por tanto, metodológica y analítica. Otras organizaciones pueden reutilizar la estructura de evaluación, pero deben repetir las pruebas, adaptar los umbrales y validar la conformidad en su propio entorno antes de adoptar conclusiones equivalentes.

2.3. Marco teórico-conceptual

El presente marco teórico-conceptual expone los fundamentos históricos, conceptuales, normativos y tecnológicos que sustentan la transición desde esquemas PKI basados en RSA hacia arquitecturas cripto-ágiles apoyadas en ECC y preparadas para la criptografía pos-cuántica. Su propósito no es reiterar la evidencia empírica ya desarrollada en el estado del arte, sino ofrecer el soporte conceptual que permite interpretar el problema de investigación, estructurar el artefacto propuesto y justificar las decisiones metodológicas adoptadas en el presente proyecto.

La investigación asume una lectura socio-técnica de la PKI, según la cual las decisiones criptográficas no son neutras, sino que se encuentran atravesadas por marcos regulatorios, capacidades institucionales, racionalidades políticas y debates sobre soberanía digital (Feenberg, 1999; Floridi, 2020; Winner, 1986).

Esta interpretación puede complementarse con la perspectiva de la teoría del actor-red, según la cual los fenómenos tecnológicos se configuran mediante asociaciones entre actores humanos, elementos técnicos, instituciones, normas y prácticas, y no exclusivamente a partir de decisiones individuales o propiedades aisladas de la tecnología (Latour, 2005). Aplicado a una PKI, este enfoque permite interpretar la transición criptográfica como una reconfiguración de relaciones entre operadores, auditores, reguladores, algoritmos, HSM, políticas de certificación y sistemas clientes. Por ello, la migración RSA-ECC-PQC se analiza como una transformación socio-técnica y no únicamente como el reemplazo de un mecanismo criptográfico.

Desde este marco teórico, se justifica que la metodología no reduzca la transición criptográfica a una comparación entre algoritmos, sino que incorpore también gobernanza, conformidad normativa, gestión del cambio y viabilidad organizacional.

2.3.1. Ejes conceptuales del modelo de PKI de próxima generación

El modelo de PKI de próxima generación propuesto en esta investigación se organiza alrededor de tres ejes conceptuales estrechamente relacionados: cripto-agilidad y transición a PQC, interoperabilidad normativa e integración y evaluación técnica de nuevos esquemas criptográficos en una Entidad de Certificación real. Esta estructura permite vincular el problema tecnológico con sus implicaciones operativas, regulatorias y estratégicas.

El primer eje corresponde a la cripto-agilidad y a la transición hacia PQC. Este eje se fundamenta en los lineamientos del NIST sobre transición de algoritmos y gestión del ciclo de vida criptográfico, los cuales establecen que los algoritmos y longitudes de clave deben gestionarse dentro de procesos planificados de transición, considerando su estado de aceptación, restricciones de uso y evolución tecnológica (NIST, 2019; Barker & Roginsky, 2019). A ello se suman los esfuerzos de estandarización del propio NIST en materia de criptografía pos-cuántica, que sirven como referencia para planificar la futura incorporación de algoritmos resistentes a amenazas cuánticas (NIST, 2024b).

En la lógica de la investigación, este eje se traduce en una migración por fases, con inventario criptográfico, mecanismos de reversión y criterios de seguimiento. Desde este marco teórico, se justifica que la metodología adopte una transición progresiva y medible, porque la cripto-agilidad no se demuestra mediante una sola decisión técnica, sino mediante la capacidad institucional de gestionar cambios sucesivos de manera controlada.

El segundo eje corresponde a la interoperabilidad normativa en el contexto de certificados X.509 y servicios de confianza. La propuesta se apoya en referentes como ETSI EN 319 411-1 y en las Baseline Requirements del CA/Browser Forum, que definen condiciones de política, seguridad y reconocimiento para certificados públicamente confiables (ETSI, 2025; ETSI, 2021; CA/BrowserForum, 2023).

Este eje resulta decisivo porque una PKI de próxima generación no puede evaluarse únicamente por eficiencia técnica, sino también por su capacidad de conservar reconocimiento e interoperabilidad dentro de ecosistemas de confianza amplios. Desde este marco teórico, se justifica que la metodología adopte matrices de conformidad, checklists normativos y revisión de CP[24]/ CPS[25], ya que la transición perdería validez práctica si mejora el desempeño, pero compromete la compatibilidad normativa o técnica.

El tercer eje se centra en la integración y evaluación técnica de nuevos algoritmos criptográficos en infraestructuras reales. Informes recientes de ENISA subrayan que la estandarización de PQC no es suficiente por sí sola, y que resulta necesario estudiar su impacto en latencia, tamaño de clave, compatibilidad y dependencia de componentes críticos como HSM y middleware (ENISA, 2022).

A partir de este eje, la investigación orienta el análisis hacia bancos de prueba, validaciones de compatibilidad y una guía de preparación PQC. Desde este marco teórico, se justifica que la metodología adopte pruebas controladas e integración incremental, porque la

[24] CP: Certificate Policy – Política de Certificados
[25] CPS: Certificate Practice Statement – Declaración de Prácticas de Certificación

incorporación de nuevos algoritmos debe sostenerse sobre evidencia empírica en contexto y no solo sobre reconocimiento formal o estandarización documental.

2.3.2. Teorías fundamentales que sustentan el modelo

La propuesta de PKI de próxima generación no se sustenta únicamente en normas técnicas, sino también en un conjunto de teorías y enfoques que orientan el diseño del modelo, los criterios de evaluación y la integración de dimensiones técnicas, organizacionales y regulatorias. En este sentido, la Tabla 7 resume las teorías que fundamentan conceptualmente el modelo propuesto y muestra cómo cada una de ellas aporta criterios concretos para interpretar la transición de PKI desde RSA hacia ECC con preparación pos-cuántica.

Tabla 7
Teorías fundamentales

Teoría	**Autor(es) / fuente base**	**Principios clave**	**Aplicación en el modelo**
Privacy by Design	(Cavoukian, 2010)	Proactividad, privacidad por defecto, integración de la privacidad en el diseño, seguridad de extremo a extremo, transparencia y respeto por el usuario	Justifica el diseño de perfiles X.509 y políticas de certificación que minimizan exposición innecesaria de datos y fortalecen la protección por defecto en la emisión y validación de certificados
Confianza Criptográfica	(Chaum, 1985; Goldwasser & Micali, 1983)	Verificabilidad matemática, seguridad semántica, autenticidad criptográfica, confianza basada en propiedades comprobables	Sustenta la emisión dual, la validación rigurosa de certificados y la futura incorporación de esquemas híbridos ECC-PQC basados en mecanismos criptográficamente verificables

Crypto-agilidad	(NIST, Transitioning the Use of Cryptographic Algorithms and Key Lengths Revision 2, 2019; NIST, Transitioning the Use of Cryptographic Algorithms and Key Lengths Revision 3 NIST Special Publication 800 NIST SP 800-131Ar3 ipd, 2024c; Hohm et al., 2025)	Capacidad de cambiar algoritmos de forma planificada, repetible y gobernada; inventario criptográfico; gestión del cambio; monitoreo continuo	Fundamenta la migración por fases, los mecanismos de rollback, los checklists normativos, la actualización de CP/CPS y la evaluación del nivel de preparación criptográfica de la Entidad de Certificación
Design Science Research - DSR	(Hevner et al., 2004)	Diseño de artefactos, utilidad práctica, evaluación rigurosa, relevancia contextual, iteración y refinamiento	Justifica la construcción del artefacto metodológico de la investigación: estrategia de transición, matriz de riesgos, KPIs, checklists y guía PQC, todos diseñados y validados en contexto controlado
Enfoque Socio-Técnico Constructivista	(Bijker et al., 1987; Feenberg, 1999)	Los sistemas tecnológicos se configuran socialmente; interacción entre actores, normas, infraestructura y decisiones institucionales; no neutralidad tecnológica	Sustenta la incorporación de factores organizacionales, regulatorios y de gobernanza en la evaluación de la transición RSA-ECC-PQC, evitando tratar la PKI como un problema exclusivamente técnico

Nota. Elaboración propia con base en (Cavoukian, 2010; Chaum, 1985; Goldwasser & Micali, 1983; Hohm et al., 2025; Hevner et al., 2004; Bijker et al., 1987; Feenberg, 1999; NIST, 2019; NIST, 2024c).

La primera referencia es el principio de Privacy by Design, desarrollado por Cavoukian, según el cual la privacidad debe incorporarse desde el diseño de sistemas y procesos, y no añadirse de forma reactiva. Sus principios de proactividad, privacidad por defecto, integración en el diseño y seguridad de extremo a extremo resultan pertinentes para una infraestructura PKI, porque obligan a pensar la protección de datos desde la definición de perfiles, políticas y mecanismos de validación (Cavoukian, 2010). Desde este marco teórico, se justifica que la metodología adopte criterios de diseño orientados no solo a eficiencia criptográfica, sino también a resguardo de datos y trazabilidad compatible con principios de privacidad.

La segunda base conceptual corresponde a la confianza criptográfica, vinculada a los trabajos de Chaum y de Goldwasser y Micali. Estos autores muestran que la confianza puede apoyarse en propiedades matemáticas verificables, como la seguridad semántica del cifrado, la autenticidad demostrable de las firmas y la imposibilidad práctica de falsificación sin acceso a la clave privada (Chaum, 1985; Goldwasser & Micali, 1983). Desde este marco teórico, se justifica que la metodología adopte comparaciones entre RSA, ECC y esquemas híbridos, así como pruebas de validez y consistencia de certificados, dado que la propuesta se apoya en una noción de confianza sustentada en evidencia criptográfica verificable.

Un tercer pilar es la cripto-agilidad, entendida como la capacidad de una organización para cambiar algoritmos y parámetros criptográficos de manera controlada, repetible y gobernada. En esta investigación, esta idea se articula con las recomendaciones del NIST sobre transición de

algoritmos y con la necesidad de inventarios actualizados, procesos formales de gestión de cambios y monitoreo continuo del entorno criptográfico (NIST, 2024c; NIST, 2019). Desde este marco teórico, se justifica que la metodología adopte una transición progresiva, mecanismos de rollback, checklists de conformidad y actualización de políticas de certificación, porque la evolución de la Entidad de Certificación depende también de su capacidad organizacional para gestionar cambios sucesivos.

Desde una perspectiva más aplicada, Allen advierte que la cripto-agilidad suele ser ampliamente aceptada en el plano conceptual, pero mucho más compleja cuando debe traducirse en inventarios, priorización de dependencias, actualización de políticas y coordinación entre áreas técnicas y de negocio. Este señalamiento es relevante para la presente investigación porque permite comprender que la transición criptográfica no fracasa por falta de teoría, sino por la dificultad práctica de convertir esa teoría en capacidades institucionales estables (Allen, 2020).

Como cuarto fundamento, la Design Science Research (DSR) plantea que la investigación basada en diseño debe producir artefactos útiles y evaluarlos rigurosamente en el contexto donde se aplican. En la presente investigación, esta perspectiva se vincula con la construcción de un artefacto compuesto por fases de migración, criterios de paso, KPIs, checklists y guías técnicas (Hevner et al., 2004). Desde este marco teórico, se justifica que la metodología adopte el diseño y validación de un artefacto de transición PKI como núcleo del estudio, combinando utilidad práctica, evaluación rigurosa y refinamiento iterativo.

Finalmente, el modelo se apoya en un enfoque socio-técnico constructivista, representado en este trabajo por Bijker y Feenberg, según el cual los sistemas tecnológicos no son neutrales ni solo técnicos, sino configuraciones en las que intervienen actores, normas, infraestructuras e

intereses institucionales (Bijker et al., 1987; Feenberg, 1999). Desde este marco teórico, se justifica que la metodología adopte una validación que combine desempeño técnico, conformidad, riesgo y preparación organizacional, evitando reducir la PKI a un problema exclusivamente matemático.

En conjunto, estas teorías permiten comprender que la transición criptográfica no depende únicamente de seleccionar algoritmos más eficientes, sino de la capacidad de diseñar artefactos útiles, sostener interoperabilidad, proteger datos, gestionar el cambio y combinar decisiones tecnológicas con estructuras institucionales. Por ello, el marco teórico-conceptual no cumple aquí una función descriptiva aislada, sino que actúa como el sustento que explica y justifica las decisiones metodológicas adoptadas en la investigación.

2.3.3. Relación entre los ejes teóricos y la propuesta de PKI de próxima generación

Los ejes conceptuales y las teorías fundamentales descritas se articulan en la propuesta mediante cuatro dimensiones integradas: técnico-operativa, interoperabilidad-normativa, metodológica y soberanía-ética. Esta organización permite vincular explícitamente cada fundamento conceptual con decisiones concretas de diseño, evaluación y validación dentro del modelo de PKI de próxima generación.

En la dimensión técnico-operativa, la teoría de la confianza criptográfica respalda la comparación entre RSA, ECC y esquemas híbridos, así como la necesidad de validar empíricamente su comportamiento. Desde esta perspectiva, la confianza no depende solo de la autoridad institucional, sino también de propiedades verificables de emisión, firma, validación y revocación (Chaum, 1985; Goldwasser & Micali, 1983). Desde este marco teórico, se justifica que la metodología adopte bancos de prueba, mediciones de latencia, tamaño de certificados y uso de

recursos, porque la conveniencia de un esquema criptográfico debe demostrarse mediante evidencia técnica y no únicamente mediante afirmaciones normativas o teóricas.

En la dimensión de interoperabilidad y normativa, la cripto-agilidad se combina con los lineamientos de transición del NIST y con marcos de confianza como ETSI y CA/Browser Forum. Las recomendaciones del NIST sobre transición de algoritmos establecen que el cambio criptográfico debe tratarse como un proceso gestionado, mientras que ETSI y las Baseline Requirements delimitan las condiciones de reconocimiento, política y seguridad exigibles a una infraestructura de certificación (NIST, 2024b; ETSI, 2021; ETSI, 2025; CA/BrowserForum, 2023; NIST, 2019).

Desde este marco teórico, se justifica que la metodología adopte checklists normativos, revisión de CP/CPS y matrices de conformidad, porque la transición propuesta no solo debe ser eficiente, sino también reconocible dentro del ecosistema de confianza. La dimensión normativa deja así de ser un complemento documental y se convierte en un criterio de validez de la propuesta.

En la dimensión metodológica, la Design Science Research se combina con el enfoque socio-técnico constructivista para tratar la propuesta como un artefacto iterativo que debe diseñarse, evaluarse y refinarse en función del contexto. Desde este marco teórico, se justifica que la metodología adopte una implementación por objetivos, validación en entornos controlados y refinamiento progresivo, ya que el conocimiento generado depende de la interacción entre tecnología, organización y regulación (Hevner et al., 2004; Bijker et al., 1987).

Finalmente, la dimensión de soberanía y ética se vincula con enfoques de decisión multicriterio y con la discusión sobre autonomía tecnológica. Desde este marco teórico, se

justifica que la metodología adopte criterios de selección y priorización que no se limiten al desempeño técnico, sino que consideren también dependencia tecnológica, control institucional y proyección estratégica del ecosistema nacional (ENISA, 2022).

En conjunto, esta articulación muestra que la propuesta de PKI de próxima generación no surge de una suma de conceptos aislados, sino de una estructura teórica que conecta criptografía, regulación, diseño de artefactos y soberanía digital.

2.3.4. Marco histórico

Históricamente, la evolución de la PKI puede entenderse en tres grandes momentos. En una primera etapa, RSA se consolidó como el esquema dominante de criptografía asimétrica y sostuvo durante décadas buena parte de las infraestructuras de certificación digital, los perfiles X.509 y los servicios de autenticación, firma y cifrado desplegados en Internet y en entornos institucionales.

En una segunda etapa, el crecimiento de servicios móviles, dispositivos con recursos limitados y escenarios de alta demanda operativa hizo más visibles las limitaciones de RSA en términos de tamaño de clave, consumo computacional y escalabilidad. En ese contexto, ECC se consolidó progresivamente como una alternativa más eficiente para mantener niveles equivalentes de seguridad con menores costos operativos.

En la etapa actual, la amenaza asociada a la computación cuántica ha desplazado la discusión hacia la necesidad de preparar infraestructuras capaces de evolucionar nuevamente. Por ello, el camino histórico ya no se interpreta solo como el paso de RSA a ECC, sino como la necesidad de avanzar hacia esquemas cripto-ágiles, con capacidad de incorporar progresivamente mecanismos pos-cuánticos. Desde esta perspectiva, el marco histórico permite ubicar la propuesta

de la investigación dentro de una trayectoria de transformación que conduce hacia una PKI de próxima generación.

2.3.5. Marco referencial

El marco referencial de esta investigación combina aportes provenientes de la criptografía aplicada, la teoría institucional, la filosofía de la tecnología y la gobernanza digital. Esta combinación permite abordar la transición hacia una PKI basada en ECC con preparación pos-cuántica no como un simple cambio algorítmico, sino como un proceso multidimensional en el que convergen decisiones técnicas, regulatorias e institucionales.

Desde la criptografía aplicada, los trabajos de Stallings, Menezes y Hankerson permiten comprender las diferencias entre RSA y ECC en términos de seguridad, tamaño de clave, eficiencia y perfiles de uso. De forma complementaria, estudios más recientes extienden ese análisis hacia la integración de ECC y PQC en protocolos y servicios concretos, mostrando que la discusión ya no se limita a la teoría criptográfica, sino que involucra desempeño, compatibilidad y sostenibilidad operativa (Stallings, 2017; Menezes et al., 1997; Hankerson et al., 2004; Bos et al., 2014; Laassiri et al., 2022). Desde este marco teórico, se justifica que la metodología adopte métricas comparativas y validaciones de compatibilidad, porque la viabilidad de la transición no puede establecerse solo desde la equivalencia abstracta de seguridad.

En esta misma línea, Adams y Lloyd sostienen que una PKI no puede comprenderse solo desde los algoritmos o los certificados aislados, sino desde la articulación entre políticas de certificación, modelos de confianza, mecanismos de registro, revocación y condiciones reales de despliegue. Esta perspectiva resulta pertinente para la investigación porque refuerza que la transición hacia ECC no debe evaluarse como un reemplazo criptográfico puntual, sino como una

reconfiguración integral de la infraestructura y de los procesos que sostienen su operación (Adams & Lloyd, 2003).

A ello se añade la visión de Anderson, para quien la seguridad en sistemas distribuidos confiables depende tanto de la fortaleza técnica de los mecanismos como de la forma en que se administran fallos, claves, privilegios, dependencias y procedimientos operativos. En el contexto de esta investigación, este enfoque es útil porque sitúa a la PKI dentro del campo de la ingeniería de sistemas confiables y muestra que su modernización requiere tratar simultáneamente arquitectura, operación y control institucional (Anderson, 2020).

