AÑO 4. No. 1
ISSN:2992-7978

TRANSICIÓN DE PKI HACIA ECC EN AUTORIDADES DE CERTIFICACIÓN: ANÁLISIS TÉCNICO Y ESTRATEGIA HÍBRIDA RSA/ECC

Lenin Alberto Vásquez González [1]

[1] Universidad Americana de Europa UNADE, Tesista / investigador, leninalbertov@gmail.com

AÑO 4. No. 1
ISSN:2992-7978

RESUMEN

El estudio evaluó la viabilidad de migrar infraestructura de clave pública hacia criptografía de curva elíptica en Autoridades de Certificación, combinando síntesis normativa y análisis cuantitativo. Inicialmente, se resumió fundamentos de ECDSA y equivalencias de seguridad cercanas a 128 bits entre RSA-3072, ECC-256 (P-256) y AES-128, con implicaciones en dimensionamiento de claves y perfiles X.509. A continuación, se diseñó un micro-benchmark reproducible con un tamaño de muestra n=80 por operación y algoritmo, que comparó RSA-2048, RSA-3072 y ECDSA P-256 en tareas de firma y verificación. Los resultados mostraron que ECC-256 reduce el tiempo de firma frente a RSA, es decir 0,95 ms vs 3,14–6,21 ms, mientras que RSA conservó ventaja en verificación, es decir 0,36–0,55 ms vs 1,09 ms. Además, se compiló evidencia de adopción internacional tomando como referencia credenciales y guías de Estonia, Alemania, Estados Unidos, Brasil y España. Esto respaldó la factibilidad regulatoria de ECC en esquemas de gran escala. El análisis propuso un enfoque híbrido RSA/ECC alineado con auditoría y compatibilidad. Los resultados cuantitativos se basaron en datos sintéticos simulados, no en mediciones directas sobre OpenSSL y HSM y se interpretaron como comparación relativa.

Palabras clave: Criptografía, Estrategia, Infraestructura de Clave Pública.

ABSTRACT

The study evaluated the feasibility of migrating Public Key Infrastructure to Elliptic Curve Cryptography within Certification Authorities by combining regulatory synthesis and quantitative analysis. First, it summarized the fundamentals of ECDSA and security equivalences close to 128 bits among RSA-3072, ECC-256 (P-256), and AES-128, with implications for key sizing and X.509 profiles. Next, a reproducible micro-benchmark was designed with a sample size of n=80 per operation and algorithm, comparing RSA-2048, RSA-3072, and ECDSA P-256 for signing and verification tasks. The results showed that ECC-256 reduces signing time compared to RSA, i.e., 0.95 ms vs 3.14–6.21 ms, while RSA retained an advantage in verification, i.e., 0.36–0.55 ms vs 1.09 ms. In addition, evidence of international adoption was compiled by referencing credentials and guidelines from Estonia, Germany, the United States, Brazil, and Spain. This supported the regulatory feasibility of ECC in large-scale schemes. The analysis proposed a hybrid RSA/ECC approach aligned with auditing and compatibility. The quantitative results were based on simulated synthetic data, not on direct measurements using OpenSSL and HSMs, and were interpreted as a relative comparison.

Keywords: Cryptography, Public Key Infrastructure, Strategy.

AÑO 4. No. 1
ISSN:2992-7978

INTRODUCCIÓN

Las Autoridades de Certificación (ACs) sostienen servicios digitales que requieren disponibilidad, interoperabilidad y cumplimiento. En ese contexto, la criptografía de curva elíptica (ECC[2]) resulta atractiva porque ofrece niveles de seguridad equivalentes con claves más cortas, lo que reduce tamaño de certificados y firmas, además de disminuir carga de procesamiento en escenarios de alta concurrencia (NIST, 2020).

Este trabajo delimita su alcance empírico desde el inicio, el análisis cuantitativo se apoya en un micro-benchmark[3] con datos sintéticos simulados y se interpreta como comparación relativa entre algoritmos, sin instrumentar implementaciones reales en OpenSSL o HSM[4] en esta versión.

En la práctica, las migraciones criptográficas se condicionan por compatibilidad con clientes heredados. Cambios recientes de cadenas de confianza en el ecosistema público evidencian que las transiciones graduales y la telemetría reducen riesgos de ruptura, por lo que los despliegues híbridos RSA[5]/ECC son comunes durante el período de convivencia (Kozlov, 2024; Mozilla, 2025; Sutaria, 2024).

