Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 11.1
Edición Especial XI 2026

LA DESMATERIALIZACIÓN DE LA FE PÚBLICA: DESAFÍOS DEL PROTOCOLO DIGITAL Y LA CIBERSEGURIDAD

DEMATERIALIZATION OF PUBLIC FAITH: CHALLENGES OF DIGITAL PROTOCOL AND CYBERSECURITY

Autores: [1]Aarón Stefano Fajardo Rodríguez, [2]Allison Dayana Cruz Gavilanez, [3]Alberto Alexander Alvarado Ajila y [4]Lissette Amelia Alvarado Ajila.
[1]ORCID ID: https://orcid.org/0009-0001-9847-3396
[2]ORCID ID: https://orcid.org/0009-0008-6146-1747
[3]ORCID ID: https://orcid.org/0000-0002-5908-6879
[4]ORCID ID: https://orcid.org/0009-0006-7050-1451
[1]E-mail de contacto: asfajardor@ube.edu.ec
[2]E-mail de contacto: adcruzg@ube.edu.ec
[3]E-mail de contacto: aalvaradoa@ube.edu.ec
[4]E-mail de contacto: laalvaradoa@ube.edu.ec
Afiliación: [1*2*3*4*]Universidad Bolivariana del Ecuador, (Ecuador).
Artículo recibido: 8 de Octubre del 2026.
Artículo revisado: 25 de Octubre del 2026.
Artículo aprobado: 25 de Octubre del 2026.
[1]Abogado de los Tribunales y Juzgados de la República del Ecuador, graduado de la Universidad de Guayaquil, (Ecuador), con 1 año de experiencia laboral. Maestrante de la maestría en Derecho Notarial y Registral de la Universidad Bolivariana del Ecuador, (Ecuador).
[2]Abogada de los Tribunales y Juzgados de la República del Ecuador, graduada de la Universidad de Guayaquil, (Ecuador), con 1 año de experiencia laboral. Maestrante de la maestría en Derecho Notarial y Registral de la Universidad Bolivariana del Ecuador, (Ecuador).
[3]Abogado de los Tribunales y Juzgados de la República del Ecuador, graduado de la Universidad de Guayaquil, (Ecuador) con 7 años de experiencia laboral. Ingeniero en Gestión Empresarial, graduado de la Universidad Particular San Gregorio de Portoviejo, (Ecuador). Magíster en Derecho Procesal, egresado de la Universidad Tecnológica ECOTEC, (Ecuador). Maestrante de la Maestría en Derecho Constitucional, Universidad Católica Andrés Bello, (Venezuela). Doctorante en Derecho de la Universidad Católica Andrés Bello, (Venezuela).
[4]Abogada de los Tribunales y Juzgados de la República del Ecuador, egresada de la Universidad de Guayaquil, (Ecuador), con 16 años de experiencia laboral. Contadora Pública Autorizada, graduada de la Universidad de Guayaquil, (Ecuador). Magíster en Derechos Fundamentales y Justicia Constitucional, graduada de la Universidad de Guayaquil, (Ecuador). Maestrante de la maestría en Derecho Constitucional, Universidad Católica Andrés Bello, (Venezuela). Doctorante en Derecho Universidad Católica Andrés Bello, (Venezuela).

Resumen

Esta investigación tiene como objetivo analizar la incidencia de la desmaterialización de la fe pública en el servicio notarial ecuatoriano sobre la seguridad jurídica, la autenticidad documental y la ciberseguridad, circunscribiendo su alcance al ordenamiento normativo nacional y a su articulación con estándares técnicos de seguridad de la información y ciberseguridad aplicables a la preservación, integridad y autenticidad del protocolo digital. Para ello, se emplea un enfoque cualitativo de carácter dogmático-jurídico y descriptivo-analítico, fundamentado en los métodos analítico-sintético, exegético-normativo y comparativo-conceptual, mediante los cuales se examinan la Ley Notarial, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y las resoluciones institucionales pertinentes, en contraste con estándares técnicos de seguridad informática. El análisis documental permitió identificar que, si bien el ordenamiento jurídico ecuatoriano reconoce la equivalencia funcional del mensaje de datos y de la firma electrónica, persisten insuficiencias reglamentarias y técnicas relacionadas con la preservación digital a largo plazo, los estándares mínimos de ciberseguridad y la distribución de responsabilidades frente a incidentes informáticos. Estos hallazgos permiten sostener que la eficacia jurídica del acto notarial telemático no depende únicamente de su reconocimiento normativo, sino también de la existencia de mecanismos técnicos que garanticen la integridad, autenticidad, trazabilidad y disponibilidad del protocolo digital.

Palabras clave: Desmaterialización de la fe pública, Protocolo matriz electrónico, Servicio notarial telemático, Seguridad jurídica, Ciberseguridad, Firma electrónica, Infraestructura de Clave Pública (PKI).

Abstract

This research aims to analyze the impact of the dematerialization of public faith in the Ecuadorian notarial service on legal certainty, documentary authenticity, and cybersecurity, limiting its scope to the national legal framework and its alignment with technical information security and cybersecurity standards applicable to the preservation, integrity, and authenticity of the digital protocol. To this end, a qualitative approach of a dogmatic-legal and descriptive-analytical nature is employed, based on the analytical-synthetic, exegetical-normative, and comparative-conceptual methods, through which the Notarial Law, the Law on Electronic Commerce, Signatures and Data Messages, and the relevant institutional resolutions are examined in contrast with technical information security standards. Documentary analysis revealed that, although Ecuadorian law recognizes the functional equivalence of data messages and electronic signatures, regulatory and technical shortcomings persist related to long-term digital preservation, minimum cybersecurity standards, and the distribution of responsibilities in the face of computer incidents. These findings support the view that the legal effectiveness of the telematic notarial act depends not only on its normative recognition, but also on the existence of technical mechanisms that guarantee the integrity, authenticity, traceability, and availability of the digital protocol.