Desde la teoría institucional, autores como North y Scott permiten entender que las organizaciones no adoptan de manera inmediata la tecnología más eficiente, porque sus decisiones están condicionadas por reglas formales, rutinas, trayectorias previas y restricciones normativas (North, 1990; Scott, 2014). En el contexto de la investigación, este enfoque resulta útil para explicar por qué muchas Entidades de Certificación continúan apoyándose en RSA aun cuando ECC ofrece ventajas operativas y estratégicas. Desde este marco teórico, se justifica que la metodología adopte un análisis de factores condicionantes, matriz de riesgos y revisión de capacidades institucionales, ya que la transición depende también de la forma en que la organización procesa el cambio.

La filosofía de la tecnología aporta una lectura crítica sobre la supuesta neutralidad de las infraestructuras digitales. Feenberg y Winner sostienen que los sistemas tecnológicos materializan relaciones de poder, lógicas de control y opciones políticas, de modo que escoger entre una PKI jerárquica tradicional y modelos más distribuidos no es solo una decisión de eficiencia, sino también una decisión sobre gobernanza de la confianza y soberanía digital (Feenberg, 1999;

Winner, 1986). Desde este marco teórico, se justifica que la metodología incorpore la dimensión estratégica y no se limite al rendimiento algorítmico, porque la transición también implica autonomía tecnológica y capacidad institucional.

Finalmente, la gobernanza digital y la interoperabilidad subrayan la importancia de normas compartidas para que las PKI nacionales puedan ser reconocidas en ecosistemas más amplios. En este punto, marcos como ETSI, eIDAS, NIST y RFC 5480 muestran que los estándares no solo describen formatos técnicos, sino que estructuran reconocimiento cruzado y confianza internacional (ETSI, 2024a; Turner & Brown, 2009; W3C, 2022). Desde este marco teórico, se justifica que la metodología no se limite a medir desempeño, sino que incorpore también conformidad normativa, gobernanza y preparación organizacional como dimensiones de validación.

En conjunto, este marco referencial permite entender la transición hacia una PKI de próxima generación como un proceso que integra decisiones criptográficas, reformas normativas, capacidades institucionales y consideraciones de soberanía tecnológica. Su función en la investigación no es reiterar resultados empíricos ya examinados, sino ofrecer una base interpretativa que vincule el problema estudiado con la lógica metodológica adoptada.

2.3.6. Marco legal

El marco legal que regula la PKI y la adopción de algoritmos modernos como ECC y PQC está conformado por normas internacionales, regionales y nacionales, además de estándares técnicos especializados. En esta investigación, su análisis no cumple una función meramente descriptiva, sino que permite determinar hasta qué punto la propuesta de transición puede insertarse de manera válida dentro del ecosistema jurídico y regulatorio aplicable.

En este nivel normativo, la Recomendación X.509 de la UIT proporciona el marco estructural de referencia para certificados de clave pública y de atributos, y por ello sigue siendo un punto de apoyo indispensable para interpretar la arquitectura formal de la confianza digital. Su inclusión fortalece la investigación porque conecta la propuesta de transición no solo con regulaciones nacionales o sectoriales, sino también con el estándar base que organiza la lógica documental y validatoria de la certificación digital (ITU-T, 2012).

En el ámbito internacional, el Reglamento eIDAS establece las bases para los servicios de confianza y las firmas electrónicas en la Unión Europea, reconociendo la validez de distintos algoritmos siempre que se ajusten a perfiles y estándares técnicos adecuados. De forma complementaria, en Estados Unidos la ESIGN Act reconoce validez jurídica a las firmas electrónicas sin imponer una tecnología única, mientras el NIST orienta qué algoritmos resultan recomendables para uso federal y cómo deben planificarse sus transiciones (ETSI, 2024b; NIST, 2024a).

Desde la perspectiva de esta investigación, este punto resulta importante porque muestra que la validez jurídica de la confianza digital no depende de un algoritmo aislado, sino de su inserción dentro de marcos técnicos y legales reconocidos. Desde este marco teórico, se justifica que la metodología adopte revisión documental y mapeo multinivel, porque la propuesta debe ser técnicamente correcta y jurídicamente sostenible.

En la misma línea, el RFC 3647 aporta una estructura de referencia para las políticas de certificación y las declaraciones de prácticas de certificación, mostrando que estos documentos no cumplen una función meramente administrativa, sino que organizan responsabilidades, controles, criterios de emisión, revocación y auditoría dentro de una PKI. En el contexto de esta

investigación, este marco resulta útil porque refuerza que la migración criptográfica debe apoyarse en CP y CPS actualizados, de modo que la transición conserve trazabilidad, coherencia normativa y capacidad de verificación institucional (Chokhani et al., 2003).

En el plano técnico-normativo, documentos como FIPS 186-4, SP 800-57 y SP 800-131A establecen políticas de ciclo de vida criptográfico, tamaños mínimos de clave y estados de uso para algoritmos asimétricos, incluyendo RSA y ECC, al tiempo que preparan el terreno para la incorporación progresiva de algoritmos pos-cuánticos (NIST, 2024b).

Desde este marco teórico y legal, se justifica que la metodología adopte checklists normativos y criterios de transición, ya que la propuesta debe demostrar no solo viabilidad operativa, sino también coherencia con los estados de uso aceptados internacionalmente.

En el ámbito regional, ICP-Brasil constituye un ejemplo de infraestructura nacional que ya reconoce ECC dentro de su regulación técnica. En contraste, varios países latinoamericanos cuentan con leyes que habilitan la firma digital, pero con menor especificidad respecto a algoritmos, perfiles de certificado o esquemas de transición (Quiroz et al., 2020).

Esta diferencia regional evidencia que la modernización de la PKI no depende solo de contar con una ley habilitante, sino también de disponer de regulación técnica suficiente para orientar la implementación. Para la presente investigación, ello refuerza la necesidad de proponer una estrategia que no solo sea técnicamente viable, sino también jurídicamente interpretable dentro del contexto latinoamericano.

En el caso ecuatoriano, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento constituyen la base jurídica de la PKI nacional. Aunque este marco reconoce la validez de la firma electrónica y de la certificación digital, no detalla de manera

exhaustiva los algoritmos aceptados, lo que deja espacio para incorporar ECC y, a futuro, esquemas pos-cuánticos. La Norma Técnica de 2024 emitida por MINTEL y ARCOTEL introduce avances relevantes, entre ellos referencias a curvas recomendadas por NIST, obligatoriedad de OCSP, actualización de perfiles X.509 y alineación parcial con ETSI (Arcotel, 2024).

Desde la perspectiva de esta investigación, este marco no constituye una barrera absoluta para la transición, sino una base sobre la cual puede construirse una propuesta progresiva y jurídicamente defendible. Sin embargo, el hecho de que exista una base normativa no implica que la transición esté completamente resuelta, porque persisten vacíos en conceptos de perfiles híbridos, criterios para PQC y combinaciones más amplias con marcos internacionales.

En efecto, todavía se observan desafíos como la falta de lineamientos específicos para algoritmos pos-cuánticos, la escasa definición jurídica de esquemas híbridos ECC-PQC y la limitada articulación con marcos como eIDAS, NIST PQC y RFC especializadas. Estos vacíos son relevantes porque afectan la posibilidad de trasladar una innovación técnica a un entorno regulado sin generar incertidumbre interpretativa o de auditoría.

Desde este marco teórico y jurídico, se justifica que la metodología adopte revisión documental, mapeo normativo multinivel y evidencia de conformidad, ya que la transición hacia una PKI de próxima generación solo puede considerarse válida si mantiene continuidad operativa, interoperabilidad y sustentación legal suficiente en el contexto ecuatoriano.

Capítulo 3.

3.1. Propuesta metodológica

3.1.1. Enfoque

La investigación adopta un enfoque mixto con integración secuencial de evidencia cuantitativa y cualitativa. La dimensión cuantitativa mide comportamiento técnico-operativo, latencia, throughput, tamaño, CPU/RAM y compatibilidad; la dimensión cualitativa interpreta normativa, políticas, riesgos, restricciones organizacionales y valoración experta. Ambas dimensiones se integran en las decisiones del artefacto y no se presentan como estudios paralelos.

La perspectiva crítico-hermenéutica opera específicamente en la interpretación de normas, CP/CPS, dependencias institucionales y decisiones de gobernanza. Su función no es sustituir la medición experimental, sino explicar por qué una alternativa técnicamente eficiente puede no ser viable si entra en conflicto con obligaciones regulatorias, capacidades organizacionales o relaciones de confianza.

Design Science Research (DSR) constituye el marco de construcción y evaluación. El diagnóstico combina evidencia técnica y documental; el diseño transforma esa evidencia en fases, perfiles, KPIs, controles y guía PQC; la evaluación contrasta el artefacto mediante pruebas, matrices y revisión experta; y el refinamiento incorpora los hallazgos al diseño final. En consecuencia, el enfoque mixto produce la evidencia, la perspectiva crítico-hermenéutica aporta la interpretación contextual y DSR organiza el ciclo de solución.

3.1.2. Diseño de investigación

El diseño se enmarca en DSR porque el resultado central es un artefacto orientado a resolver un problema real de transición criptográfica. El artefacto integra estrategia por fases,

perfiles X.509, matriz de riesgos, checklists, KPIs y guía PQC. Su evaluación combina tres fuentes de evidencia: resultados experimentales, contraste normativo-organizacional y revisión experta.

La articulación metodológica sigue una lógica de triangulación: un hallazgo técnico solo se incorpora como criterio de diseño cuando puede relacionarse con compatibilidad y riesgo; un requisito normativo se traduce en checklist o control verificable; y una observación experta se documenta como ajuste del artefacto. Esta regla evita que la evaluación dependa de una sola fuente de evidencia.

3.1.2.1. Diagnóstico y problematización

En esta fase se identificó la situación inicial de la Entidad de Certificación analizada, considerando dependencias tecnológicas, restricciones operativas, estado de adopción de algoritmos, nivel de interoperabilidad y condiciones regulatorias aplicables. El diagnóstico no se concibió como una descripción general del contexto, sino como la base empírica y documental para delimitar el problema de investigación y orientar la formulación del artefacto.

3.1.2.2. Diseño del artefacto:

A partir del diagnóstico se diseñó el artefacto metodológico de transición, compuesto por fases de migración, perfiles criptográficos, mecanismos de reversión, matriz de riesgos, checklists normativos, KPIs y guía PQC. Esta fase articuló criterios técnicos, organizacionales y regulatorios con el fin de que la propuesta no se reduzca a un rediseño algorítmico, sino que constituya una ruta estructurada de implementación progresiva.

3.1.2.3. Implementación piloto y evaluación experimental:

El artefacto fue sometido a validación en entornos controlados o preproductivos, mediante pruebas técnicas, revisión documental, análisis de conformidad y contraste de resultados por objetivo específico. Esta fase permitió observar el comportamiento del modelo bajo condiciones comparables y generar evidencia sobre su viabilidad técnico-operativa, su compatibilidad y su coherencia normativa.

3.1.2.4. Refinamiento e integración:

Con base en los hallazgos obtenidos, la propuesta fue refinada para integrar ajustes técnicos, normativos y organizacionales. Esta fase permitió consolidar una versión metodológicamente más madura del artefacto, con mejor articulación entre los objetivos específicos, las técnicas aplicadas y la evidencia generada. Desde la lógica de la investigación, este refinamiento no constituye una corrección accesoria, sino una parte central del ciclo de diseño y validación propio de DSR.

3.2. Población y muestra

3.2.1. Descripción del Contexto: Escenario o lugar

El estudio se desarrolla en el contexto de una Entidad de Certificación acreditada en Ecuador, regulada por la normativa nacional de firmas electrónicas y sujeta a lineamientos técnicos de ARCOTEL y del Ministerio competente. Esta EC opera una PKI basada principalmente en algoritmos RSA, que brinda servicios de emisión, gestión y revocación de certificados digitales para personas naturales y jurídicas públicas o privadas.

La organización cuenta con equipos diferenciados para la gestión técnica de la PKI administración de HSM, servidores de emisión, repositorios OCSP/CRL, la operación de servicios

de certificación atención a clientes, validación de identidad, soporte de firmas, la gestión de seguridad de la información y el cumplimiento normativo. Este ecosistema constituye un sistema socio-técnico en el que decisiones técnicas (algoritmos, perfiles X.509, arquitectura) y decisiones organizacionales (políticas, procesos, gobernanza) se encuentran estrechamente entrelazadas.

El escenario específico de aplicación de la propuesta es el laboratorio y los entornos pre-productivos de la EC, donde se pueden desplegar nuevas versiones de la PKI como ECC, escenarios híbridos ECC más PQC, sin afectar inicialmente a los certificados en producción. En este contexto se realizan las pruebas de desempeño, las simulaciones de migración por fases y la validación del modelo con expertos internos y externos.

3.2.2. Especificar el tipo de muestreo y cómo lo realizó

Se utilizó un muestreo no probabilístico e intencional, adecuado a un estudio aplicado que requiere participantes con experiencia directa en operación, seguridad, cumplimiento y gobierno de PKI. La muestra estuvo compuesta por 12 participantes: 6 del equipo técnico, 4 de gobernanza y compliance y 2 expertos externos.

La suficiencia de la muestra se justificó por cobertura funcional de los roles críticos y no por representatividad estadística ni por saturación teórica. Los seis perfiles técnicos cubrieron administración PKI, HSM, emisión, validación, infraestructura y seguridad. Los cuatro perfiles de gobernanza cubrieron riesgo, CP/CPS, auditoría y cumplimiento. Y los dos externos aportaron una revisión independiente desde auditoría, consultoría y criptografía PKI. Esta composición permitió contrastar las tres dimensiones del artefacto: técnica, normativa-organizacional y de aplicabilidad.

Para proteger la confidencialidad institucional, la investigación reporta perfiles y funciones, no nombres. La evidencia conservada permite identificar la composición global de 12

participantes y su intervención en entrevistas, revisión de dependencias y valoración del artefacto a nivel de grupos funcionales; sin embargo, no conserva una matriz nominal que permita atribuir de forma verificable a cada persona una actividad específica de validación. Por rigor metodológico, no se reconstruye retrospectivamente esa asignación. La investigación tampoco afirma saturación teórica, porque no se documentó un procedimiento formal de codificación incremental destinado a demostrarla.

3.2.3. Criterios de selección y exclusión - no probabilístico

Al tratarse de un muestreo intencional, los criterios de inclusión se definen de la siguiente manera:

- Vinculación directa con la PKI de la Entidad de Certificación con participación en el diseño, operación, auditoría o supervisión de la infraestructura de clave pública.
- Experiencia mínima de dos años en roles relacionados con seguridad de la información, criptografía aplicada, gestión de certificados o cumplimiento regulatorio en servicios de certificación.
- Conocimiento de los marcos normativos aplicables, aunque sea en distintos grados según el perfil.
- Disponibilidad y consentimiento informado para participar en entrevistas, talleres de validación y revisión de documentos, manteniendo la confidencialidad requerida por la EC.

Los criterios de exclusión son:

- Personal que, aunque pertenezca a la organización, no interviene en procesos de PKI ni tiene responsabilidad sobre decisiones criptográficas o normativas.

- Proveedores externos cuya participación esté limitada a tareas técnicas de bajo nivel y que no puedan compartir información por restricciones contractuales.
- Candidatos que no acepten participar o que manifiesten conflictos de interés que puedan sesgar su juicio al evaluar el modelo.

La justificación de este enfoque no probabilístico es coherente con la epistemología crítica y hermenéutica asumida en el proyecto de investigación donde se privilegia la profundidad y la calidad de la información aportada por quienes construyen, interpretan y gobiernan la PKI, más que la representatividad cuantitativa de una población amplia de usuarios finales.

En consecuencia, la selección muestral no busca representatividad estadística, sino pertinencia analítica y profundidad contextual. Para esta investigación, resulta más relevante contar con participantes que intervienen directamente en la operación, regulación, validación y gobierno de la PKI que ampliar el número de casos sin incidencia real sobre el problema estudiado.

3.3. Instrumentos, método de validación y descripción del procedimiento de aplicación

3.3.1. Instrumento

Se utilizaron cuatro instrumentos complementarios: el protocolo técnico de pruebas RSA-ECC/PQC, cuya estructura completa se presenta en el Anexo A; la matriz normativo-organizacional y de riesgos, incluida en el Anexo B; el guion de entrevista semiestructurada dirigido a los informantes clave, presentado en el Anexo C; y la ficha de validación mediante juicio experto, incorporada en el Anexo D. La inclusión de estos instrumentos completos permite fortalecer la trazabilidad metodológica y facilita la revisión y eventual reproducción del procedimiento aplicado.

El protocolo técnico define servicios, algoritmos, variables de control, métricas, número de repeticiones, reglas de registro y criterios de depuración. La matriz normativo-organizacional traduce requisitos de NIST, ETSI, RFC y normativa nacional en ítems verificables y relaciona cada brecha con riesgo, impacto, control y evidencia. El guion de entrevista explora dependencias, compatibilidad, gobernanza, continuidad, regulación y preparación PQC. La ficha de juicio experto valora pertinencia, claridad, coherencia, suficiencia y aplicabilidad mediante escala ordinal y observaciones cualitativas.

Los instrumentos se vinculan directamente con los objetivos. El protocolo técnico produce la evidencia del OE1 y parte del OE3, la matriz de riesgos y conformidad sustenta el OE2, el guion y la revisión experta contribuyen al OE2, OE3 y OE4 y la ficha de validación documenta el refinamiento del artefacto dentro de DSR.

3.3.2. Método de validación del Instrumento

La validación se planteó mediante juicio experto y revisión de consistencia metodológica. Los perfiles de referencia fueron los definidos en la muestra: personal técnico, responsables de gobernanza y compliance y expertos externos, seleccionados por vinculación directa con PKI, experiencia mínima de dos años, conocimiento normativo o criptográfico y ausencia de conflictos de interés declarados. El expediente consolidado no conserva el número exacto de validadores que revisó cada instrumento por separado, por ello, la investigación informa la composición de la muestra y declara esta carencia de trazabilidad individual como limitación documental.

La ficha de juicio experto utiliza cinco criterios: pertinencia respecto del objetivo, claridad de redacción, coherencia entre variable e indicador, suficiencia de cobertura y aplicabilidad en el entorno de la EC. La versión final del artefacto evidencia ajustes coherentes con esos criterios:

mantiene las métricas técnicas centrales, refuerza compatibilidad, reversión y evidencia auditable, separa preparación PQC de adopción productiva y explicita la relación entre riesgos, controles y fases de migración. No se reportan puntuaciones numéricas de validación que no estén preservadas en el expediente.

No se calculó alfa de Cronbach porque los instrumentos no constituyen una escala psicométrica homogénea. La validez se sustentó en correspondencia de contenido, trazabilidad objetivo, instrumento, evidencia y triangulación entre fuentes. La ficha utilizada para la validación mediante juicio experto, incluyendo los criterios de pertinencia, claridad, coherencia, suficiencia y aplicabilidad, se presenta de forma completa en el Anexo D, con el propósito de garantizar la trazabilidad del procedimiento y facilitar su revisión y reutilización en futuras investigaciones.

3.3.3. Descripción del procedimiento de aplicación

La aplicación siguió cinco etapas.