El objetivo del estudio es sintetizar la base normativa que habilita ECC en la infraestructura de clave pública (PKI[6]) de confianza pública: comparar el rendimiento relativo de firma y verificación entre RSA-2048, RSA-3072 y ECDSA[7] P-256; y proponer una estrategia híbrida RSA/ECC con gobernanza y auditoría, preparada para una futura convergencia con criptografía poscuántica (PQC[8]) (ENISA, 2021; NIST, 2025).

En este contexto, el estudio sintetiza la base normativa que habilita ECC en PKI de confianza pública, en consecuencia, se plantea la siguiente pregunta de investigación: ¿en qué medida ECDSA P-256 mejora el rendimiento de firma y verificación frente a RSA-2048 y RSA-3072 en una PKI de confianza pública, y cómo se traducen esas diferencias en una estrategia híbrida RSA/ECC que preserve la compatibilidad y el cumplimiento auditable?

ESTADO DEL ARTE

La literatura y guías técnicas convergen en una idea central: para un nivel de seguridad cercano a 128 bits, RSA-3072 y ECC-256 (P-256) se consideran equivalentes, mientras AES[9]-128 actúa como referencia simétrica. La diferencia práctica está en la eficiencia, ECC logra objetos criptográficos más compactos y firmas más ligeras, lo que favorece cargas de firma intensiva y dispositivos con recursos limitados (NIST, 2020; NIST, 2023).

En adopción real, el factor que más condiciona el ritmo de migración es la compatibilidad. Por ello, las organizaciones tienden a preferir transiciones escalonadas, con coexistencia temporal (emisión dual) y monitoreo de impacto antes de retirar algoritmos heredados, especialmente cuando existe una base instalada de clientes antiguos.

En paralelo, se observa una adopción creciente de ECC en entornos regulados y de confianza pública, lo que sugiere que existen perfiles y prácticas auditables para operar ECC a escala, respaldando una hoja de ruta híbrida con metas realistas.

---

[2] ECC: Elliptic Curve Cryptography – Criptografía de curva elíptica
[3] Micro-benchmark: Técnica de evaluación de rendimiento centrada en medir la velocidad y eficiencia de componentes de software muy pequeños
[4] HSM: Hardware Security Module – Módulo de seguridad de hardware
[5] RSA: Rivest-Shamir-Adleman – Cifrado
[6] PKI: Public Key Infrastructure – Infraestructura de claves públicas
[7] ECDSA: Elliptic Curve Digital Signature Algorithm – Algoritmo de firma digital de curva elíptica
[8] PQC: Post-Quantum Cryptography – Criptografía Postcuántica
[9] AES: Advanced Encryption Standard – Estándar de cifrado avanzado

AÑO 4. No. 1
ISSN:2992-7978

MARCO TEÓRICO

El marco teórico define los elementos técnicos que guían el diseño de una PKI híbrida RSA/ECC. En particular, aborda criterios de dimensionamiento y ciclo de vida de claves, requisitos normativos y auditables para certificados X.509[10]. Compatibilidad operativa durante la migración y fundamentos de ECDSA con consideraciones de implementación segura.

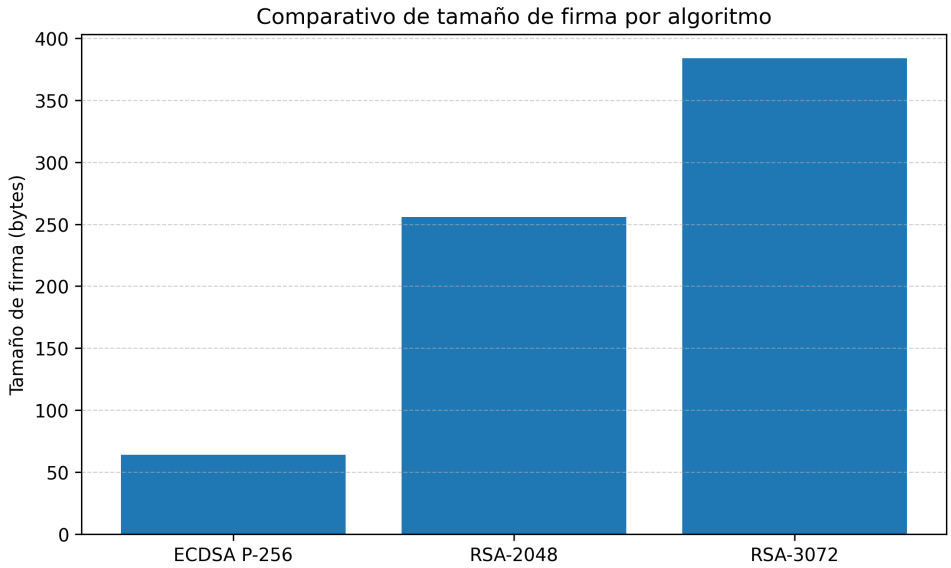
Equivalencias de seguridad y dimensionamiento