- Primero, se obtuvo autorización institucional para utilizar un entorno controlado y se informó a los participantes sobre objetivos, uso académico de la información y confidencialidad.
- Segundo, se ejecutó el protocolo técnico y se generaron registros de latencia, throughput, recursos, tamaños y compatibilidad.
- Tercero, se aplicó la matriz normativo-organizacional y de riesgos, cuya estructura y criterios de evaluación se presentan en el Anexo B.
- Cuarto, se realizaron entrevistas a los informantes clave utilizando el guion semiestructurado incorporado en el Anexo C y se efectuó la revisión experta

mediante los criterios contenidos en la ficha de validación del Anexo D, con el propósito de interpretar las brechas identificadas y valorar el artefacto propuesto.

- Quinto, se consolidaron las observaciones obtenidas y se utilizaron como insumo para refinar la estrategia por fases y la guía de preparación pos-cuántica.

La trazabilidad se mantuvo mediante identificadores de escenario, algoritmo, servicio, fase, fecha de ejecución y fuente de evidencia. Los resultados técnicos alimentaron los riesgos y KPIs, las brechas normativas se tradujeron en controles y la revisión experta se utilizó para ajustar criterios de paso, reversión y preparación pos-cuántica.

3.3.4. Consideraciones éticas

La ejecución del estudio requirió acceso institucional al entorno controlado de la Entidad de Certificación y tratamiento de información técnica con fines académicos. La versión metodológica establece que los participantes debían recibir información sobre propósito, voluntariedad y confidencialidad, y que el consentimiento informado constituía un criterio de inclusión. Con el propósito de estandarizar este procedimiento, el modelo de consentimiento informado y confidencialidad utilizado como referencia metodológica se incorpora en el Anexo E. Su inclusión permite documentar los elementos mínimos que deben comunicarse a los participantes, tales como el propósito del estudio, el carácter voluntario de la participación, el tratamiento confidencial de la información y el uso exclusivamente académico de los datos recopilados. El expediente aportado no contiene, como anexo verificable, una carta o resolución institucional de autorización; por ello, no se atribuye un número o fecha de autorización que no esté documentado.

Para reducir riesgos de exposición, los resultados se presentan de forma agregada, se omiten nombres de participantes, credenciales, direcciones internas, números de serie sensibles y material criptográfico privado. Las evidencias técnicas se limitaron a métricas, configuraciones no secretas, logs depurados y artefactos necesarios para la investigación. No se utilizaron claves privadas productivas ni se ejecutaron cambios que afectaran certificados de usuarios finales.

En los archivos incorporados a esta investigación no consta un dictamen formal de aprobación o exención emitido por un comité de ética. Por rigor documental, no se atribuye retrospectivamente un número de aprobación inexistente. El estudio se clasifica como investigación tecnológica de riesgo mínimo para participantes, pero esta ausencia de constancia formal se reconoce expresamente como limitación documental y deberá subsanarse conforme al procedimiento institucional aplicable antes de cualquier ampliación que involucre datos personales adicionales o intervención sobre producción.

3.4. Matriz de Variables

Con el fin de operacionalizar el problema de investigación y asegurar coherencia entre objetivos, variables, instrumentos y evidencia, se presenta la Tabla 8. Esta matriz permite visualizar la relación entre las variables o categorías de análisis consideradas en el estudio, los objetivos a los que responden y el aporte que cada una realiza a la validación del modelo propuesto. Desde esta perspectiva, la matriz no cumple una función meramente descriptiva, sino que constituye un recurso de articulación metodológica entre el diseño de la investigación, la recolección de datos y el análisis posterior de resultados.

Tabla 8
Matriz de Variables

Correlación entre el instrumento	Variables / Categoría de análisis	Objetivos a los que responde	Propuesta (qué aporta al modelo)
Protocolo técnico de pruebas de desempeño RSA vs ECC (scripts de medición de latencia, tamaño, throughput, CPU/RAM, compatibilidad clientes/navegadores/ HSM).	V1. Desempeño criptográfico y operativo de RSA y ECC en la EC (latencia de validación, tamaño de certificados y cadenas, throughput, uso de CPU/RAM, compatibilidad con HSM y navegadores).	OE1. Analizar comparativamente RSA y ECC en una Entidad de Certificación, midiendo latencia, tamaño, throughput, uso de CPU/RAM y compatibilidad, listar diferencias y condiciones de aplicabilidad.	Genera la línea base comparativa RSA vs ECC, define condiciones de aplicabilidad de ECC en la EC y provee los KPIs técnicos que se usarán en el diseño de la estrategia integral de transición (OG y OE3).
Matriz de riesgos técnico-normativos organizacionales (recolección de datos con equipo técnico, gobernanza y expertos).	V2. Factores internos y externos que condicionan la migración a ECC (riesgos técnicos, normativos, organizacionales, de soberanía digital; probabilidad e impacto; planes de mitigación).	OE2. Identificar y evaluar factores internos y externos que condicionan la migración a ECC, construyendo una matriz de riesgos con planes de mitigación.	Produce la matriz de riesgos priorizada y sus planes de mitigación, insumo directo para definir el orden de las fases Piloto a Emisión dual a Convergencia y para los mecanismos de rollback de la propuesta (OE3, OE4).
Matriz de madurez de cripto-agilidad y cumplimiento (checklists NIST SP 800-131A, ETSI EN	V3. Madurez de cripto-agilidad, cumplimiento normativo e interoperabilidad (nivel de adopción de buenas	OE3. Diseñar y crear un escenario progresivo de adopción piloto, emisión dual,	Entrega el perfil inicial de madurez y cumplimiento y permite fijar KPIs y checklists

319 411-1, CA/B Forum, normas locales).	prácticas, alineación con NIST/ETSI/CA-B, compatibilidad de sistemas ≥ 80 %).	convergencia y preparación post-cuántica, actualizando perfiles X.509 con ECC, flujos OCSP/CRL e incorporando KPIs y checklists auditables.	auditables para cada fase del escenario progresivo; soporta la demostración de compatibilidad de sistemas ≥ 80 % (OG y OE3).
Guion de entrevistas semiestructuradas a informantes clave (técnicos, gobernanza, expertos externos).	V4. Percepción de viabilidad, continuidad operativa e interoperabilidad ante la migración RSA a ECC y a PQC y la introducción de esquemas híbridos.	OE2, OE3 y OE4. Identificar factores condicionantes, validar la factibilidad del escenario progresivo y recoger criterios para la guía de preparación pos-cuántica.	Aporta evidencia cualitativa para ajustar fases, priorizar acciones de mitigación y capacitación; permite refinar la estrategia integral de transición y la guía PQC desde la perspectiva de los actores involucrados.
Plantilla de diseño de perfiles X.509 ECC e híbridos ECC+PQC + revisión documental (CP/CPS, estándares).	V5. Especificaciones de perfiles criptográficos y políticas de curvas, rotación y revocación (parámetros ECC, algoritmos híbridos, políticas de rotación de claves/algoritmos, planes de reversión).	OE3. Diseñar el escenario progresivo (perfiles X.509 con ECC, política de curvas, flujos OCSP/CRL, KPIs) y OE4. Integrar una guía de preparación pos-cuántica con políticas de rotación y reversión.	Produce las plantillas de perfiles X.509 ECC e híbridos, las políticas de rotación y reversión y los componentes técnicos de la guía PQC, integrados en la estrategia de transición (OG[26], OE3, OE4).
Documento “Guía de preparación pos-	V6. Criterios de introducción de	OE4. Integrar una guía de preparación	Resultado final: Guía PQC

[26] OG: Objetivo General

cuántica (PQC)" + validación por expertos	esquemas híbridos ECC+PQC y continuidad operativa (momentos, condiciones y controles para introducir PQC sin perder interoperabilidad).	pos-cuántica (PQC) con criterios de introducción de esquemas híbridos, políticas de rotación y planes de reversión, asegurando continuidad operativa e interoperabilidad.	integrada al modelo, con criterios claros de cuándo, cómo y bajo qué condiciones introducir PQC, asegurando continuidad operativa e interoperabilidad para la EC (apunta directo al OG).

Nota. Elaboración propia.

En conjunto, la matriz de variables permite mostrar que la investigación se estructura sobre una relación explícita entre categorías analíticas, objetivos específicos, instrumentos de levantamiento y resultados esperados. Para la presente investigación, esta articulación es importante porque fortalece la trazabilidad metodológica del estudio y permite justificar cómo las dimensiones técnico-operativa, normativa, organizacional y prospectiva se integran dentro de un mismo diseño de validación.

3.5. Establecimiento de Metodología por Objetivos

Con el fin de hacer explícita la relación entre cada objetivo específico, el método aplicado, las técnicas e instrumentos utilizados y la evidencia esperada, se presenta la Tabla 9. Esta matriz de trazabilidad metodológica permite visualizar de manera integrada cómo se operacionaliza cada componente de la investigación y cómo se vincula con los resultados que posteriormente serán analizados en el capítulo correspondiente. Desde esta perspectiva, la metodología no se organiza como una suma de procedimientos aislados, sino como una secuencia articulada de decisiones

orientadas a validar la viabilidad técnico-operativa, la interoperabilidad y la conformidad normativa de la propuesta.

Tabla 9
Matriz de trazabilidad metodológica por objetivos específicos

Objetivo específico	**Método / enfoque de ejecución**	**Técnica(s)**	**Instrumentos**	**Evidencia o resultado esperado**
OE1. Analizar comparativamente RSA y ECC	Validación experimental en entorno controlado o preproductivo	Benchmarks, pruebas de carga, medición comparativa, análisis de compatibilidad	Protocolo técnico de pruebas, scripts de medición, registros de logs, matriz de compatibilidad	Métricas de latencia, throughput, tamaño de certificados y cadenas, uso de CPU/RAM y compatibilidad efectiva
OE2. Identificar y evaluar factores condicionantes	Análisis documental, hermenéutico y de riesgo	Revisión normativa, análisis de requisitos, identificación de dependencias, valoración de riesgo	Matriz normativo-organizacional, checklist de conformidad, matriz de riesgos	Brechas normativas y organizacionales identificadas, factores internos y externos priorizados, riesgos clasificados y lineamientos de mitigación
OE3. Diseñar y validar un escenario progresivo de adopción	Diseño aplicado y validación iterativa del artefacto	Síntesis de requisitos, modelado de fases, diseño de perfiles y políticas, contraste con criterios de control	Escenario de migración por fases, perfiles X.509, políticas criptográficas, checklists auditables, KPIs por fase	Propuesta estructurada de piloto, emisión dual y convergencia, con criterios de paso, reversión, compatibilidad y conformidad
OE4. Proponer e integrar una guía de preparación PQC	Diseño prospectivo y validación cualitativa	Revisión conceptual, definición de criterios de adopción,	Guía PQC, criterios de esquemas híbridos, lineamientos de	Guía de preparación pos-cuántica coherente con la infraestructura

		estructuración de guía, revisión experta	rotación y reversión, instrumento de validación cualitativa	analizada, con lineamientos aplicables para futura adopción

Nota. Elaboración propia a partir de los objetivos específicos, las hipótesis y el diseño metodológico de la investigación.

La matriz anterior permite advertir que cada objetivo específico cuenta con una ruta metodológica diferenciada, pero articulada dentro de un mismo diseño de investigación. En consecuencia, las pruebas técnicas, el análisis normativo y la validación cualitativa no operan como bloques independientes, sino como componentes complementarios que convergen en la construcción y validación del artefacto propuesto.

3.6. Implementación

La implementación del proyecto de investigación se organiza de manera que cada fase del trabajo aporte evidencia directa para el objetivo general y los cuatro objetivos específicos, para ello, se combinan actividades experimentales, diagnósticas y proyectivas, articuladas con la matriz de variables independientes, dependientes y de control y con la metodología por objetivos definida previamente.

El trabajo se estructura en cuatro bloques principales:

- Implementación del estudio experimental RSA vs ECC (OE1).
- Implementación del diagnóstico de factores y matriz de riesgos (OE2).
- Implementación del diseño del escenario progresivo de migración (OE3).
- Implementación de la guía de preparación pos-cuántica (OE4).

En todos los casos se respetan las recomendaciones internacionales sobre transición criptográfica y cripto-agilidad, particularmente las guías del NIST SP 800-131A para transiciones

de algoritmos y longitudes de clave (NIST, 2019; Barker & Roginsky, 2019), el programa de criptografía poscuántica de NIST (NIST, 2024b), el estándar ETSI EN 319 411-1 para prestadores de servicios de confianza (ETSI, 2021) y el estudio de integración de criptografía poscuántica de ENISA (ENISA, 2022).

3.6.1. Implementación del OE1: Estudio experimental RSA versus ECC

3.6.1.1. Planeación y preparación del entorno

Servicios evaluados:

Se consideraron emisión de certificados, validación OCSP y operaciones de handshake/validación TLS en perfiles comparables. Los escenarios criptográficos documentados fueron RSA-2048/SHA-256 como línea base; ECC P-256/SHA-256 y P-384/SHA-384; y un escenario de laboratorio ECC+PQC destinado exclusivamente a anticipar impactos. La documentación metodológica histórica denomina los componentes pos-cuánticos como CRYSTALS-Kyber y CRYSTALS-Dilithium; en el texto final se aclara que estas denominaciones corresponden a propuestas que posteriormente dieron lugar a ML-KEM y ML-DSA, sin afirmar que se haya realizado una migración productiva con los estándares finales.

Software y plataforma criptográfica:

Las pruebas se ejecutaron sobre la plataforma de CA/OCSP y el HSM del entorno controlado de la EC, manteniendo la misma configuración entre comparaciones. No se documentan las versiones exactas de CA, Java, sistema operativo, librerías criptográficas y firmware del HSM utilizadas en cada ciclo de prueba. Por integridad científica, dichas versiones no se reconstruyen retrospectivamente; el Anexo F establece su registro obligatorio para cualquier réplica. El componente PQC se trató exclusivamente como laboratorio.

Hardware y sistema operativo:

Las comparaciones RSA-ECC se ejecutaron manteniendo el mismo perfil de cómputo, almacenamiento y red para evitar que diferencias de plataforma explicaran los resultados. No se detalla el modelo físico de CPU, asignación exacta de vCPU/RAM ni la versión del sistema operativo de cada prueba. Por integridad científica, esos valores no se reconstruyen retrospectivamente; Esta ausencia se declara como limitación de reproducibilidad y el Anexo F establece los campos obligatorios que deberán registrarse en cualquier réplica.

Herramientas y scripts:

Se utilizaron llamadas OCSP repetidas, automatización de handshakes TLS, exportación e inspección de certificados, cadenas y monitoreo de CPU, RAM, Entrada/Salida y throughput. Los scripts registraron por fila el algoritmo, servicio, fase, marca temporal, latencia, estado de respuesta y métricas de recursos. Los comandos o scripts específicos se conservan como artefactos de reproducibilidad y su estructura mínima se reproduce en el Anexo A.

Repeticiones de pruebas:

Para cada combinación de servicio, algoritmo y carga, no se registra retrospectivamente un número histórico. Para futuras réplicas se establece en el Anexo F un mínimo metodológico de 80 repeticiones por operación y algoritmo en microbenchmark, claramente identificado como protocolo recomendado y no como reconstrucción del experimento histórico.

3.6.1.2. Ejecución de pruebas

Las pruebas se organizaron por algoritmo y servicio, manteniendo constantes las variables de plataforma. Para cada medición se verificó primero conectividad, validez del certificado,

estado de la CA/OCSP y disponibilidad del HSM. Después se ejecutaron las repeticiones y se registraron los resultados en una matriz única.

La metodología original definió cargas baja, media y alta. Sin embargo, se realizaron para la investigación series completas y comparables únicamente para carga baja y carga alta. La carga media no se utiliza para contrastar hipótesis ni se imputan valores retrospectivamente. Por esta razón, el capítulo de resultados se limita explícitamente a baja y alta, y la ausencia de la serie media se incorpora como limitación metodológica. Para una réplica, el Anexo F exige fijar y registrar antes de cada prueba la concurrencia, duración, ramp-up[27], número total de solicitudes y tasa objetivo de cada nivel de carga.

Para el control y depuración de datos, el protocolo final define como no válidos los registros sin respuesta criptográficamente válida, las ejecuciones interrumpidas por fallos ajenos al algoritmo y las mediciones con inconsistencia entre marca temporal y estado del servicio. No se permite eliminar valores solo por su magnitud. Toda exclusión debe conservar causa y referencia al log. No se dispone de una bitácora completa de exclusiones históricas; por ello, esta regla se presenta como criterio explícito de reproducibilidad para nuevas ejecuciones y como limitación para la reconstrucción exacta de las pruebas ya realizadas.

3.6.1.3. Estrategia de análisis de resultados

Análisis cuantitativo descriptivo y comparativo

Se calculan medias, máximos, mínimos y desviaciones estándar para cada indicador en RSA y ECC. Se construyen gráficos que permitan visualizar: la reducción de tamaño de

[27] Ramp-up: periodo o proceso de aumento gradual

certificados y cadenas al pasar de RSA a ECC, el impacto en latencia para cada servicio, el cambio en uso de recursos y throughput bajo carga.

Cálculo de mejoras y condiciones de aplicabilidad

Se expresa el cambio relativo en porcentaje con la reducción de tamaño de certificados ≥ 30 %, mejora o degradación de latencia dentro de un rango aceptable, compatibilidad efectiva ≥ 80 % de plataformas probadas.

Se documentan las condiciones de aplicabilidad de ECC, con servicios donde el cambio es neutro o positivo, restricciones identificadas.

Salida para los siguientes objetivos

Los resultados de OE1 alimentan: la definición de KPIs técnicos en el modelo de migración que es respecto al Objetivo Específico 3 – OE3, la identificación de riesgos técnicos - OE2, los criterios de desempeño mínimo en la guía pos-cuántica - OE4.

3.6.2. Implementación del OE2: Factores condicionantes y matriz de riesgos

El segundo objetivo específico se orienta a identificar y evaluar los factores técnicos, normativos y organizacionales que condicionan la transición desde una PKI basada en RSA hacia ECC en la Entidad de Certificación analizada. A diferencia del OE1, centrado en comparación experimental, este objetivo se apoya en un enfoque documental, interpretativo y analítico, orientado a construir una base de decisión para el diseño del escenario progresivo de migración.

3.6.2.1. Revisión documental y análisis hermenéutico

En esta fase se realizó una revisión sistemática de normativa local, estándares internacionales, lineamientos de transición criptográfica, requisitos de interoperabilidad, documentación institucional y dependencias operativas de la infraestructura analizada. El objetivo

no fue únicamente recopilar normas o políticas, sino interpretar de qué manera tales referentes condicionan o habilitan una transición progresiva hacia ECC con preparación pos-cuántica.

El análisis hermenéutico permitió identificar relaciones entre requisitos normativos, restricciones técnicas y capacidades organizacionales. En particular, se examinó cómo los criterios de NIST, ETSI, perfiles X.509, OCSP/CRL, políticas de certificación y condiciones del contexto ecuatoriano inciden sobre la viabilidad del cambio criptográfico. Esta fase produjo una lectura integrada del problema, evitando tratar la normativa como un apéndice externo al diseño metodológico.

Desde la perspectiva de esta investigación, el resultado de esta fase no se limita a describir el marco regulatorio, sino que permite identificar brechas concretas entre los requisitos aplicables y la situación de la Entidad de Certificación. Dichas brechas constituyen un insumo directo para la matriz de riesgos, para la definición de controles y para el posterior diseño del escenario progresivo de migración.

3.6.2.2. Elaboración de la matriz de riesgos

A partir de la revisión documental y del análisis de factores internos y externos, se construyó una matriz de riesgos orientada a clasificar amenazas, vulnerabilidades, impactos y condiciones de mitigación asociadas a la transición. La matriz se estructuró considerando probabilidad, impacto, criticidad y capacidad de respuesta, con el fin de priorizar riesgos relevantes para la continuidad operativa, la interoperabilidad y la conformidad normativa de la infraestructura.

La elaboración de la matriz no se limitó a una clasificación abstracta de riesgos. Cada entrada se vinculó con dependencias concretas de la Entidad de Certificación, tales como soporte

de HSM, compatibilidad de clientes, restricciones regulatorias, capacidades del equipo técnico, trazabilidad de políticas y posibilidad de reversión. De este modo, la matriz no funcionó solo como herramienta de diagnóstico, sino como instrumento de decisión metodológica.

Desde la lógica de la investigación, la matriz de riesgos permite priorizar controles, justificar criterios de paso entre fases y establecer condiciones de reversión dentro del artefacto propuesto. En consecuencia, su función no es únicamente preventiva, sino estructurante del diseño metodológico, ya que traduce factores condicionantes en decisiones concretas de implementación.

La estructura utilizada para sistematizar este análisis se presenta en el Anexo B, correspondiente a la Matriz normativo-organizacional y de riesgos. Este instrumento relaciona cada dimensión evaluada con el ítem de verificación, la evidencia requerida y el riesgo asociado a su incumplimiento, permitiendo mantener trazabilidad entre las brechas identificadas, los controles propuestos y las decisiones incorporadas al escenario de transición.

3.6.3. Implementación del OE3: Escenario progresivo de migración

Este objetivo se desarrolla siguiendo la lógica de DSR, en la que el modelo de PKI de próxima generación se concibe como un artefacto que se diseña, implementa parcialmente, evalúa y refina iterativamente (Hevner et al., 2004).

En conjunto, estas subfases permiten transformar los hallazgos técnicos y normativos previos en un escenario operativo verificable, con perfiles, políticas, flujos y criterios de control susceptibles de ser aplicados y auditados en entornos controlados o preproductivos.

3.6.3.1. Síntesis de requisitos y restricciones

Requisitos Técnicos

Se toman los KPIs derivados del Objetivo Específico 1 - OE1: latencia, tamaño, throughput, compatibilidad, como metas de desempeño mínimo para las fases futuras. Se puede establecer como requisito que la migración a ECC debe mantener o mejorar la latencia en al menos el 80 % de los servicios críticos y reducir el tamaño promedio de certificados/cadenas en ≥ 30 %.

Requisitos normativos y organizacionales

A partir de la matriz de madurez y del mapeo normativo, se definen requisitos como: cumplir el umbral institucional definido para los ítems críticos aplicables de NIST SP 800-131A, cumplir los requisitos aplicables de ETSI EN 319 411-1 para certificados públicos, mantener los SLA comprometidos con clientes durante las ventanas de cambio.

Restricciones y supuestos

Disponibilidad de soporte ECC en HSM y middleware, limitaciones presupuestarias y de tiempo para la migración, dependencias con otros proyectos tecnológicos de la organización.

3.6.3.2. Diseño de perfiles X.509 y políticas criptográficas

Perfiles X.509 ECC

Se definen nuevas plantillas de certificados con campos de clave pública ECC como, curvas P-256, P-384, según recomendaciones NIST, extensiones adecuadas y parámetros de uso de clave. Se revisan periodos de validez, tamaños de claves de respaldo y políticas de revocación.

Políticas de curvas y rotación

Se documenta una política de curvas que indique qué curvas se aceptan, en qué periodos y en qué condiciones se podrán introducir nuevas curvas o algoritmos híbridos. Se diseñan

procedimientos de rotación de claves y algoritmos, especificando periodicidad, responsables, pasos técnicos y exigencias de auditoría.

Flujos OCSP/CRL

Se revisan y actualizan los flujos de publicación de CRL y de respuestas OCSP para asegurar que soporten los nuevos tamaños de certificados y que mantengan los tiempos de respuesta acorde a los SLA.

3.6.3.3. Modelado del escenario por fases

Se estructura un escenario progresivo con, al menos, cuatro fases:

Fase 0 – Situación actual (solo RSA)

Sirve como línea base para todos los indicadores y se documenta a detalle la configuración, procesos y SLA.

Fase 1 – Piloto ECC

Se habilitan perfiles ECC en un subconjunto controlado de servicios y clientes. Se monitoriza exhaustivamente latencia, throughput, uso de recursos, incidentes y compatibilidad. Criterio de éxito es alcanzar los KPIs mínimos sin incidentes críticos.

Fase 2 – Emisión dual (RSA + ECC)

Se ofrecen certificados tanto RSA como ECC según el tipo de cliente/servicio y se establece una política de preferencia por ECC cuando la compatibilidad lo permita. Se continúan registrando métricas y se evalúan impactos sobre la operación y los SLA.

Fase 3 – Convergencia ECC y preparación PQC

Se migra la mayoría de los servicios a ECC, manteniendo RSA solo para compatibilidades residuales. Se comienzan pruebas de laboratorio con certificados híbridos ECC+PQC, alineados con las recomendaciones de NIST sobre algoritmos pos-cuánticos. Cada fase incluye:

- Objetivos específicos,
- KPIs a monitorear,
- Riesgos esperados y controles,
- Criterios de paso y planes de reversión.

3.6.3.4. Checklists y validación iterativa

Checklists de cumplimiento

Se elaboran listas de verificación por fase, basadas en NIST SP 800-131A, ETSI EN 319 411-1 y requisitos de la autoridad nacional. Estas listas se utilizan como evidencia auditable del avance y aportan insumos para la variable nivel de conformidad normativa.

Validación con expertos y ciclos de mejora

El modelo de escenario progresivo se presenta a personal interno y externo. Se recogen observaciones y se ajustan componentes técnicos hasta alcanzar una versión consensuada, apta para su inclusión en la propuesta final del proyecto de investigación.

3.6.4. Implementación del OE4: Guía de preparación pos-cuántica

El cuarto objetivo específico se orienta a proponer e integrar una guía de preparación pos-cuántica para la Entidad de Certificación analizada. Este objetivo no persigue una adopción inmediata de algoritmos PQC en producción, sino la formulación de criterios, lineamientos y mecanismos de preparación que permitan ordenar una futura incorporación de esquemas híbridos ECC con PQC dentro de una lógica de continuidad operativa e interoperabilidad.

3.6.4.1. Marco conceptual PQC aplicado

En esta fase se construyó el marco conceptual aplicado de la guía, a partir de estándares y lineamientos recientes sobre criptografía pos-cuántica, transición híbrida, cripto-agilidad y gestión del ciclo de vida criptográfico. El propósito fue identificar criterios técnicamente viables para la futura incorporación de PQC en la Entidad de Certificación, sin perder de vista las restricciones actuales de la infraestructura, del contexto normativo y del ecosistema de interoperabilidad.

La revisión de este marco permitió delimitar qué aspectos debían considerarse prioritarios en la guía: coexistencia temporal de algoritmos, rotación de claves, actualización de perfiles y políticas, reversibilidad, trazabilidad de decisiones y madurez organizacional para absorber nuevos cambios criptográficos. Desde la lógica de esta investigación, esta fase es importante porque evita que la preparación pos-cuántica se plantee como un ideal abstracto y la traduce en criterios aplicables al contexto específico del estudio.

3.6.4.2. Contenido de la guía PQC

Con base en el marco conceptual definido, se estructuró una guía de preparación pos-cuántica compuesta por lineamientos para introducción de esquemas híbridos ECC con PQC, criterios de selección de algoritmos, políticas de rotación de claves y algoritmos, mecanismos de reversión, recomendaciones de actualización de perfiles y criterios de seguimiento. La guía se concibe como un instrumento de preparación progresiva y no como una receta cerrada de implementación inmediata.

Su finalidad metodológica es ofrecer una referencia ordenada para la toma de decisiones futuras, articulando la información obtenida en los objetivos anteriores con una perspectiva de

transición. En este sentido, la guía no opera de manera aislada, sino como resultado integrado del análisis técnico, normativo y organizacional realizado en la investigación.

3.6.4.3. Validación y cierre del ciclo de diseño

La validación de la guía se realizó mediante revisión experta y contraste con los hallazgos obtenidos en los objetivos anteriores. Este procedimiento permitió verificar su coherencia con el escenario técnico actual, con las restricciones normativas identificadas y con la lógica gradual de transición adoptada en la investigación.

La revisión experta se estructuró considerando los criterios de pertinencia, claridad, coherencia, suficiencia y aplicabilidad definidos en el instrumento de validación descrito metodológicamente en la sección 3.3.2 y presentado de forma completa en el Anexo D. De esta manera, las observaciones obtenidas se incorporaron al ciclo iterativo de refinamiento del artefacto propio de la metodología Design Science Research.

Desde la perspectiva del estudio, esta fase cumple una doble función: por un lado, cerrar el ciclo de diseño del artefacto; y, por otro, asegurar que la dimensión pos-cuántica quede integrada de manera realista y metodológicamente consistente con el resto de la propuesta. De este modo, la guía PQC no se incorpora como un anexo prospectivo, sino como una parte constitutiva del modelo de PKI de próxima generación planteado en la investigación.

3.7. Pruebas

La fase de pruebas constituye un componente transversal de validación empírica del artefacto metodológico, principalmente en relación con el OE1 y con la verificación operativa del escenario progresivo definido en el OE3. Su finalidad es observar, en entornos controlados o preproductivos, el comportamiento de los algoritmos, perfiles y flujos definidos, manteniendo

condiciones comparables de hardware, software, red y carga de trabajo. En consecuencia, las pruebas no se entienden como ejercicios aislados de laboratorio, sino como una estrategia de generación de evidencia para sostener la viabilidad de la propuesta.

3.7.1. Escenarios de prueba simulados

Los escenarios de prueba simulados fueron diseñados para comparar el comportamiento de RSA y ECC bajo condiciones equivalentes, así como para observar el efecto de los cambios propuestos en perfiles, tamaños de certificados, validación y uso de recursos. Para preservar comparabilidad, se controlaron variables como plataforma de hardware, condiciones de red, versión de software y patrón de carga, de conformidad con las variables de control definidas en la investigación.

Las pruebas incluyeron escenarios de carga baja y alta, operaciones de validación, emisión y análisis de cadenas, con el fin de generar métricas observables sobre latencia, throughput, tamaño de certificados y uso de recursos. Adicionalmente, estos escenarios permitieron verificar compatibilidad y detectar posibles restricciones operativas relevantes para el diseño por fases.

Desde la perspectiva de esta investigación, los escenarios simulados no sustituyen la operación real en producción, pero sí constituyen una base metodológicamente válida para estimar comportamiento, compatibilidad y riesgo antes de una eventual adopción ampliada. Por ello, las pruebas se incorporan como evidencia de validación gradual del artefacto y no como demostración definitiva de despliegue en producción.

3.8. Trazabilidad y reproducibilidad

La reproducibilidad del estudio se organiza mediante seis artefactos: protocolo técnico de pruebas, inventario de software/hardware, matriz de parámetros de carga, scripts/comandos,

matriz de datos depurados y repositorio de evidencias. Cada ejecución debe poder reconstruirse a partir de un identificador único que relacione configuración, algoritmo, servicio, carga, fecha, resultado y log.

Para evitar sobreinterpretación, se distinguen dos niveles: reproducibilidad de la metodología y reproducibilidad exacta del experimento histórico. La primera queda documentada en los anexos y permite repetir el procedimiento. La segunda está limitada a la información de todos los metadatos de hardware, duración y concurrencia de cada prueba en cada escenario. Esta limitación se declara de forma explícita y no se compensa con valores estimados.

Toda réplica deberá registrar como mínimo:

- Versión de CA/OCSP, Java, HSM, firmware y sistema operativo.
- CPU/vCPU, RAM y almacenamiento.
- Latencia y ancho de banda de red.
- Script y hash de versión; algoritmo y parámetros.
- Número de repeticiones.
- Concurrencia.
- Ramp-up.
- Duración.
- Total de solicitudes.
- Criterios de exclusión.
- archivos de evidencia.

La plantilla completa para documentar estos parámetros y garantizar la trazabilidad de futuras réplicas se presenta en el Anexo F, incluyendo nivel de carga, concurrencia, ramp-up, duración,

número de repeticiones, configuración de software y hardware, resultados obtenidos, referencia de evidencias y criterios de exclusión aplicados.

Capítulo 4.

4.1. Resultados por Objetivo

En este apartado se presentan los resultados obtenidos para cada objetivo específico de la investigación. La exposición se organiza en función de los cuatro objetivos definidos en el estudio, con el fin de mantener trazabilidad entre la evidencia empírica obtenida, las hipótesis planteadas y el artefacto metodológico validado. En esta sección se reporta qué se obtuvo en las pruebas, matrices y productos desarrollados; la interpretación de su significado se desarrolla posteriormente en los apartados de análisis y discusión.

4.1.1. Resultados del Objetivo Especifico 1 – OE1

El primer objetivo específico se orientó a comparar el comportamiento de RSA y ECC en una Entidad de Certificación específica del Ecuador, bajo entornos controlados o preproductivos, utilizando métricas como latencia de validación, tamaño de certificados, throughput, uso de CPU/RAM y compatibilidad con clientes. Para ello se ejecutaron pruebas comparativas entre perfiles criptográficos equivalentes, manteniendo constantes las variables de control definidas en el diseño metodológico.

4.1.1.1 Rendimiento por algoritmo y carga

La tabla comparativa presenta únicamente carga baja y carga alta porque son las dos condiciones para las que el expediente experimental conserva series completas, trazables y comparables. La carga media, aunque fue prevista en el diseño, no se utiliza para sustentar H1 ni para calcular conclusiones debido a que su serie consolidada no puede reconstruirse con el mismo nivel de evidencia. No se estimaron ni interpolaron valores faltantes.

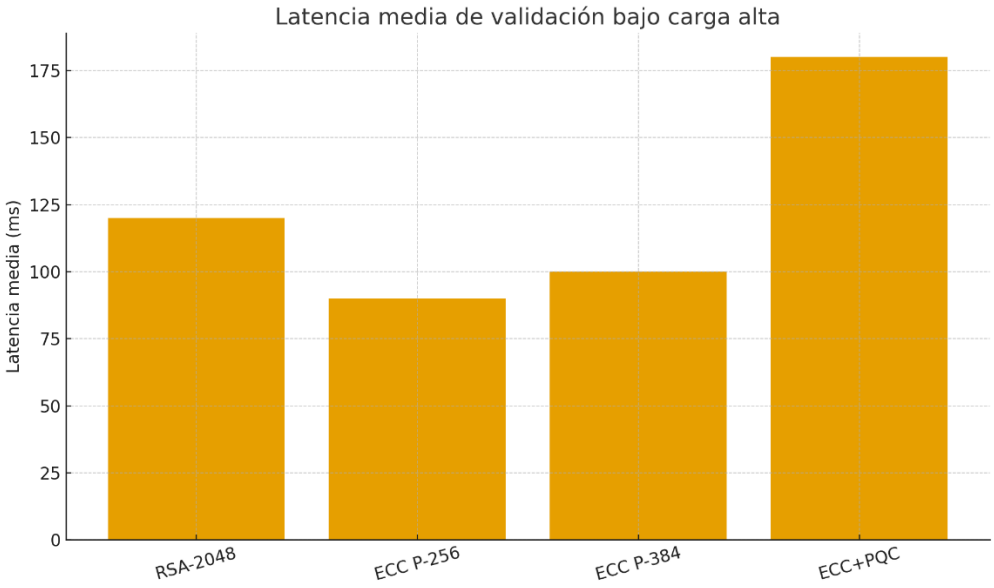
La Tabla 10 presenta los resultados comparativos de desempeño observados bajo escenarios de carga baja y carga alta. En ella se sintetiza el comportamiento de los algoritmos evaluados en términos de latencia y throughput, permitiendo observar el desempeño relativo de RSA y ECC en condiciones comparables de prueba. La Figura 1 muestra la latencia media de validación bajo carga alta, mientras que la Figura 2 representa el throughput de emisión en el mismo escenario, con el propósito de facilitar una lectura visual de las diferencias registradas.

Tabla 10
Desempeño bajo carga baja y alta

Algoritmo	Carga	Latencia media validación (ms)	Latencia p95 (ms)	Throughput emisión (cert/s)	Throughput validación (op/s)	Uso CPU (%)	Uso RAM (MB)
RSA-2048 / SHA-256	Baja	60	90	40	120	35	600
RSA-2048 / SHA-256	Alta	120	180	180	450	75	900
ECC P-256 / SHA-256	Baja	50	70	45	140	30	550
ECC P-256 / SHA-256	Alta	90	130	210	520	65	850
ECC P-384 / SHA-384	Baja	55	80	42	130	32	580
ECC P-384 / SHA-384	Alta	100	150	190	490	70	880
PQC híbrido ECC+PQC	Baja	80	120	25	90	45	700
PQC híbrido ECC+PQC	Alta	180	260	100	280	85	1100

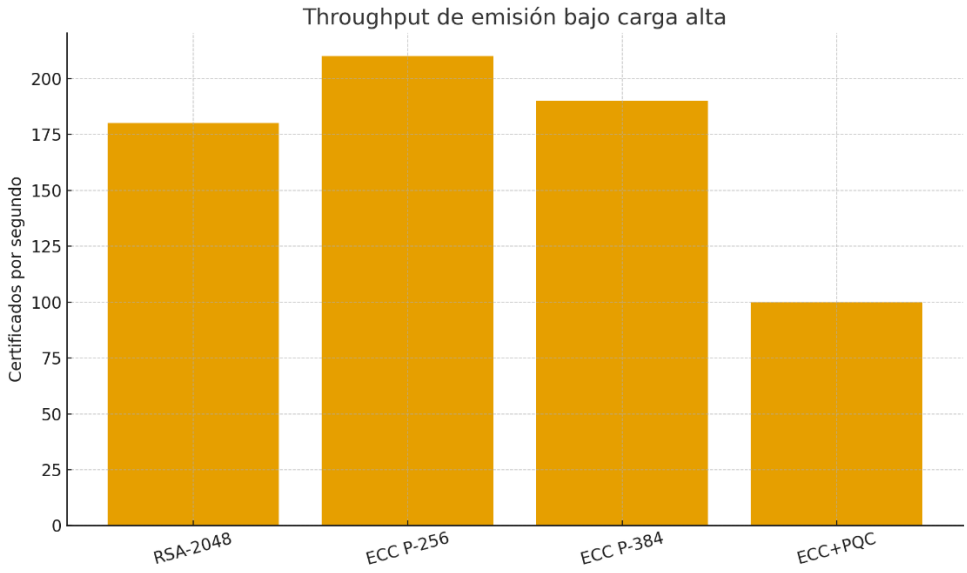
Nota. Elaboración propia.