NIST SP 800-57 Part 1 Rev.5 presenta correspondencias entre tamaños de clave y bits de seguridad. Para un nivel cercano a 128 bits, RSA-3072 se considera equivalente a ECC-256 (P-256), y AES-128 se utiliza como referencia simétrica. Estas equivalencias orientan políticas de selección de parámetros, periodos de vigencia y decisiones de transición en una PKI híbrida (NIST, 2020).

En términos prácticos, la ventaja de ECC no está en más seguridad con los mismos bits, sino en la eficiencia: firmas y claves públicas más compactas, como se ve en la figura 1. Esto reduce la sobrecarga en certificación, firma masiva y escenarios con restricciones de cómputo o ancho de banda.

Figura 1

Equivalencias de seguridad por tamaño de clave RSA vs ECC



Nota. Elaboración propia con base en (NIST, 2020).

Marco normativo aplicado a PKI híbrida RSA/ECC

El marco normativo vigente habilita ECC en entornos de confianza pública y define criterios auditables para operar una PKI híbrida:

- **NIST SP 800-57:** guía equivalencias de seguridad y gestión del ciclo de vida de clave (NIST, 2020).
- **FIPS[11] 186-5:** define algoritmos de firma digital aprobados, incluyendo ECDSA, lo que sustenta su validez criptográfica en implementaciones formales (NIST, 2023).
- **RFC 5280:** establece el marco técnico PKIX/X.509 para certificados, extensiones y reglas de validación, base para perfiles interoperables en clientes y servidores (IETF, 2008).

[10] X.509: Estándar internacional para certificados de clave pública utiliza en una PKI
[11] FIPS: Federal Information Processing Standards – Estándar de procesamientos de información Federal

- **ETSI[12] EN 319 411-1 y ETSI EN 319 412:** fijan requisitos auditables para prestadores de servicios de confianza y perfiles/certificados X.509, proporcionando controles y criterios verificables de operación (ETSI, 2023).
- **Las Baseline Requirements CA/Browser Forum:** determina prácticas de emisión y validación relevantes para certificados en ecosistemas de confianza pública, condicionando compatibilidad y despliegue web (CA/Browser_Forum, 2023).

En conjunto, estos estándares ofrecen una base suficiente para justificar una transición controlada hacia ECC sin romper interoperabilidad, apoyándose en perfiles X.509 y reglas de validación ampliamente aceptadas.

Adopción internacional y compatibilidad

Más allá de la equivalencia criptográfica, el principal condicionante de la migración es la compatibilidad del ecosistema: clientes legados, bibliotecas antiguas, dispositivos embebidos y cadenas de confianza existentes. Por ello, una migración realista suele ejecutarse en fases:

- **Coexistencia temporal RSA/ECC:** en la emisión PKI híbrida.
- **Monitoreo de impacto:** en validación, handshakes TLS[13], y aceptación por clientes.
- **Retiro gradual:** de algoritmos heredados cuando el riesgo de incompatibilidad se vuelve marginal.

Esta estrategia reduce el riesgo operativo y permite cumplir requisitos auditables sin forzar cambios abruptos en consumidores de certificados. Ver Tabla 1.

Tabla 1

Ejemplos de países/estándares con uso o soporte de ECC 2020-2025

País	Credencial / Política	Estado / Algoritmo
Estonia	ID-card (EstEID)	ECC 384-bit en ID-card
Alemania	BSI TR-03110/03111 (eID)	Directrices ECC (ECDSA/ECDH, Brainpool)
Estados Unidos	NIST SP 800-78-5 (PIV)	ECC P-256/P-384 aprobado
Brasil	DOC-ICP-01.01 v5.0	Permite ECC (Brainpool) y ECDSA
España	DNIe 3.0	Uso principal RSA-2048; soporte ECC depende del perfil y/o servicio

Nota. Elaboración propia con base en (BSI, 2023; DNIe, 2025; ITI, 2022; NIST, 2023; RIA, 2025).