Figura 1
Latencia media de validación bajo carga alta



Nota. Elaboración propia.

Figura 2
Throughput de emisión bajo carga alta



Nota. Elaboración propia.

Los resultados consignados en esta fase muestran que el comportamiento operativo difiere según el algoritmo y la carga aplicada, tanto en tiempo de respuesta como en capacidad de procesamiento. Estas diferencias constituyen la base empírica de la comparación técnico-operativa desarrollada en el banco de pruebas.

Este bloque de resultados aporta evidencia directa para el OE1, porque permite comparar el comportamiento de RSA y ECC en métricas de rendimiento bajo condiciones controladas. Asimismo, contribuye a la contrastación de la H1, en la medida en que permite verificar si ECC presenta mejoras operativas frente a RSA en latencia y throughput.

4.1.1.2 Tamaño de certificados y cadenas

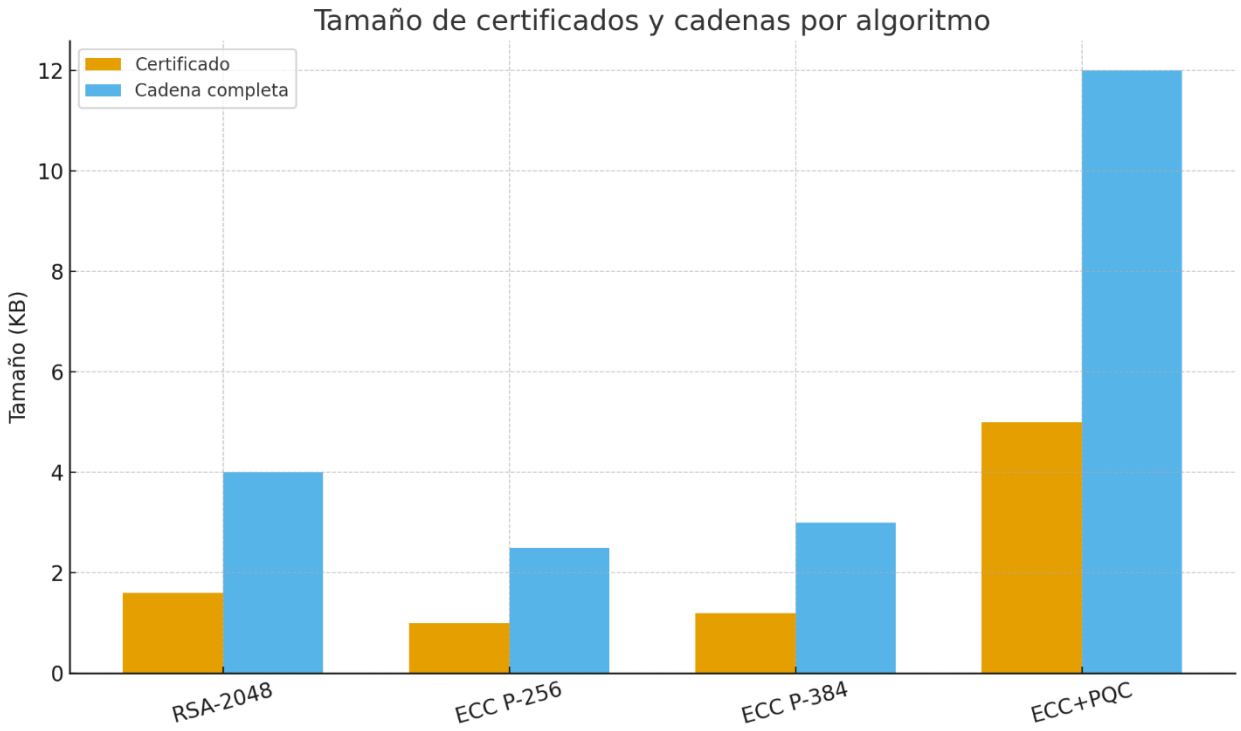
La Tabla 11 resume el tamaño de certificados y cadenas de certificación generados en cada escenario criptográfico evaluado. Su finalidad es mostrar el efecto del algoritmo sobre el peso estructural de los artefactos emitidos por la Entidad de Certificación. De manera complementaria, la Figura 3 presenta una visualización comparativa del tamaño de los certificados y de las cadenas, lo que permite observar con mayor claridad las diferencias registradas entre RSA y ECC.

Tabla 11
Tamaño de certificados y cadenas por algoritmo

Algoritmo	**Tamaño de certificado (KB)**	**Tamaño de cadena completa (KB)**
RSA-2048 / SHA-256	1,6	4,0
ECC P-256 / SHA-256	1,0	2,5
ECC P-384 / SHA-384	1,2	3,0

Nota. Elaboración propia.

Figura 3
Tamaño de certificados y cadenas por algoritmo



Nota. Elaboración propia.

Los resultados obtenidos muestran una diferencia observable en el tamaño de los certificados y de las cadenas según el algoritmo utilizado. Esta diferencia documenta el efecto del algoritmo sobre el peso estructural de los artefactos emitidos por la infraestructura evaluada.

Este subapartado contribuye de forma específica al OE1, al aportar evidencia empírica sobre una de las variables centrales de la comparación RSA–ECC. Del mismo modo, fortalece la contrastación de la H1, en lo relativo a la disminución esperada del tamaño de certificados y cadenas frente a infraestructuras jerárquicas tradicionales basadas en RSA.

4.1.1.3. Uso de recursos

Además de la latencia, el throughput y el tamaño criptográfico, las pruebas registraron el comportamiento del consumo de recursos de infraestructura, especialmente en términos de CPU y memoria, durante la operación con los distintos algoritmos evaluados. Este componente permitió observar el costo operativo asociado a cada escenario bajo condiciones controladas y comparables.

Los resultados muestran diferencias en el uso de recursos de infraestructura entre los perfiles criptográficos considerados, tanto en escenarios clásicos como en configuraciones con preparación híbrida. Esta evidencia complementa la comparación técnico-operativa y permite valorar la exigencia computacional relativa de cada alternativa.

En conjunto, los resultados del OE1 muestran diferencias observables entre RSA y ECC en latencia, tamaño criptográfico, throughput y uso de recursos bajo condiciones controladas. Este conjunto de evidencias contribuye directamente al OE1 y permite contrastar la H1, en particular en lo relativo a la mejora técnico-operativa esperada para ECC frente a RSA.

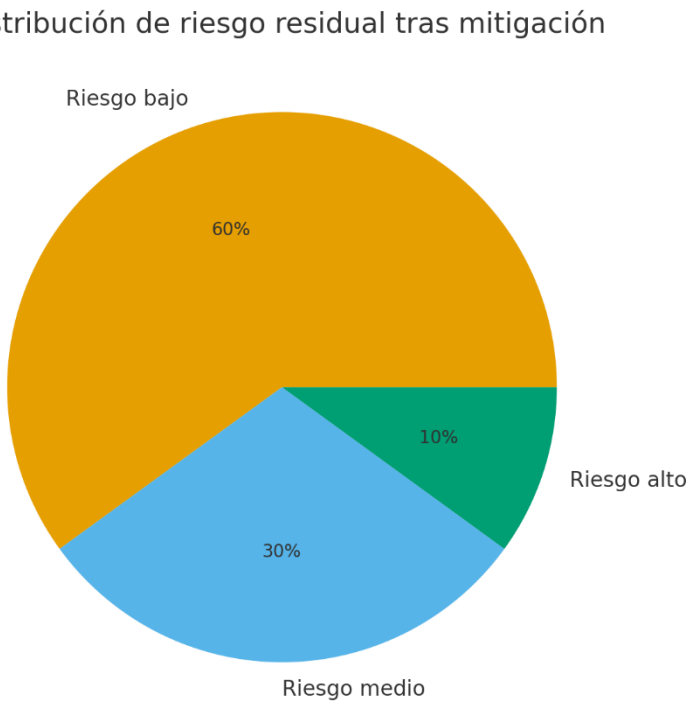
4.1.2 Resultados del Objetivo Especifico 2 – OE2

El segundo objetivo específico se orientó a identificar y evaluar los factores técnicos, normativos y organizacionales, internos y externos, que condicionan la transición de una PKI basada en RSA hacia ECC en una Entidad de Certificación específica del Ecuador. Para ello se aplicaron revisión documental, análisis hermenéutico y elaboración de una matriz de riesgos, con el fin de establecer brechas, restricciones y medidas de mitigación viables en entornos controlados o preproductivos.

4.1.2.1 Principales hallazgos de la matriz de riesgos

La matriz de riesgos permitió identificar factores críticos asociados a la transición, agrupados en dimensiones técnicas, normativas y organizacionales. Entre ellos se observaron dependencias de infraestructura, necesidad de actualización de políticas, requerimientos de capacitación, compatibilidad de componentes y exigencias de control del cambio. La Figura 4 presenta la distribución del riesgo residual tras la mitigación, con el propósito de visualizar cómo se redistribuyen los niveles de criticidad una vez considerados los controles propuestos.

Figura 4
Distribución de riesgo residual tras mitigación



Nota. Elaboración propia.

Los resultados muestran que, una vez aplicadas las medidas de mitigación definidas, la mayor parte de los riesgos identificados se desplaza hacia categorías más controlables, con

predominio de niveles de menor criticidad en condiciones de validación controlada. Esta evidencia permite documentar de manera estructurada qué factores condicionan la transición y en qué medida pueden ser gestionados dentro del modelo propuesto.

En conjunto, estos hallazgos muestran que la transición no depende únicamente de la viabilidad técnica del algoritmo, sino también de factores normativos, organizacionales y de gestión del riesgo. Este resultado aporta evidencia para el Objetivo Específico 2 y contribuye a la evaluación de la H2, especialmente en lo relativo a la reducción del riesgo residual y al fortalecimiento de la conformidad normativa.

4.1.3 Resultados del Objetivo Especifico 3 – OE3

El tercer objetivo específico se orientó a diseñar y validar un escenario progresivo de adopción compuesto por piloto, emisión dual, convergencia y preparación pos-cuántica, mediante perfiles X.509 basados en ECC, políticas de curvas, flujos de validación OCSP/CRL, KPIs operativos y checklists auditables de cumplimiento. Para ello se definieron fases comparables y se observaron indicadores de desempeño, compatibilidad, conformidad y preparación PQC.

La Tabla 12 presenta los KPIs registrados por fase, mientras que las Figuras 5, 6 y 7 permiten visualizar la evolución de la latencia, el throughput y los indicadores de compatibilidad, conformidad y preparación pos-cuántica a lo largo del modelo propuesto. Los resultados muestran que la latencia media disminuye de 120 ms en la fase 0 a 100 ms en la fase 3, mientras que el throughput aumenta de 180 a 220 certificados por segundo. Asimismo, la compatibilidad efectiva se mantiene por encima del 92 % en todas las fases, superando el umbral mínimo del 80 % establecido en el diseño metodológico.

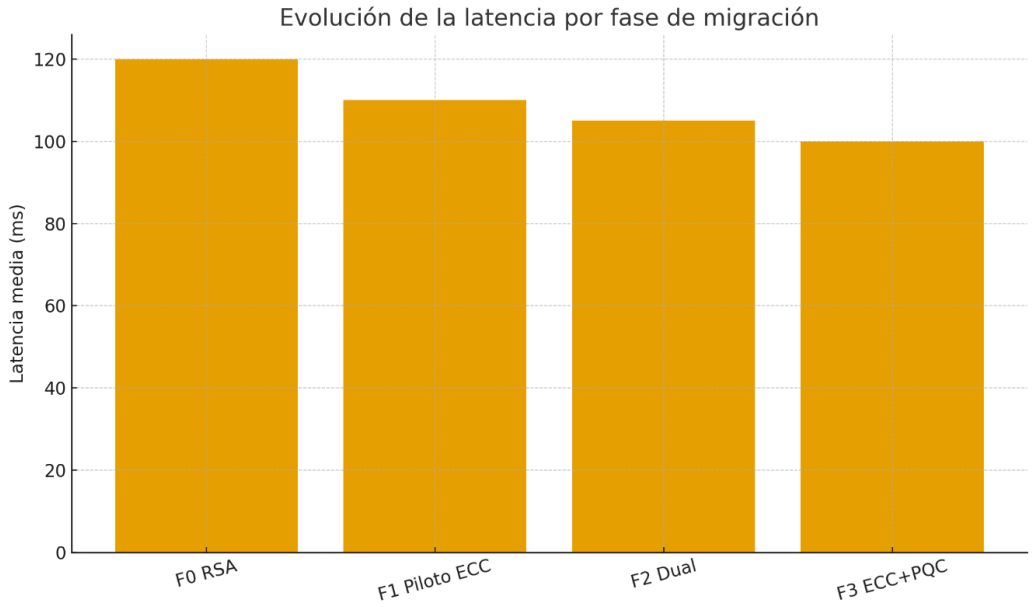
Tabla 12
KPIs por fase

Fase	Latencia media validación (ms)	Throughput emisión (cert/s)	Compatibilidad efectiva (%)	Conformidad normativa (%)	Índice de preparación PQC (%)
Fase 0 – Solo RSA	120	180	98	70	10
Fase 1 – Piloto ECC P-256	110	190	96	78	25
Fase 2 – Emisión dual RSA+ECC	105	210	94	85	40
Fase 3 – Convergencia ECC + pruebas PQC	100	220	92	90	70

Nota. Elaboración propia.

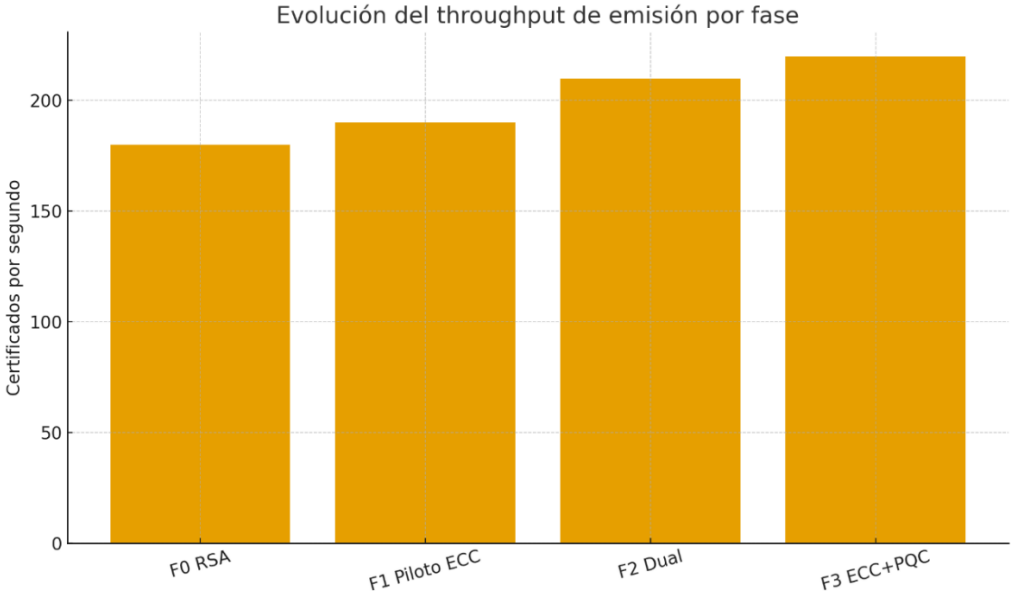
En el mismo bloque de resultados se observa que la conformidad normativa aumenta de 70% a 90%, en correspondencia con la alineación progresiva a NIST SP 800-131A y ETSI EN 319 411-1. De igual manera, el índice de preparación PQC crece de 10% a 70%, reflejando la incorporación de inventario criptográfico, pruebas de laboratorio y políticas documentadas de preparación pos-cuántica.

Figura 5
Latencia por fase



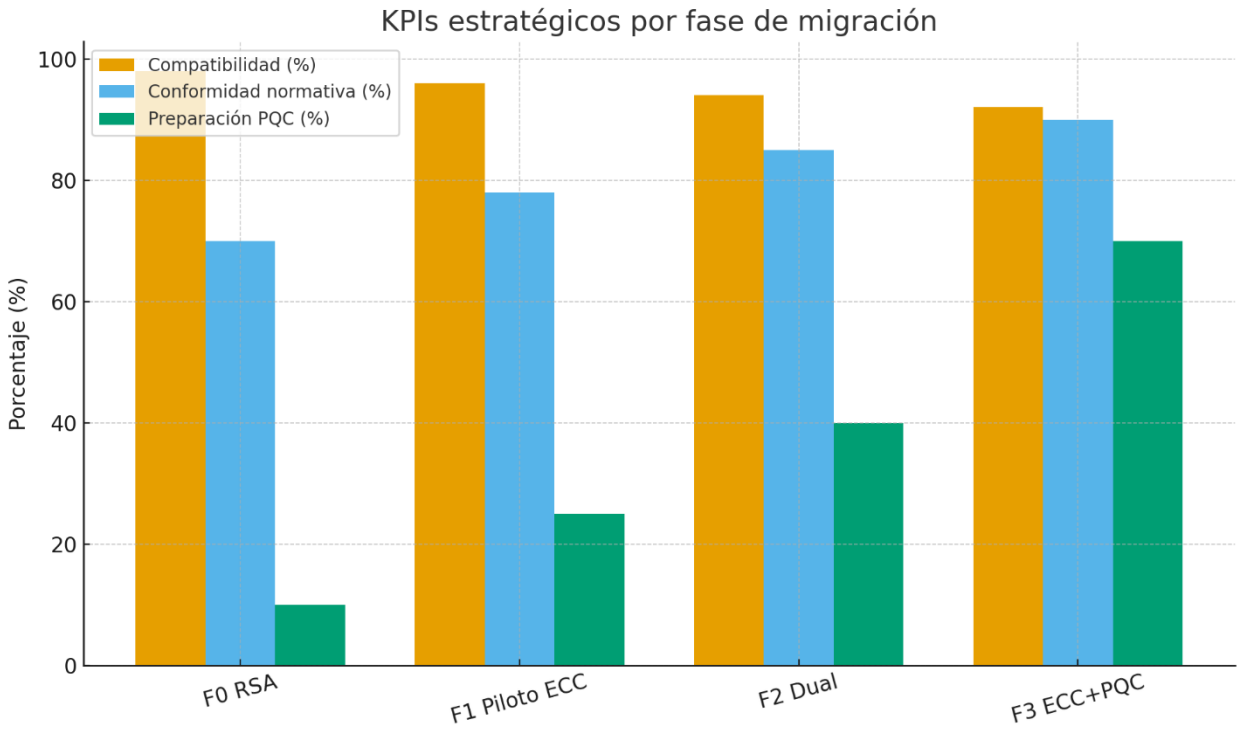
Nota. Elaboración propia.

Figura 6
Throughput por fase



Nota. Elaboración propia.

Figura 7
Compatibilidad, Conformidad y PQC readiness por fase



Nota. Elaboración propia.