Fundamentos matemáticos y criptográficos (ECDSA)

ECDSA permite demostrar la autoría de un mensaje sin revelar la clave privada. A alto nivel, el firmante calcula el hash del mensaje y genera una firma como par (r, s) usando operaciones sobre una curva elíptica; el verificador usa el mensaje, la firma y la clave pública para confirmar autenticidad e integridad. FIPS 186-5 define formalmente ECDSA como esquema de firma aprobado (NIST, 2023).

Un punto crítico de seguridad es la generación del valor temporal (nonce). No debe reutilizarse ni ser predecible, ya que un fallo en este componente puede comprometer la clave privada. Por ello, la implementación debe asegurar una generación robusta y controles que reduzcan riesgos de filtración por fallos de aleatoriedad o exposición lateral.

En una curva elíptica $E/\mathbb{F}p$ con generador G de orden n, la clave privada es $d \in \{1,\ldots,n-1\}$ y la pública $Q=d \cdot G$. La firma ECDSA se define como $r=xR \pmod n$ y $s=k^{-1}(H(m)+d \cdot r) \pmod n$. La verificación acepta si el valor calculado $xV \pmod n$ coincide con r (NIST, 2023).

[12] ETSI: uropean Telecommunications Standards Institute – Instituto Europeo de Normas de Telecomunicaciones
[13] TLS: Transport Layer Security – Seguridad de la capa de transporte

AÑO 4. No. 1
ISSN:2992-7978

METODOLOGÍA

El estudio empleó un enfoque mixto basado en revisión documental de estándares para el marco normativo y el estado del arte, y un componente cuantitativo mediante un micro-benchmark reproducible. El área de estudio correspondió a la migración criptográfica las PKI operadas por AC, con énfasis en desempeño y compatibilidad de algoritmos de firma digital en flujos de emisión y validación de certificados X.509. La población de estudio se definió como el conjunto de ejecuciones posibles de las operaciones criptográficas de firma y verificación evaluadas en tres configuraciones: RSA-2048, RSA-3072 y ECDSA P-256. La unidad de análisis fue el tiempo de ejecución por operación (ms).

Para el componente cuantitativo se generaron n=80 observaciones por combinación algoritmo y operación de firma y verificación, para RSA-2048, RSA-3072 y ECDSA P-256, sobre datos sintéticos simulados (ms). Se reportaron medias y desviaciones estándar, y se aplicaron pruebas t de Welch para comparar diferencias de medias bajo varianzas no necesariamente iguales. Además, se calculó el tamaño de efecto (d de Cohen) y el intervalo de confianza al 95% de la diferencia de medias.

Dado que no se instrumentaron librerías criptográficas reales, los resultados representaron una línea base comparativa para orientar decisiones de diseño. Como trabajo futuro se planteó replicar el micro-benchmark sobre OpenSSL/BoringSSL y HSM con validación FIPS 140-3.

RESULTADOS

La Tabla 2 resume los estadísticos descriptivos obtenidos para firma y verificación, con n=80 observaciones por combinación de algoritmo y operación. Se observa menor tiempo promedio de firma en ECDSA P-256 y menor tiempo promedio de verificación en RSA.

Tabla 2

Medias (ms), desviación estándar y n por algoritmo y operación.

Algoritmo / Operación	Media (ms)	SD (ms)	N
ECDSA P-256 – Firma	0,950	0,173	80
RSA-2048 – Firma	3,136	0,414	80
RSA-3072 – Firma	6,205	0,877	80
ECDSA P-256 – Verificación	1,085	0,172	80
RSA-2048 – Verificación	0,360	0,063	80
RSA-3072 – Verificación	0,546	0,094	80

Nota. Elaboración propia

En la Tabla 3 se presentan las comparaciones entre algoritmos utilizando la t de Welch, junto con el IC95% y el tamaño de efecto (d de Cohen). Se reportan estos indicadores para describir la diferencia de medias y su magnitud práctica.

AÑO 4. No. 1
ISSN:2992-7978

Tabla 3

Pruebas t de Welch, IC95 % y tamaño de efecto. (d de Cohen)

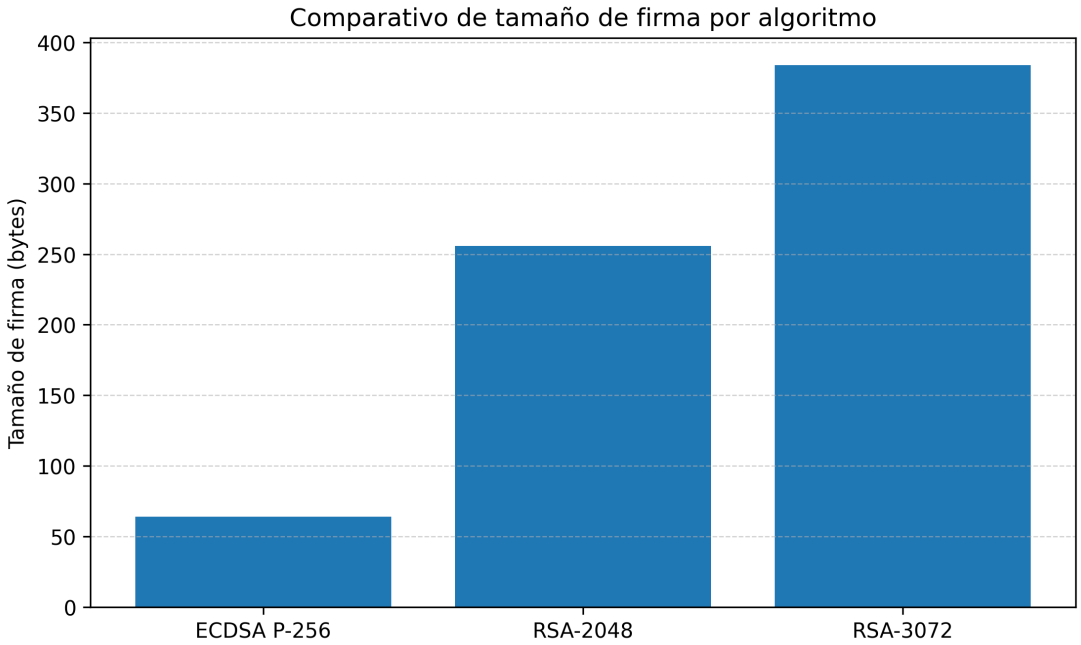
Operación	Comparación	Dif. media (ms)	IC95 % inf	IC95 % sup	t (Welch)	d (Cohen)
Firma	ECDSA P-256 vs RSA-2048	-2,1865	-2,2859	-2,0870	-43,592	-6,893
Firma	ECDSA P-256 vs RSA-3072	-5,2551	-5,4538	-5,0564	-52,579	-8,313
Firma	RSA-2048 vs RSA-3072	-3,0686	-3,2835	-2,8538	-28,303	-4,475
Verificación	ECDSA P-256 vs RSA-2048	0,7258	0,6850	0,7665	35,373	5,593
Verificación	ECDSA P-256 vs RSA-3072	0,5396	0,4961	0,5830	24,580	3,886
Verificación	RSA-2048 vs RSA-3072	-0,1862	-0,2111	-0,1612	-14,759	-2,334

Nota. Elaboración propia

En términos de tamaño de artefactos, la firma ECDSA P-256 ocupa 64 bytes dos componentes de 32 bytes, mientras que una firma RSA ocupa el tamaño del módulo: 256 bytes con RSA-2048 y 384 bytes con RSA-3072, como se ve en la figura 2 (NIST, 2020; NIST, 2023).

Figura 2

Comparativo de tamaño de firma por algoritmo (bytes)



Nota. Elaboración propia

AÑO 4. No. 1
ISSN:2992-7978

DISCUSIÓN

En conjunto, los resultados apoyan decisiones de arquitectura cuando el cuello de botella es la firma, como en sellado masivo o emisión intensiva; en ese escenario, ECC aporta mejoras en latencia y eficiencia. Cuando predomina la verificación en el cliente, RSA mantiene ventajas prácticas. Esta asimetría respalda una estrategia híbrida, donde el algoritmo se selecciona por carga y compatibilidad.