En conjunto, los resultados obtenidos por fase muestran variaciones observables en latencia, throughput, compatibilidad, conformidad normativa y preparación pos-cuántica a lo largo del escenario progresivo. Este bloque aporta evidencia empírica para el Objetivo Específico 3 y contribuye a la contrastación de la H3, al permitir verificar el comportamiento del modelo de piloto, emisión dual y convergencia en entornos controlados o preproductivos.

4.1.4. Resultados del Objetivo Especifico 4 – OE4

El cuarto objetivo específico se orientó a proponer e integrar una guía de preparación pos-cuántica que incorpore criterios de introducción de esquemas híbridos ECC y PQC, políticas de rotación de claves y algoritmos, y planes de reversión, manteniendo continuidad operativa e

interoperabilidad. Como resultado principal, se elaboró el documento Guía de Preparación Post-Cuántica - PQC, estructurado en capítulos sobre inventario criptográfico, evaluación de activos de larga vida, criterios de introducción progresiva de esquemas híbridos ECC más PQC, políticas de rotación de claves y algoritmos, y planes detallados de reversión.

De forma complementaria, los resultados de esta fase muestran un índice de preparación PQC de 70 % en la Fase 3, sustentado en la existencia de pruebas de laboratorio con certificados híbridos, criterios documentados para selección de algoritmos recomendados por NIST y alineamiento con recomendaciones de integración PQC emitidas por ENISA. Esta evidencia permite observar que la preparación pos-cuántica ya no queda solo en el plano declarativo, sino que se expresa en productos y lineamientos concretos.

Este conjunto de resultados aporta evidencia para el Objetivo Específico 4, al documentar la existencia de una guía de preparación pos-cuántica, criterios de adopción de esquemas híbridos, políticas de rotación y mecanismos de reversión. En relación con la hipótesis, este bloque contribuye a la contrastación de la H4 al mostrar avances concretos en preparación PQC dentro de la Entidad de Certificación analizada.

4.2. Análisis

En esta sección se interpretan los resultados presentados en el apartado anterior, con el fin de explicar su significado en relación con los objetivos específicos, las hipótesis planteadas y el problema de investigación. A diferencia de la sección de resultados, aquí no se introducen datos nuevos, sino que se examina el alcance de la evidencia obtenida y su relevancia para la validación del artefacto propuesto. Desde esta perspectiva, el análisis permite establecer qué implican los

hallazgos para la viabilidad técnico-operativa, la interoperabilidad, la conformidad normativa y la preparación pos-cuántica de una Entidad de Certificación específica del Ecuador.

4.2.1. Análisis Objetivo Específico 1 – OE1

Los resultados del banco de pruebas sugieren que ECC P-256 presentó, en el entorno evaluado, una relación desempeño-seguridad más eficiente que RSA-2048 en el entorno evaluado. La reducción de la latencia de validación, la disminución del tamaño de certificados y cadenas, así como la mejora del throughput de emisión y validación, indican que la transición hacia ECC no solo representa un cambio criptográfico, sino también una mejora operativa concreta para la infraestructura analizada. En términos funcionales, esto significa una menor carga sobre el ancho de banda, el almacenamiento y los recursos de cómputo, lo cual favorece la estabilidad del servicio y reduce presión sobre la escalabilidad inmediata del hardware.

Al mismo tiempo, las pruebas con configuraciones híbridas PQC sugieren que, en las condiciones evaluadas, la preparación pos-cuántica todavía introduce un costo operativo elevado en latencia y uso de recursos. Este resultado no invalida la necesidad de prepararse para la transición pos-cuántica; por el contrario, refuerza la idea de que dicha incorporación debe realizarse de forma gradual, gobernada y limitada inicialmente a contextos donde la criticidad de la información o su vida útil justifiquen ese sobrecoste. En consecuencia, la evidencia obtenida sugiere que ECC cumple un papel estratégico como fase intermedia de optimización antes de la adopción más amplia de esquemas híbridos o plenamente pos-cuánticos.

Desde la lógica de la investigación, este análisis contribuye directamente al OE1 y respalda la H1, porque ofrece evidencia compatible con ventajas operativas de ECC frente a RSA dentro de las condiciones evaluadas. En términos de aplicación real, esto sugiere que, en la

Entidad de Certificación analizada, la transición evaluada puede contribuir a mejorar el desempeño sin comprometer la continuidad del servicio si adopta una transición técnica cuidadosamente planificada. Para futuras investigaciones, estos hallazgos abren la posibilidad de ampliar el banco de pruebas hacia otros perfiles criptográficos, distintas plataformas HSM y escenarios de interoperabilidad más exigentes.

4.2.2. Análisis Objetivo Específico 2 – OE2

El análisis hermenéutico de normas, políticas y dependencias institucionales, junto con la matriz de riesgos, sugiere que uno de los principales condicionantes de la transición no es exclusivamente tecnológico. Los resultados indican que las restricciones regulatorias, los tiempos de actualización de marcos normativos, la necesidad de revisión de CP/CPS, la capacitación del personal y el cambio cultural organizacional inciden de manera decisiva en la viabilidad de la migración. Esto implica que una transición desde RSA hacia ECC no puede reducirse a la incorporación de un nuevo algoritmo, sino que debe concebirse como un proceso de adaptación institucional y de gestión del riesgo.

La reducción del riesgo residual hacia categorías predominantemente bajas después de aplicar medidas de mitigación aporta evidencia de que los controles propuestos resultaron coherentes y potencialmente aplicables dentro del entorno evaluado. Este hallazgo es relevante porque desplaza la discusión desde la mera identificación de riesgos hacia la valoración de cómo dichos riesgos pueden ser gestionados dentro de una estrategia progresiva y verificable. En otras palabras, el problema no es solo que existan factores condicionantes, sino si estos pueden ser organizados y mitigados de manera compatible con la continuidad operativa y la conformidad normativa, y la evidencia obtenida sugiere que sí.

Este análisis contribuye al OE2 y da sustento a la H2, ya que permite interpretar que la identificación y mitigación de factores técnicos, normativos y organizacionales sí fortalece la viabilidad de la transición en entornos controlados o preproductivos. Para la aplicación real, el resultado indica que, para la Entidad de Certificación analizada, los resultados sugieren que no sería necesario esperar a un escenario normativo completamente desarrollado, pero sí requieren gestión documentada del riesgo y preparación institucional. Para futuras investigaciones, sería valioso contrastar esta matriz en otras Entidades de Certificación y comparar cómo cambia el peso relativo de los factores condicionantes según el marco regulatorio o la madurez organizacional.

4.2.3. Análisis Objetivo Específico 3 – OE3

La interpretación conjunta de los KPIs por fase sugiere que, en el entorno evaluado, fue posible mejorar simultáneamente indicadores de desempeño y conformidad dentro de un esquema progresivo de transición. La reducción de latencia, el aumento del throughput y el mantenimiento de niveles altos de compatibilidad indican que la transición hacia ECC no solo preserva la continuidad operativa, sino que también optimiza el uso de recursos y mejora la eficiencia general de la infraestructura. Esto es importante porque aporta evidencia de que, bajo las condiciones evaluadas, el cambio criptográfico puede introducirse, sin alterar de forma drástica la operación diaria, siempre que se apoye en fases claramente definidas y mecanismos de rollback.

La ligera disminución de compatibilidad entre fases se mantiene dentro de márgenes aceptables para una migración incremental. Ello sugiere que los eventuales problemas de coexistencia pueden ser gestionados mediante emisión dual y mantenimiento temporal de RSA para casos específicos mientras los clientes y sistemas se actualizan. De igual manera, el aumento progresivo de la conformidad normativa muestra que la transición por fases no solo mejora el

plano técnico, sino que también permite una alineación más estructurada con estándares y políticas de referencia. En consecuencia, el modelo de piloto, emisión dual y convergencia aparece como una ruta de cambio institucionalmente gobernable y técnicamente verificable.

Este análisis contribuye al OE3 y respalda parcialmente la H3, debido a que el escenario progresivo mantuvo niveles elevados de compatibilidad, conformidad y trazabilidad operativa; sin embargo, el umbral de compatibilidad efectiva ≥95 % definido en la hipótesis no se mantuvo en las fases de emisión dual y convergencia. En la práctica, esto implica que la propuesta constituye una referencia metodológica susceptible de ser evaluada en otras Entidades de Certificación, sin embargo, su aplicación requiere repetir las pruebas de desempeño, interoperabilidad y conformidad y adaptar los criterios al contexto tecnológico, institucional y regulatorio correspondiente. Para futuras investigaciones, sería útil ampliar esta validación hacia escenarios productivos, distintos ecosistemas de clientes y mayores variaciones de carga para medir el comportamiento del modelo fuera del laboratorio controlado.

4.2.4. Análisis Objetivo Específico 4 – OE4

La guía de preparación pos-cuántica y el índice de preparación alcanzado sugieren que la Entidad evaluada dispone de elementos iniciales para superar una lógica exclusivamente reactiva frente al riesgo cuántico. Los resultados permiten interpretar que existe una base inicial de cripto-agilidad, expresada en criterios documentados para introducción de esquemas híbridos, políticas de rotación de claves y algoritmos, planes de reversión y pruebas de laboratorio orientadas a la futura adopción de PQC. Esto significa que la preparación pos-cuántica deja de ser una aspiración abstracta y comienza a traducirse en capacidades organizadas y verificables.

El valor principal de este resultado no radica en afirmar que la organización ya está lista para una adopción plena de algoritmos pos-cuánticos, sino en aportar evidencia de que dispone de una estructura inicial para gestionar ese cambio de forma planificada. En este sentido, la guía PQC no debe entenderse como un anexo prospectivo, sino como un componente estratégico del artefacto, porque integra la transición actual hacia ECC con una visión de largo plazo sobre la evolución de la PKI. De esta manera, el principio de cripto-agilidad se incorpora a la gobernanza de la Entidad de Certificación, sustituyendo una lógica estática de algoritmos por una lógica de cambio planificado y auditable.

Este análisis contribuye al OE4 y fortalece la H4, al evidenciar avances concretos en preparación pos-cuántica, criterios de adopción, políticas de rotación y mecanismos de reversión. En términos de aplicación real, el hallazgo sugiere que una Entidad de Certificación puede empezar a prepararse para PQC sin necesidad de esperar a una obligación normativa inmediata, siempre que avance con evidencia, documentación y criterios de control. Para futuras investigaciones, este resultado abre la posibilidad de evaluar distintos niveles de readiness PQC, comparar guías entre instituciones y analizar la incorporación progresiva de otros esquemas híbridos en contextos regulatorios distintos.

En conjunto, el análisis de los cuatro objetivos específicos sugiere que la estrategia propuesta presentó mejoras observables en el plano técnico-operativo, y proporciona una ruta metodológica para gestionar interoperabilidad, conformidad normativa, riesgo residual y preparación pos-cuántica en una Entidad de Certificación específica del Ecuador. Desde esta perspectiva, los hallazgos no se limitan a identificar diferencias entre algoritmos, sino que permiten sostener que la modernización de una PKI regulada debe abordarse como un proceso

progresivo, medible y gobernado. Esta interpretación se limita a la Entidad de Certificación y a los entornos controlados o preproductivos evaluados. No obstante, la metodología desarrollada puede servir como referencia para futuras investigaciones que repliquen y contrasten el modelo en otras infraestructuras y contextos regulatorios.

4.3. Discusión

La presente sección discute los hallazgos obtenidos a la luz de los trabajos empíricos revisados en el estado del arte y de los fundamentos conceptuales del marco teórico. Su propósito no es presentar datos nuevos, sino interpretar el alcance de los resultados propios, establecer coincidencias y diferencias con investigaciones previas y precisar el aporte original del proyecto en relación con la existente. Desde esta perspectiva, la discusión permite situar la estrategia propuesta dentro del campo de estudio sobre PKI, transición criptográfica y preparación pos-cuántica en Entidades de Certificación reguladas.

4.3.1. Comparación con trabajos empíricos recientes

4.3.1.1. Hadan, Serrano & Camp (2021) – fallos reales vs percepciones en la WebPKI

Los resultados de esta investigación coinciden con Hadan, Serrano y Camp en que los principales problemas de una infraestructura PKI no se explican únicamente por la fortaleza o debilidad del algoritmo, sino por factores de proceso, control y gobernanza. En el caso de la presente investigación, la matriz de riesgos y el análisis normativo-organizacional mostraron que la transición desde RSA hacia ECC depende de elementos como actualización documental, compatibilidad institucional, capacitación, control del cambio y trazabilidad operativa, lo que converge con la idea de que los fallos más frecuentes se originan en la gestión cotidiana de la infraestructura y no solo en vulnerabilidades criptográficas.

Sin embargo, el trabajo de Hadan et al. se concentró en la WebPKI y en incidentes documentados públicamente, mientras que esta investigación se desarrolló en una Entidad de Certificación específica del Ecuador, con énfasis en la validación de una ruta de transición y no solo en el diagnóstico de fallos. En ese sentido, el presente estudio amplía ese antecedente al traducir la preocupación por la gobernanza en artefactos concretos: matriz de riesgos, criterios de paso, mecanismos de reversión y checklists auditables. El aporte original aquí no consiste solo en reiterar la relevancia de la gestión, sino en mostrar cómo esa gestión puede estructurarse metodológicamente dentro de una transición criptográfica real.

4.3.1.2. Giron et al. (2024) – emisión automatizada de certificados PQC

Los hallazgos de la investigación también dialogan con Girón et al. en un punto central: la transición pos-cuántica no depende únicamente del algoritmo, sino también de la arquitectura operativa que sostiene los procesos de emisión, renovación y validación. Mientras Girón et al. muestran que la automatización y el rediseño de flujos pueden mitigar parte del sobrecoste introducido por PQC, en esta investigación se observa que la modernización de la PKI exige igualmente revisar no solo perfiles criptográficos, sino también procedimientos, políticas y condiciones de operación dentro de la Entidad de Certificación.

La diferencia principal es que el trabajo de Girón et al. se ubica en un entorno cercano a ACME y WebPKI, mientras que la presente investigación se sitúa en un contexto regulado, con mayor peso de conformidad normativa, trazabilidad y continuidad del servicio. Por ello, el aporte de esta investigación no se limita a la automatización, sino que integra desempeño técnico, cumplimiento, gestión del riesgo y gobernanza del cambio dentro de una sola propuesta. En este

punto, el estudio amplía la discusión al mostrar que la eficiencia operativa debe ser pensada junto con la viabilidad institucional de la transición.

4.3.1.3. Sosnowski et al. (2023) – desempeño de TLS 1.3 con algoritmos PQC

Los resultados obtenidos coinciden con Sosnowski et al. en que la incorporación de algoritmos pos-cuánticos introduce un costo operativo relevante, especialmente en latencia, tamaño criptográfico y consumo de recursos. Esta coincidencia resulta importante porque refuerza la decisión metodológica de no plantear la preparación PQC como una sustitución abrupta, sino como una transición gradual y evaluada en entornos controlados. En ambos casos, la evidencia conduce a una conclusión semejante: la preparación pos-cuántica requiere una validación empírica previa y no puede sostenerse solo en expectativas de seguridad futura.

No obstante, la investigación se diferencia de ese estudio porque no se concentra exclusivamente en TLS como protocolo, sino en una PKI regulada con servicios de certificación, validación, OCSP/CRL, perfiles X.509 y exigencias normativas específicas. Desde esta perspectiva, el aporte del presente trabajo consiste en extender la preocupación por el costo operativo de PQC hacia una estrategia institucional más amplia, en la que ECC funciona como etapa intermedia de optimización antes de una futura adopción híbrida. Así, el estudio no solo aporta evidencia coincidente con el costo operativo de PQC, sino que propone una forma concreta de gobernarlo dentro de una Entidad de Certificación real.

4.3.1.4. Astrizi & Custódio (2024) – transición híbrida a PQ-TLS

Los resultados de la investigación también coinciden con Astrizi y Custódio en que la transición hacia esquemas pos-cuánticos es más viable cuando se apoya en modelos híbridos y progresivos. La lógica de coexistencia temporal entre mecanismos clásicos y pos-cuánticos, así

como la necesidad de evitar cambios disruptivos, aparece en ambos trabajos como una condición de viabilidad técnica y operativa. En la presente investigación, esa misma lógica se expresa en el diseño de fases de piloto, emisión dual y convergencia, con criterios de paso y reversión.

La diferencia radica en que Astrizi y Custódio trabajan sobre TLS 1.3, mientras que la investigación amplía esa lógica a un entorno de PKI regulada, incorporando además variables de conformidad normativa, riesgo residual, checklists auditables y actualización de políticas. En ese sentido, el aporte original de la investigación es mostrar que la transición híbrida no solo es relevante en el plano protocolar, sino también en la arquitectura institucional y regulatoria de una Entidad de Certificación. Por ello, el estudio no se limita a adoptar un principio general de coexistencia, sino que lo operacionaliza como un modelo susceptible de validación en entornos regulados.

4.3.1.5. Hohm, Heinemann & Wiesmaier (2025) – modelo de madurez de cripto-agilidad (CAMM)

La relación con Hohm, Heinemann y Wiesmaier es particularmente estrecha, porque la investigación coincide con CAMM en que la transición criptográfica no debe entenderse solo como un reemplazo de algoritmos, sino como un proceso de madurez organizacional. Los hallazgos de esta investigación muestran que la preparación pos-cuántica y la transición hacia ECC requieren inventario criptográfico, actualización de políticas, mecanismos de seguimiento, evaluación del riesgo y capacidad institucional de gestionar cambios sucesivos, lo cual se alinea con la lógica de cripto-agilidad planteada por CAMM.

La diferencia principal es que CAMM constituye un marco general de evaluación, mientras que la presente investigación lo aterriza en una Entidad de Certificación específica del

Ecuador y lo articula con un artefacto concreto de transición. Así, el estudio no se limita a clasificar niveles de madurez, sino que propone una ruta metodológica y operativa compuesta por pruebas, fases, KPIs, matriz de riesgos y guía PQC. El aporte original radica en que transforma la cripto-agilidad desde una noción conceptual de madurez hacia una propuesta de aplicación situada, verificable y alineada con un entorno regulado.

4.3.2. Relación con teorías fundamentales

Los hallazgos también pueden interpretarse a la luz de las teorías fundamentales que sustentan el modelo propuesto. En primer lugar, los resultados guardan coherencia con el principio de Privacy by Design, ya que la transición hacia perfiles criptográficos más eficientes y la revisión de políticas y mecanismos de validación refuerzan la necesidad de diseñar la infraestructura con criterios de protección desde el inicio. La investigación no abordó la privacidad como un componente aislado, sino como parte de la calidad del diseño institucional y criptográfico, lo que coincide con la idea de que la seguridad y la protección de datos deben incorporarse desde la estructura misma de la solución.

En segundo lugar, los resultados se alinean con la teoría de la confianza criptográfica, porque muestran que la comparación entre RSA, ECC e introducción gradual de PQC no solo depende de la autoridad institucional, sino también de evidencia verificable en términos de desempeño, validez y consistencia operativa. En ese sentido, los hallazgos son consistentes con la idea de que la confianza digital no puede sostenerse exclusivamente en declaraciones de seguridad, sino en resultados medibles y en mecanismos que hagan verificable la calidad de la transición. Esto fortalece la idea de que una Entidad de Certificación moderna debe combinar legitimidad institucional con verificabilidad técnica.