La estrategia híbrida se fundamenta en asignar el algoritmo al tipo de carga. En operaciones intensivas de firma, ECDSA P-256 ofrece menor latencia y firmas más pequeñas, lo cual mejora capacidad en AC y prestador de Servicios de confianza (TSP[14]). En verificación masiva, RSA conserva ventaja y se alinea con compatibilidad amplia en clientes heterogéneos; en lugar de un reemplazo abrupto, el despliegue recomendado es gradual y medible.

Desde la perspectiva de compatibilidad, la emisión dual temporal coexistiendo certificados de suscriptor RSA y ECC, permite mantener continuidad con clientes heredados mientras se recopila telemetría de fallos y se planifica el retiro de perfiles antiguos. Este enfoque reduce riesgos asociados a cambios de cadena, reconfiguraciones de confianza y actualizaciones de bibliotecas criptográficas (Mozilla, 2025; Sutaria, 2024).

Finalmente, la agenda poscuántica sugiere diseñar la transición como un camino, no como un salto. Una PKI que ya opera perfiles y gobernanza de convivencia RSA/ECC se encuentra mejor preparada para incorporar pruebas piloto y, cuando aplique, modos híbridos hacia PQC, sin comprometer interoperabilidad (ENISA, 2021; NIST, 2025).

Modelo de gobernanza y auditoría

La transición a un esquema híbrido RSA/ECC requiere controles operativos y evidencias auditables. La AC actualiza su CP[15]/CPS[16], define perfiles X.509 por caso de uso TLS, firma, OCSP[17] y establece métricas de compatibilidad. Además, centraliza claves de AC en HSM con controles de acceso, segregación de funciones y registros de auditoría. En el marco europeo, ETSI EN 319 411-1/319 412 formalizan requisitos de política y seguridad para TSP; en TLS público, CA/Browser Forum homologa prácticas de emisión y ciclo de vida (CA/Browser_Forum, 2023; ETSI, 2023).

Para el manejo de riesgos, se recomienda alinear el cambio con un sistema de gestión, incorporando evaluación de impacto, control de cambios, planes de reversión y verificación periódica del servicio de validación CRL[18]/OCSP. La gobernanza reduce la probabilidad de incidentes durante la convivencia y facilita auditorías recurrentes (ISO/IEC, 2022).

La Tabla 4 resume, de forma comparativa, qué aporta cada marco al funcionamiento y auditoría de una PKI que migra hacia ECC. Se priorizan normas usadas directamente en el análisis para evitar reiteraciones.

[14] TSP: Trust Service Provider – Prestador de servicios de confianza
[15] CP: Certificate Policy – Política de certificados
[16] CPS: Certification Practice Statement – Declaración de prácticas de certificación
[17] OCSP: Online Certificate Status Protocol – Protocolo de estado de certificado en línea
[18] CRL: Certificate Revocation List - Lista de certificados revocados

AÑO 4. No. 1
ISSN:2992-7978

Tabla 4

Comparativo normativo esencial para PKI híbrida RSA/ECC

Marco/Norma	Rol y alcance	Ámbito	Ventaja principal	Reto principal
RFC 5280 (X.509)	Perfil técnico de certificados/CRL	Global	Interoperabilidad y extensiones maduras	No define políticas de CA/TSP
ETSI EN 319 411-1	Política y seguridad para TSP	UE / referencia	Requisitos auditables (CP/CPS, ciclo de vida)	Mayor carga de cumplimiento
ETSI EN 319 412	Perfiles de certificados (incl. QC)	UE / referencia	Semántica armonizada de perfiles	Complejidad de perfiles/versiones

Nota. Elaboración propia con base en (IETF, 2008) (ETSI, 2023)

Implicaciones estratégicas

Para una transición operativa hacia ECC minimizando riesgos de interoperabilidad, se recomienda adoptar un esquema híbrido RSA/ECC con ejecución por fases. Primero, habilitar emisión dual y perfiles X.509 compatibles, priorizando ECDSA P-256 para nuevos certificados donde el ecosistema lo soporte, y manteniendo RSA-3072 o RSA-2048 como alternativa para legados. Segundo, actualizar la documentación de gobernanza CP/CPS, controles de auditoría y trazabilidad, incorporando políticas de generación de claves, manejo de nonces y mitigaciones contra canal lateral. Tercero, validar el impacto en infraestructura crítica mediante pruebas controladas con OpenSSL/HSM, midiendo latencias de firma y verificación, tasas de error, y consumo de recursos en escenarios representativos. Finalmente, establecer un plan de compatibilidad y una ruta de actualización gradual que reduzca fricción en usuarios y servicios dependientes.