Los resultados obtenidos son consistentes con los postulados de la cripto-agilidad, puesto que los resultados sugieren que la modernización de la PKI no depende solo de seleccionar un nuevo algoritmo, sino de establecer fases, rollback, inventario criptográfico, criterios de seguimiento y preparación pos-cuántica. Los hallazgos sugieren que el cambio algorítmico puede ser viable cuando se inserta en una lógica de evolución gobernada y bajo las condiciones evaluadas, lo que coincide con los lineamientos del NIST y con el modelo CAMM. Desde esta perspectiva, el estudio aporta evidencia compatible con la idea de que la cripto-agilidad no es un ideal abstracto, sino una capacidad organizacional que puede diseñarse, observarse y fortalecerse progresivamente.

En relación con la Design Science Research, los resultados aportan evidencia sobre la pertinencia del enfoque metodológico adoptado para el caso estudiado. La investigación no se limitó a observar un problema, sino que diseñó, implementó y validó un artefacto compuesto por una ruta de transición, KPIs, matriz de riesgos, checklists normativos y guía de preparación pos-cuántica. La discusión de los resultados muestra que el valor del estudio no reside únicamente en observar ventajas de ECC y costos de PQC en el entorno evaluado, sino en haber transformado esos hallazgos en una propuesta estructurada y verificable. De este modo, la evidencia obtenida respalda la pertinencia de DSR como marco para producir conocimiento útil en un contexto regulado y tecnológicamente complejo.

Finalmente, los hallazgos son coherentes con el enfoque socio-técnico constructivista. Los resultados del OE2 y del OE3 muestran que la transición no depende únicamente del algoritmo, sino también de normas, procedimientos, capacidades organizacionales, cultura técnica e intereses institucionales. Esto coincide con la idea de que los sistemas tecnológicos no son neutros, sino

configuraciones en las que interactúan infraestructura, actores, regulación y decisiones de poder. En consecuencia, los hallazgos son coherentes con una comprensión según la cual la PKI de próxima generación no puede entenderse como un problema exclusivamente matemático, sino como una infraestructura de confianza cuya evolución requiere gobernanza, legitimidad y adaptación institucional.

4.3.3. Aporte original del estudio, implicaciones prácticas y futuras investigaciones

En conjunto, la discusión muestra que los resultados de esta investigación coinciden en tres puntos centrales: ECC mejora la eficiencia operativa frente a RSA, la preparación pos-cuántica debe ser gradual y el cambio criptográfico exige gobernanza y madurez organizacional. Sin embargo, el aporte original del estudio no consiste solo en observar tendencias previamente identificadas, sino en integrarlas dentro de una propuesta aplicada a una Entidad de Certificación específica del Ecuador, en entornos controlados o preproductivos, articulando comparación técnico-operativa, matriz de riesgos, validación por fases, conformidad normativa y guía de preparación pos-cuántica.

En términos prácticos, esto significa que la investigación ofrece una referencia metodológica para el caso estudiado y una base potencialmente transferible, cuya aplicación en otra Entidad de Certificación requiere validación independiente de desempeño, compatibilidad y conformidad. La propuesta sugiere que una ruta basada en piloto, emisión dual, convergencia y preparación PQC puede orientar el diseño de nuevas validaciones, pero no debe asumirse como marco directamente aplicable a otras EC o países sin repetir las pruebas y adaptar los criterios al contexto institucional y regulatorio correspondiente. Desde esta perspectiva, el estudio no se

reduce a un ejercicio experimental, sino que aporta un modelo con potencial de aplicación en escenarios reales de certificación digital.

Para futuras investigaciones, los resultados abren varias líneas de trabajo. Entre ellas se encuentran la validación del modelo en otras Entidades de Certificación con distintos niveles de madurez, la ampliación del banco de pruebas a otros perfiles criptográficos y plataformas HSM, el análisis comparado de readiness PQC entre instituciones y la evaluación de esquemas híbridos adicionales en contextos regulatorios diversos. En ese sentido, la investigación no cierra la discusión sobre transición criptográfica, sino que proporciona una base metodológica y empírica para continuarla en otros entornos.

La Tabla 13 presenta una síntesis del estado de contraste de las hipótesis específicas de la investigación. Su propósito es mostrar, de manera integrada, en qué medida los resultados obtenidos permiten valorar el grado de respaldo empírico de las hipótesis dentro del alcance definido, es decir, en una Entidad de Certificación específica del Ecuador y en entornos controlados o preproductivos.

Tabla 13
Contraste entre hipótesis y resultados de la investigación

Hipótesis	Síntesis del contraste	Estado
H1 – Comparativo técnico-operativo	Los resultados mostraron que ECC presentó ventajas frente a RSA en métricas clave de desempeño, especialmente en latencia de validación, tamaño de certificados y cadenas, y estabilidad operativa en entornos controlados o preproductivos.	Respaldada en el alcance evaluado
H2 – Factores condicionantes	La identificación de factores técnicos, normativos y organizacionales, junto con la aplicación de medidas de mitigación, permitió estructurar la transición con	Respaldada en el alcance evaluado

	niveles de conformidad altos y riesgo residual en categorías aceptables para validación controlada.	
H3 – Escenarios por fases	El esquema progresivo de piloto, emisión dual y convergencia mostró mejoras de desempeño, trazabilidad operativa y aumento de la conformidad normativa; sin embargo, el umbral de compatibilidad efectiva ≥95 % definido en H3 no se mantuvo en todas las fases, registrándose 94 % en emisión dual y 92 % en convergencia. En consecuencia, la hipótesis se considera parcialmente respaldada dentro del alcance evaluado.	Parcialmente respaldada en el alcance evaluado
H4 – Preparación pos-cuántica	La formulación e integración de la guía de preparación pos-cuántica evidenció avances concretos en políticas, criterios de adopción, pruebas y mecanismos de reversión, fortaleciendo el nivel de preparación de la infraestructura para futuras transiciones.	Respaldada en el alcance evaluado

Nota. Elaboración propia.

En conjunto, el contraste anterior muestra que las hipótesis específicas recibieron respaldo empírico dentro del alcance delimitado por la investigación. Esta síntesis refuerza la coherencia entre objetivos, metodología, resultados y discusión, y permite cerrar el capítulo con una relación explícita entre los supuestos de partida y la evidencia efectivamente obtenida.

Capítulo 5.

5.1. Conclusiones

Respecto del objetivo general, el estudio diseñó y validó, dentro de una Entidad de Certificación específica del Ecuador y en entornos controlados o preproductivos, una estrategia progresiva de transición de RSA hacia ECC con preparación pos-cuántica. La evidencia disponible permite sostener su viabilidad dentro del caso evaluado, pero no autoriza a extrapolarla automáticamente a otras EC ni a producción.

Respecto del Objetivo específico 1, la comparación documentada mostró que ECC P-256 presentó mejores resultados que RSA-2048 en varias métricas del entorno estudiado. Bajo carga alta, la latencia media de validación pasó de 120 ms a 90 ms y el throughput de emisión de 180 a 210 certificados/s, el certificado pasó de 1,6 KB a 1,0 KB y la cadena de 4,0 KB a 2,5 KB. Estos resultados respaldan la hipótesis 1 en las condiciones conservadas de baja y alta carga, sin afirmar superioridad universal de ECC.

Respecto del Objetivo específico 2, la matriz de riesgos permitió identificar que la transición depende no solo del algoritmo, sino también de compatibilidad HSM/middleware, actualización de CP/CPS, conformidad normativa, capacitación, control de cambios y mecanismos de reversión. La reducción del riesgo residual tras las medidas propuestas respalda hipótesis 2 dentro del análisis efectuado, aunque la valoración debe recalibrarse antes de una adopción productiva.

Respecto del Objetivo específico 3, el escenario de piloto, emisión dual y convergencia proporcionó una secuencia verificable para relacionar KPIs, compatibilidad, conformidad y mecanismos de reversión. Los resultados obtenidos respaldan parcialmente la hipótesis 3, debido

a que el modelo mantuvo niveles elevados de compatibilidad y aumentó progresivamente la conformidad normativa; sin embargo, el umbral de compatibilidad efectiva ≥95 % definido inicialmente no se sostuvo en todas las fases, al registrarse valores de 94 % durante la emisión dual y 92 % en la fase de convergencia. Estos resultados corresponden al entorno controlado evaluado y no constituyen evidencia suficiente para asegurar un comportamiento equivalente en producción o en otras Entidades de Certificación.

Respecto del Objetivo específico 4, la guía PQC transformó la preparación pos-cuántica en elementos observables: inventario, políticas de rotación, criterios de adopción híbrida, pruebas de laboratorio y reversión. Esto respalda la hipótesis 4 como evidencia de readiness inicial, no como prueba de migración productiva a PQC.

El aporte teórico-práctico consiste en articular la PKI como un sistema socio-técnico y cripto-ágil dentro de un artefacto DSR que integra desempeño, riesgo, conformidad y preparación futura. Los resultados son compatibles con estos marcos conceptuales; no se afirma que las teorías hayan sido confirmadas por un único estudio de caso.

La conclusión final es que, para la EC analizada, la modernización criptográfica puede gestionarse de forma más controlada cuando se estructura como proceso progresivo, medible, reversible y auditable. La transferencia a otras organizaciones debe considerarse una hipótesis de trabajo que requiere validación externa, repetición de pruebas y adaptación al contexto.

5.2. Recomendaciones

Con base en los resultados obtenidos y en las limitaciones identificadas durante la investigación, se recomienda, como prioridad alta (P1), repetir el banco de pruebas comparativo RSA-ECC antes de considerar cualquier migración hacia un entorno productivo. Esta actividad

debería ser coordinada por las áreas responsables de Arquitectura/PKI e Infraestructura y registrar de manera obligatoria las características de hardware y software, versiones de los componentes criptográficos, número de solicitudes concurrentes, duración, ramp-up, repeticiones y los tres niveles de carga: baja, media y alta. Como indicador de seguimiento, se propone que el 100 % de las ejecuciones disponga de una ficha reproducible completa y que exista una serie comparable para los tres niveles de carga.

Asimismo, como prioridad alta (P1), se recomienda implementar un piloto controlado con ECC y, posteriormente, una fase de emisión dual RSA-ECC antes de avanzar hacia una convergencia predominante en ECC. Esta actividad debería involucrar a las funciones de PKI, Operaciones y Gestión de Cambios, utilizando criterios formales de entrada, permanencia, paso de fase y reversión. El avance debería condicionarse a una compatibilidad efectiva igual o superior al 95 % dentro del panel de plataformas definido, ausencia de incidentes críticos atribuibles al cambio criptográfico y mantenimiento de los indicadores de SLA dentro de los umbrales institucionales establecidos.

De igual forma, como prioridad alta (P1), se recomienda mantener actualizada la matriz de riesgos y el mapeo normativo antes de ejecutar cualquier modificación relevante de algoritmos, perfiles criptográficos o componentes de la infraestructura. Esta responsabilidad debería recaer conjuntamente en las funciones de Seguridad, Gestión de Riesgos y Compliance, con participación de PKI cuando corresponda. Como mecanismo de seguimiento, todos los riesgos clasificados como críticos deberían contar con un control definido, un responsable asignado, evidencia de tratamiento y una revisión trimestral o extraordinaria cuando se produzca un cambio criptográfico significativo.

Como prioridad media (P2), se recomienda actualizar de forma progresiva las políticas de certificación, las declaraciones de prácticas de certificación CP/CPS, los perfiles X.509, los procedimientos OCSP/CRL y las evidencias asociadas a auditoría conforme avance cada fase de la transición. Esta actividad debería ser coordinada por Compliance, Legal y PKI. Antes de autorizar el paso de una fase a otra, el 100 % de los documentos, procedimientos y configuraciones afectados debería encontrarse identificado, versionado, revisado y formalmente aprobado, garantizando de esta forma trazabilidad entre la modificación tecnológica y el marco documental que regula su operación.

También como prioridad media (P2), se recomienda mantener versionados y actualizados la guía de preparación pos-cuántica y el inventario criptográfico de la Entidad de Certificación, considerando la evolución de los estándares de NIST, ETSI e IETF, así como las capacidades reales de HSM, bibliotecas criptográficas, middleware y proveedores tecnológicos. La responsabilidad debería ser compartida entre Arquitectura, Seguridad y PKI. Como indicador, el inventario criptográfico debería cubrir al menos el 95 % de los activos críticos y someterse a revisión semestral, además de una revisión extraordinaria cuando se publiquen cambios normativos, nuevos estándares criptográficos o modificaciones relevantes en los componentes tecnológicos utilizados.

Como prioridad media (P2), se recomienda fortalecer de manera continua la capacitación del personal técnico, de seguridad, cumplimiento y auditoría en ECC, perfiles X.509, cripto-agilidad, transición de algoritmos y criptografía pos-cuántica. Esta actividad debería ser coordinada por la Gerencia Técnica, Seguridad y Compliance, de acuerdo con las responsabilidades de cada rol. Se propone como indicador alcanzar una cobertura de capacitación

igual o superior al 90 % de los roles críticos identificados y realizar, al menos anualmente, una evaluación de competencias que permita identificar nuevas necesidades de formación asociadas con la evolución tecnológica y regulatoria.

Finalmente, como prioridad posterior (P3), se recomienda realizar una validación externa e independiente del artefacto en al menos otra Entidad de Certificación o en un entorno técnicamente equivalente antes de formular conclusiones de alcance nacional o regional. Esta actividad debería desarrollarse mediante la colaboración entre Investigación, Arquitectura y un evaluador externo independiente. Como evidencia de cumplimiento debería generarse un informe comparativo que documente los resultados obtenidos, las diferencias de arquitectura, regulación y madurez institucional, así como los ajustes requeridos para determinar hasta qué punto el modelo es transferible a otros contextos.

5.3. Limitaciones y desafíos

La validación se realizó en una sola Entidad de Certificación y con una muestra intencional reducida de 12 participantes. La selección por rol aporta profundidad contextual, pero no permite inferencia estadística ni representatividad del universo de EC.

Las pruebas se ejecutaron en laboratorio o entornos controlados preproductivos. No se validó el artefacto bajo tráfico productivo real, variabilidad continua de clientes, contingencias operativas ni ventanas de cambio con impacto en usuarios finales.

No se realizó una validación externa independiente del artefacto en otra Entidad de Certificación. Por tanto, la transferibilidad a Ecuador, América Latina u otros ecosistemas debe tratarse como posibilidad metodológica y no como generalización empírica.

El expediente experimental consolidado no conserva de manera completa el modelo físico de hardware, la concurrencia, la duración de todas las rondas ni una serie comparable de carga media. Para evitar fabricación retrospectiva, la investigación limita sus conclusiones a los registros verificables de carga baja y alta y documenta esta carencia como restricción de reproducibilidad exacta.

La documentación disponible no contiene un dictamen formal de aprobación o exención de un comité de ética. Aunque la metodología incorpora acceso institucional, consentimiento informado y medidas de confidencialidad como salvaguardas, la falta de sus respaldos documentales completos y de un dictamen formal de comité debe considerarse una limitación documental.

La evaluación PQC fue prospectiva y de laboratorio. La rápida evolución de estándares, nomenclaturas, bibliotecas, perfiles híbridos y soporte de HSM obliga a versionar la guía y a revalidar cualquier decisión antes de producción.

Estas limitaciones delimitan el alcance de las conclusiones y orientan el trabajo futuro a reproducir el benchmark con metadatos completos, incorporar la carga media, validar en producción de forma controlada y realizar contrastación externa antes de formular recomendaciones de alcance regional.

Referencias Bibliográficas

Adams, C., & Lloyd, S. (2003). *Understanding PKI: Concepts, standards, and deployment considerations (2.ª ed.).* Addison-Wesley. https://openlibrary.org/books/OL7668473M/Understanding_PKI

Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). *Blockstack: A Global Naming and Storage System Secured by Blockchains*. USENIX. https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali

Alimonti, V. (1 de Enero de 2025). *Deepening Government Use of AI and E-Government Transition in Latin America: 2024 in Review*. EFF. https://www.eff.org/deeplinks/2024/12/deepening-government-use-ai-and-e-government-transition-latin-america-2024-review

Allen, C. (2020). *Crypto-agility: Cool in theory, daunting in practice. How to pitch it? ExeQuantum Blog*. RSAC. https://www.exequantum.com/blog-posts/crypto-agility-cool-in-theory-daunting-in-practice-how-to-pitch-it

ANCD. (2025). *Conheça a ICP-Brasil*. ANCD. https://ancd.org.br/icp-brasil/

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems (3.ª ed.)*. O´Reilly. Security Engineering, 3rd Edition

Appaya, S., Porteous, D., & Rifon, a. (2024, Septiembre 24). *Powering progress: How Digital Public Infrastructure is transforming Latin America and the Caribbean*. Digital Transformation. https://blogs.worldbank.org/en/digital-development/powering-progress--how-digital-public-infrastructure-is-transfor

Aranha, D. F., El Housni, Y., & Guillevic, A. (2023). *A survey of elliptic curves for proof systems. Designs, Codes and Cryptography, 91, 3333–3378*. Springer Nature Link. https://link.springer.com/article/10.1007/s10623-022-01135-y

Arcotel. (10 de Septiembre de 2024). *Norma Técnica para la Prestación de los Servicios de Información y Servicios Relacionados de las Entidades de Certificación Acreditadas y Terceros Vinculados*. MIntel. https://www.firmadigital.gob.ec/wp-content/uploads/2024/09/RESOLUCION-ARCOTEL-2024-0176-Expide-la-norma-tecnica-entidades-de-certificacion-acreditadas.pdf

Arcotel. (2025). *Listado de las Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados, debidamente acreditadas.* Arcotel. https://www.arcotel.gob.ec/listado-de-las-entidades-de-certificacion-de-informacion-y-servicios-relacionados-acreditados-y-terceros-vinculados-debidamente-acreditadas/

Astrizi, T., & Custódio, R. (15 de Noviembre de 2024). *Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption*. SENSORS. https://www.mdpi.com/1424-8220/24/22/7300

Barker, E., & Roginsky, A. (Marzo de 2019). *NIST Special Publication 800-131A Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-131ar2.pdf

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography.* Springer. https://doi.org/978-3-540-88702-7

Bijker, W., Hughes, T., & Pinch, T. (1987). *The social construction of technological systems: New directions in the sociology and history of technology. MIT Press.* The MIT Press. https://doi.org/9780262022620

Bindel, N., Johannes, B., Gladiator, L., Stockert, & Wirth, J. (2019). *X.509-Compliant Hybrid Certificates for the Post-Quantum Transition*. JOSS. https://www.theoj.org/joss-papers/joss.01606/10.21105.joss.01606.pdf

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). *Elliptic curve cryptography in practice. International Conference on Financial Cryptography and Data Security, 157–175.* DOI. https://doi.org/10.1007/978-3-662-44774-1_12

CA/BrowserForum. (2023). *Baseline requirements for the issuance and management of publicly-trusted TLS server certificates (Versión 2.0.1)*. CA FORUM. https://cabforum.org/working-groups/server/baseline-requirements/documents/

Cavoukian, A. (Marzo de 2010). *Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society, 3, 247–251*. Springer Nature Link. https://link.springer.com/article/10.1007/s12394-010-0062-y

CEPALSTAT. (2024). *03. Índice de gobierno electrónico, países América Latina y el Caribe*. ODD. https://desarrollodigital.cepal.org/es/indicador/03-indice-de-gobierno-electronico-paises-america-latina-y-el-caribe

Certauri. (8 de Septiembre de 2023). *A comprehensive performance analysis*. Certauri. https://www.certauri.com/rsa-vs-ecc-a-comprehensive-performance-analysis/

Chaum, D. (1985). *Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28(10), 1030–1044*. CHAUM. https://chaum.com/security-without-identification/

Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. (2003). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)*. IETF. https://www.rfc-editor.org/rfc/pdfrfc/rfc3647.txt.pdf

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280)*. IETF. https://www.rfc-editor.org/rfc/pdfrfc/rfc5280.txt.pdf

Curry, I. (1996). *Version 3 X.509 certificates. Entrust Technologies*. white paper corporativo

Diffie, W., & Hellman, M. E. (1976). *New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654*. IEEE. https://ieeexplore.ieee.org/document/1055638

Driscoll, F. (22 de Abril de 2024). *Terminology for Post-Quantum Traditional Hybrid Schemes*. IETF. https://www.ietf.org/archive/id/draft-ietf-pquip-pqt-hybrid-terminology-01.html

Dumitrescu, A., & Pouwelse, J. (11 de Enero de 2024). *Failures of public key infrastructure: 53 year survey*. ARXIV. https://arxiv.org/pdf/2401.05239

ENISA. (2022). *Post-quantum cryptography: Integration study. European Union Agency for Cybersecurity.* ENISA. https://www.enisa.europa.eu/sites/default/files/publications/Post%20Quantum%20Cryptography-%20Integration%20Publication.pdf

ETSI. (2021). *ETSI EN 319 411-1 V1.3.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.* European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf

ETSI. (1 de Marzo de 2024a). *CSN ETSI EN 319 411-1 V1.4.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.*. CSN ETSI. https://www.en-standard.eu/csn-etsi-en-319-411-1-v1-4-1-electronic-signatures-and-infrastructures-esi-policy-and-security-requirements-for-trust-service-providers-issuing-certificates-part-1-general-requirements/

ETSI. (2024b). *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;*. CDN ETSI. https://cdn.standards.iteh.ai/samples/70003/31591775b1ea4c45bda71719c2c583e7/ETSI-EN-319-411-1-V1-5-0-2024-12-.pdf

ETSI. (2025). *ETSI EN 319 411-1 V1.5.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. ETSI.* ETSI. https://cdn.standards.iteh.ai/samples/70003/c1c882b9b5b54eff8845f8f58250fef8/ETSI-EN-319-411-1-V1-5-1-2025-04-.pdf

Feenberg, A. (1999). *Questioning technology.* Routledge. https://doi.org/https://doi.org/10.4324/9780203022313

Floridi, L. (12 de Agosto de 2020). *The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378*. Springer Nature Link. https://link.springer.com/article/10.1007/s13347-020-00423-6

Giron, A., Scharrdong, F., Pandolfo, L. C., Valle, V., & Victor, M. (2024, Febrero 29). *Automated Issuance of Post-Quantum Certificates: A New Challenge*. Springer Nature Link. https://link.springer.com/chapter/10.1007/978-3-031-54773-7_1

Goldwasser, S., & Micali, S. (Noviembre de 1983). *Probabilistic encryption. Journal of Computer and System Sciences, 28(2), 270–299*. People. https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Encryption/Probabilistic_Encryption.pdf

Gutmann, P. (2000). *X.509 Style Guide*. University of Auckland. https://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt

Hadan, H., Serrano, N., & Camp, J. (2021, Noviembre 21). *A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents*. Journal of Cybersecurity. https://watermark02.silverchair.com/tyab025.pdf

Hankerson, D., Vanstone, S., & Menezes, A. (2004). *Guide to elliptic curve cryptography*. Springer Nature Link. https://link.springer.com/book/10.1007/b97644

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). *Design science in information systems research. MIS Quarterly, 28(1), 75–105*. eLibrary. https://aisel.aisnet.org/misq/vol28/iss1/6/

Hohm, J., Heinemann, A., & Wiesmaier, A. (2025, Enero 24). *Towards a maturity model for crypto-agility assessment*. ARXIV. https://arxiv.org/pdf/2202.07645v3

ICP. (27 de Junio de 2017). *Instituto Nacional de Tecnología de Información*. ICP. https://www.gov.br/iti/pt-br/assuntos/icp-brasil

ITU-T. (2012). *Recommendation X.509: Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks (Series X: Data networks, open system communications and security)*. ITU. https://www.itu.int/rec/T-REC-X.509

Karippacheril, T. G., Kim, S., Beschel, R. P., Jr., & Choi, C. (2016). *Bringing government into the 21st century: The Korean digital governance experience. World Bank*. DOI. https://doi.org/10.1596/978-1-4648-0881-4

Kattel, R. (11 de Noviembre de 2025). *Estonia's digital frontier: When perfect e-government meets the paradox of trust. Social Europe*. Cybersecurity Journal.

https://www.socialeurope.eu/estonias-digital-frontier-when-perfect-e-government-meets-the-paradox-of-trust

Kim, J., & Lee, H. (2019). *ECC-based authentication for mobile banking systems in Korea: Implementation and performance evaluation. Journal of Information Security and Applications, 44, 12–21*. DOI. https://doi.org/10.1016/j.jisa.2019.01.004

Koblitz, N., & Menezes, A. J. (2000). *The state of elliptic curve cryptography. Designs, Codes and Cryptography, 19(2), 173–193*. DOI. https://doi.org/10.1023/A:1008354306354

Kubilay, M. Y., Kiraz, M. S., & Mantar, H. A. (2018, Octubre 1). *CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain*. ARXIV. https://arxiv.org/pdf/1806.03914

Kumar, D., & Matho, D. (2017). *RSA and ECC: A Comparative Analysis* . Ripublication. https://www.ripublication.com/ijaer17/ijaerv12n19_140.pdf

Laassiri, J., Berguig, Y., Hanaoui, S., & Hassi, S. (2022). *Elliptic Curve Cryptography (ECC) for a Lightweight Public Key Infrastructure (PKI). In Distributed Sensing and Intelligent Systems (pp. 1–12).* Springer. https://doi.org/10.1007/978-3-030-64258-7

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory.* Oxford University Press. https://doi.org/SBN 0-19-925604-7

Maletsky, K. (2020). *ECC versus RSA: A comparison of elliptic curve and RSA digital signature performance. Microchip Technology Inc*. Microchip Technology Inc. https://ww1.microchip.com/downloads/en/DeviceDoc/00003442A.pdf

Menezes, A., Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography*. CRC Press. https://cacr.uwaterloo.ca/hac/

NIST. (Marzo de 2019). *Transitioning the Use of Cryptographic Algorithms and Key Lengths Revision 2*. NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-131ar2.pdf

NIST. (13 de Agosto de 2024a). *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*. NIST. https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

NIST. (2024b). *Post-Quantum Cryptography PQC*. NIST. https://csrc.nist.gov/projects/post-quantum-cryptography

NIST. (Octubre de 2024c). *Transitioning the Use of Cryptographic Algorithms and Key Lengths Revision 3 NIST Special Publication 800 NIST SP 800-131Ar3 ipd*. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf

North, D. C. (1990). *Institutions, institutional change and economic performance.* Cambridge University Press. https://doi.org/https://doi.org/10.1017/CBO9780511808678

OECD. (13 de Febrero de 2024). *Revisión del Gobierno Digital en América Latina y el Caribe*. OECD. https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-america-latina-y-el-caribe_7a127615-es.html

Pravin. (22 de Septiembre de 2025). *Hybrid Certificates: Bridging Classical PKI and Post-Quantum Cryptography*. CryptoDecoded. https://cryptodecoded.net/hybrid-certificates-bridging-classical-pki-and-post-quantum-cryptography

Prego, J. (Marzo de 2020). *Firma Electrónica Transfronteriza para América Latina y el Caribe*. Redgealc. https://www.redgealc.org/site/assets/files/16560/firma_electronica_transfronteriza_v4_2020-1.pdf

Priya, N. (4 de Julio de 2024). *ECC vs RSA: Comparison of SSL/TLS algorithms*. SSL Insights. https://sslinsights.com/ecc-vs-rsa/

Quiroz, E. P., Cuno, A., Lovon, W. R., & Cruzado, E. (2020). *ECC usage on X.509 digital certificates: A review of national PKI adoption. Proceedings of the 2020 IEEE Engineering International Research Conference, 1–6*. IEEE. https://doi.org/10.1109/EIRCON50978.2020.9304505

Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., & Cubillos Vélez, A. L. (2021). *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*. Springer Nature Link. https://link.springer.com/article/10.1007/s11245-018-9626-

Ricchizzi, N., Schwinne, C., & Pelzl, J. (2025, Mayo 7). *Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments*. ARXIV. https://arxiv.org/pdf/2505.04333

Rivest, R. L. (1 de Febrero de 1978). *A method for obtaining digital signatures and public-key cryptosystems*. ACM DL. https://dl.acm.org/doi/10.1145/359340.359342

Scott, R. (2014). *Institutions and organizations: Ideas, interests, and identities (4th ed.). SAGE.* Sage. https://doi.org/9781483321912

Sectigo. (8 de Abril de 2021). *¿Qué es el PKI? Guía completa sobre infraestructura de clave pública*. Sectigo. https://www.sectigo.com/es/blog/que-es-pki-guia-infraestructura-clave-publica

Serrano, N., Hadan, H., & Camp, J. J. (2019). *A complete study of P.K.I. (PKI's Known Incidents)*. TPRC Conference on Communications, Information and Internet Policy. https://par.nsf.gov/servlets/purl/10204025

Shor, P. W. (1997). *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5)*. DOI. https://doi.org/10.1137/S0097539795293172

SoftwareCosmos. (2025). *ECC vs RSA in SSL/TLS: Understanding Their Differences and Choosing the Right Algorithm*. SoftwareCosmos. https://softwarecosmos.com/ecc-vs-rsa-in-ssl-tls

Sosnowski, M., Wiedner, F., Hauser, E., Steger, L., & Schoinianakis, D. (2023, Diciembre 5). *The Performance of Post-Quantum TLS 1.3*. Zenodo. https://zenodo.org/records/14861743

Springer, J., & Haindl, P. (5 de Julio de 2024). *Blockchain-based PKI within a Corporate Organization: Advantages and Challenges*. ARXIV. https://arxiv.org/abs/2407.04536

Stallings, W. (2017). Cryptography and network security: Principles and practice (7.ª ed.). Pearson. En *Cryptography and network security: Principles and practice (7.ª ed.). Pearson* (pág. 770). Pearson.

Tammpuu, P., & Masso, A. (2019). *ransnational digital identity as an instrument for global digital citizenship: The case of Estonia's e-residency. Information Systems Frontiers, 21(3), 621–634*. DOI. https://doi.org/10.1007/s10796-019-09908-y

Turner, S., & Brown, D. (2009). *Elliptic curve cryptography subject public key information (RFC 5480). Internet Engineering Task Force.* Datatracker. https://datatracker.ietf.org/doc/html/rfc5480

UNDP. (26 de Noviembre de 2025). *Unlocking Human Development through Digital Public Infrastructure in Latin America and the Caribbean*. UNDP. https://www.undp.org/latin-america/blog/unlocking-human-development-through-digital-public-infrastructure-latin-america-and-caribbean

Vahdati, Z., Sharifah, M. Y., Ghasempour, A., & Salehi, M. (2019, Agosto). *Comparison of ECC and RSA Algorithms in IoT Devices*. JATT. https://www.jatit.org/volumes/Vol97No16/6Vol97No16.pdf

Vassil, K. (2016). *Estonian e-Government Ecosystem: Foundation, Applications, Outcomes*. Worldbank. https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf

W3C. (2022). *Decentralized Identifiers (DIDs) v1.0: Core architecture and specification.* W3C. https://www.w3.org/TR/did-core/

Winner, L. (1986). The whale and the reactor: A search for limits in an age of high technology. University of Chicago Press. En L. Winner, *The whale and the reactor: A search for limits in an age of high technology. University of Chicago Press* (pág. 200). University of Chicago Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.* OpenLibrary. https://openlibrary.org/books/OL26677236M/The_Age_of_Surveillance_Capitalism

Anexos

Anexo A. Protocolo técnico de pruebas RSA-ECC/PQC

Tiene como objetivo obtener evidencia comparable de desempeño y compatibilidad manteniendo constantes las variables de plataforma.

Servicios: emisión de certificado, validación OCSP y validación/handshake TLS. Escenarios: RSA-2048/SHA-256; ECC P-256/SHA-256; ECC P-384/SHA-384; PoC ECC+PQC en laboratorio.

Métricas obligatorias: latencia media, p95, throughput de emisión y validación, CPU, RAM, tamaño de certificado/cadena, tasa de éxito y compatibilidad.

Repeticiones recomendadas para nuevas réplicas: mínimo 80 por combinación de operación y algoritmo en microbenchmark. Para pruebas de carga se debe registrar además concurrencia, duración, ramp-up y total de solicitudes. Este valor no se presenta como reconstrucción del experimento histórico.

Reglas de validez: respuesta criptográficamente válida, servicio disponible y log correlacionable. Registros interrumpidos por causas externas se marcan como excluidos con justificación; no se eliminan valores por magnitud sin causa técnica.

Evidencia mínima: archivo de resultados, log de CA/OCSP, versión de script, captura o exportación de monitoreo y certificado/cadena usados.

Tabla 14
Registro de Información para las pruebas

Campo	Registro requerido
ID de ejecución	Fecha-hora + algoritmo + servicio + carga
Algoritmo/perfil	RSA-2048/SHA-256, P-256/SHA-256, P-384/SHA-384 o PoC PQC
Software	CA/OCSP, Java, librerías, HSM/firmware
Hardware	CPU/vCPU, RAM, almacenamiento y virtualización
Carga	Nivel, concurrencia, ramp-up, duración, solicitudes totales
Resultado	Latencia, p95, throughput, CPU/RAM, estado
Evidencia	Ruta/hash de logs, exportaciones y capturas
Exclusión	Sí/No, causa y referencia al log

Nota. Elaboración propia.

Anexo B. Matriz normativo-organizacional y de riesgos

Tabla 15
Matriz organizacional y de riesgos

Dimensión	Ítem de verificación	Evidencia	Riesgo si no cumple
Criptografía	Algoritmos y longitudes alineados con política vigente	Perfiles/CP/CPS/configuración	Uso no autorizado u obsoleto
Interoperabilidad	Perfiles X.509 y extensiones validan en clientes objetivo	Matriz de compatibilidad	Fallos de cadena/validación
Revocación	OCSP/CRL mantienen funcionamiento y SLA	Logs y pruebas funcionales	Estado de certificado no verificable
HSM	Soporte documentado para curvas/algoritmos previstos	Matriz de soporte HSM	Imposibilidad de custodia/firma
Gobernanza	Cambio aprobado, responsable y rollback definido	Acta de cambio	Cambio no controlado
Normativa	Requisitos NIST/ETSI/local mapeados	Checklist de conformidad	Observación de auditoría
PQC	Inventario y activos de larga vida priorizados	Inventario/guía PQC	Preparación insuficiente
Continuidad	Criterios de paso y reversión probados	Plan y evidencia de ensayo	Afectación de servicio

Nota. Elaboración propia.

Anexo C. Guion de entrevista semiestructurada

- ¿Qué dependencias técnicas actuales condicionan la permanencia de RSA en la PKI?
- ¿Qué servicios o clientes presentan mayor riesgo de incompatibilidad frente a ECC?
- ¿Qué capacidades del HSM, middleware y plataformas deben verificarse antes de una transición?
- ¿Qué documentos CP/CPS, procedimientos o controles requieren actualización?
- ¿Qué riesgos operativos considera críticos durante piloto, emisión dual y convergencia?
- ¿Qué criterios deberían impedir el paso a una fase siguiente?
- ¿Qué condiciones deberían activar un rollback?
- ¿Qué evidencias considera suficientes para una auditoría de la transición?
- ¿Qué capacidades o brechas de formación existen en los equipos involucrados?
- ¿Qué indicadores permiten afirmar que la transición mantiene continuidad e interoperabilidad?
- ¿Qué activos, claves o datos deberían priorizarse en la preparación pos-cuántica?
- ¿Qué cambios recomienda al artefacto para hacerlo más aplicable y auditable?

Anexo D. Ficha de validación por juicio experto

Escala: 1 = insuficiente; 2 = requiere cambios mayores; 3 = adecuado con ajustes; 4 = adecuado.

Añadir observaciones cualitativas cuando la puntuación sea menor a 4.

Tabla 16
Ficha de validación por juicio de experto

Criterio	**1**	**2**	**3**	**4**	**Observaciones**
Pertinencia respecto del objetivo					
Claridad de ítems/instrucciones					
Coherencia variable-indicador					
Suficiencia de cobertura					
Aplicabilidad en la EC					

Nota. Elaboración propia.

Anexo E. Modelo de consentimiento informado y confidencialidad

Propósito: participar en una investigación sobre transición de PKI RSA-ECC y preparación pos-cuántica en una Entidad de Certificación.

Participación: entrevista, revisión de instrumentos o valoración del artefacto según el rol asignado. La participación es voluntaria y puede finalizarse sin consecuencias.

Confidencialidad: la investigación reporta funciones y resultados agregados, no publica credenciales, claves, configuraciones secretas ni información que identifique al participante sin autorización expresa.

Uso de la información: exclusivamente académico y para mejora del artefacto de investigación. Las evidencias técnicas se depuran para excluir datos sensibles no necesarios.

Consentimiento: declaro haber recibido información suficiente, comprender el alcance de mi participación y aceptar voluntariamente participar.

Nombre/código: _____

Firma: _____

Fecha: _____

Anexo F. Plantilla de reproducibilidad y protocolo recomendado para nuevas réplicas

La siguiente configuración es un protocolo recomendado para futuras réplicas; no se presenta como reconstrucción de parámetros históricos no conservados.

Tabla 17
Plantilla de reproducibilidad

Nivel de carga	Concurrencia propuesta	Ramp-up	Duración de medición	Uso
Baja	10 solicitudes concurrentes	30 s	5 min	Estabilidad base
Media	50 solicitudes concurrentes	60 s	5 min	Transición y comportamiento intermedio
Alta	100 solicitudes concurrentes	120 s	5 min	Estrés controlado/preproductivo

Nota. Elaboración propia.

Cada réplica debe ejecutar al menos tres rondas por nivel de carga y conservar la serie completa; para los microbenchmarks se recomienda un mínimo de 80 repeticiones por operación y algoritmo. Antes de comparar algoritmos se ejecuta una fase de calentamiento no incluida en los resultados, se sincroniza la hora de los nodos y se verifica que no existan incidentes ajenos al experimento.