CONCLUSIONES

Los resultados del micro-benchmark reproducible (n=80) indican que ECDSA P-256 reduce el tiempo promedio de firma frente a RSA-2048 y RSA-3072, mientras que RSA conserva ventaja en verificación.

El análisis indica que ECDSA P-256 ofrece un mejor desempeño relativo en operaciones de firma, mientras que RSA-2048 y RSA-3072 mantiene ventaja en verificación bajo las condiciones evaluadas.

En términos de diseño de PKI de confianza pública, estos hallazgos respaldan una estrategia híbrida RSA/ECC: utilizar ECC en escenarios de firma intensiva para reducir sobrecarga y mantener RSA donde la verificación y la compatibilidad con clientes legados resultan determinantes.

En el plano normativo, los estándares y guías analizados evidencian que ECC está habilitado y es compatible con perfiles X.509 y marcos auditables, lo que respalda su viabilidad en entornos de confianza pública. La evidencia de adopción internacional refuerza que su uso es operacionalizable en esquemas de gran escala.

Los resultados cuantitativos deben interpretarse como una comparación relativa, debido a que se basan en datos sintéticos simulados y no en mediciones directas sobre OpenSSL y HSM. Por ello, su generalización a entornos productivos requiere validación adicional bajo condiciones de operación reales.

Los hallazgos técnicos y regulatorios sustentan la viabilidad de incorporar ECC en PKI de confianza pública, siempre que se mantenga la interoperabilidad requerida por los ecosistemas y se controle el riesgo mediante validaciones en condiciones reales de operación.

AÑO 4. No. 1
ISSN:2992-7978

REFERENCIAS

BSI. (2023). *Technical guidelines on cryptography and eID (TR-03110/03111)*. BSI. https://www.bsi.bund.de/

CA/Browser_Forum. (2023). *Baseline Requirements for the Issuance and Management of PubliclyTrusted: TLS Server Certificates (v2.0.0)*.. CA/Browser Forum. https://cabforum.org/

DNIe. (2025, 05 05). *DNIe 3.0: Políticas de certificación (v3.2)*. DNIe. https://www.dnielectronico.es/PDFs/Politicas_de_certificacion_v3.2.pdf

ENISA. (2021, 05 3). *European Union Agency for Cybersecurity (ENISA). (2021). Post-quantum cryptography: Current state and quantum mitigation*. ENISA. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ETSI. (2023). *European Telecommunications Standards Institute (ETSI). (2023). ETSI EN 319 412-1: Certificate profiles; Part 1: Overview and common data structures (v1.5.1)*. ETSI. https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.05.01_60/en_31941201v010501p.pdf

IETF. (2008, 05). *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF. https://www.rfc-editor.org/rfc/rfc5280

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO/IEC. https://www.iso.org/standard/27001

ITI. (2022, 03 23). *Padrões e algoritmos criptográficos da ICP-Brasil. Instituto Nacional de Tecnologia da Informação*.. ITI. https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/IN2022_22_DOC_ICP_01.01_assinado.pdf

Kozlov, D. (2024, 03 14). *Upcoming Let's Encrypt certificate chain change and impact for Cloudflare customers*.. Cloudflare. https://blog.cloudflare.com/upcoming-lets-encrypt-certificate-chain-change-and-impact-for-cloudflare-customers/

Mozilla. (2025). *Mozilla Root Store Policy (v3.0)*.. Mozilla. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

NIST. (2020, 05). *Recommendation for Key Management: Part 1—General (SP 800-57 Part 1 Rev. 5)*. NIST. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

NIST. (2023, 02 03). *Digital Signature Standard (DSS) (FIPS PUB 186-5)*. NIST. https://csrc.nist.gov/publications/detail/fips/186/5/final

NIST. (2025, 03). *Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST IR 8545)*. NIST. https://csrc.nist.gov/pubs/ir/8545/final

RIA. (2025). *IDcard (EstEID): Information System Authority*.. ID. https://www.id.ee/en/id-card/

Sutaria, K. (2024, 04 12). *Deploying Let's Encrypt's New Issuance Chains*. Let's Encrypt. https://letsencrypt.org/2024/04/12/changes-to-issuance-chains