Keywords: Dematerialized public faith, Electronic matrix protocol, Telematic notarial service, Legal certainty, Cybersecurity, Electronic signature, Public Key Infrastructure (PKI).

Sumário

Esta pesquisa tem como objetivo analisar a incidência da desmaterialização da fé pública no serviço notarial equatoriano sobre a segurança jurídica, a autenticidade documental e a cibersegurança, circunscrevendo seu alcance ao ordenamento normativo nacional e à sua articulação com padrões técnicos de segurança da informação e cibersegurança aplicáveis à preservação, integridade e autenticidade do protocolo digital. Para isso, emprega-se uma abordagem qualitativa de caráter dogmático-jurídico e descritivo-analítico, fundamentada nos métodos analítico-sintético, exegético-normativo e comparativo-conceitual, por meio dos quais se examinam a Lei Notarial, a Lei de Comércio Eletrônico, Assinaturas e Mensagens de Dados e as resoluções institucionais pertinentes, em contraste com padrões técnicos de segurança informática. A análise documental permitiu identificar que, embora o ordenamento jurídico equatoriano reconheça a equivalência funcional da mensagem de dados e da assinatura eletrônica, persistem insuficiências regulamentares e técnicas relacionadas à preservação digital de longo prazo, aos padrões mínimos de cibersegurança e à distribuição de responsabilidades diante de incidentes informáticos. Esses achados permitem sustentar que a eficácia jurídica do ato notarial telemático não depende apenas de seu reconhecimento normativo, mas também da existência de mecanismos técnicos que garantam a integridade, a autenticidade, a rastreabilidade e a disponibilidade do protocolo digital.

Palavras-chave: Fé pública desmaterializada, Protocolo matriz eletrônico, Serviço notarial telemático, Segurança jurídica, Cibersegurança, Assinatura eletrônica, Infraestrutura de Chaves Públicas (PKI).

Introducción

En el ordenamiento jurídico ecuatoriano, la transición hacia el notariado telemático obedece a una política de modernización institucional destinada a optimizar la eficacia administrativa, la gestión archivística y la democratización del acceso a los servicios fedatarios. No obstante, dicha materialización tecnológica carece de suficiencia jurídica si no garantiza ineludiblemente la autoría, la indemnidad, la reserva, el acceso continuo y la plena eficacia demostrativa que revisten a los instrumentos públicos conferidos mediante soportes digitales. En este contexto de transformación

digital, la sustitución progresiva del protocolo físico en soporte papel por el protocolo matriz electrónico plantea una profunda reconfiguración de la noción tradicional de inviolabilidad del documento público. Como han señalado diversos autores a nivel latinoamericano (Lozano-Serrano et al., 2025; Sabando Mendoza, 2019), la desmaterialización de la fe pública va más allá de la simple plasmación de firmas electrónicas sobre mensajes de datos: requiere edificar un modelo de seguridad jurídica preventiva sustentado en la resiliencia tecnológica del sistema.

En el ordenamiento ecuatoriano, aun cuando la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y las directrices operativas establecidas en la Resolución No. 305-2022, emitida por el Consejo de la Judicatura, otorgan plena eficacia jurídica a los instrumentos autorizados en sede electrónica, la función fedataria enfrenta complejos desafíos en materia de ciberseguridad y custodia del archivo notarial digital. Al respecto, la doctrina regional especializada (Dueñas-Palma et al., 2024) coincide en que la conservación de la función autenticadora en entornos telemáticos exige la implementación de estándares estrictos de criptografía asimétrica, infraestructura de clave pública (PKI) y sellado de tiempo (*timestamping*), herramientas indispensables para neutralizar ciberamenazas y suplantaciones de identidad y para garantizar la trazabilidad e inalterabilidad del protocolo digital. Para efectos de este artículo, se emplea de manera uniforme la expresión «firma electrónica», que es la denominación adoptada por la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (art. 13) y por la Ley Notarial (arts. 18.1 y 29, numeral 10). Las expresiones «firma electrónica avanzada» o «calificada», empleadas en otros ordenamientos y en parte de la doctrina, no constituyen categorías jurídicas distintas en la normativa ecuatoriana analizada, por lo que no se utilizan como equivalentes.

Del mismo modo, la sustitución del soporte físico en papel por mensajes de datos, firmas electrónicas y archivos audiovisuales plantea un severo dilema jurídico: la agilidad procedimental no puede menoscabar las garantías de la seguridad jurídica preventiva. El problema fundamental de esta investigación radica en la vulnerabilidad técnica y operativa que afronta la matriz electrónica; la desmaterialización del protocolo deslocaliza la función notarial y, al mismo tiempo, expone los instrumentos públicos a ciberamenazas, alteración no autorizada de registros, fallas en la custodia archivística a largo plazo y suplantación de identidad en entornos virtuales.

Por consiguiente, el alcance del presente estudio se circunscribe al ordenamiento jurídico ecuatoriano y su articulación con los estándares técnicos de seguridad de la información y ciberseguridad, evaluando en qué medida la infraestructura criptográfica y los mecanismos de seguridad de la información contribuyen a reforzar la autenticidad, integridad, trazabilidad, conservación y eficacia probatoria del acto notarial desmaterializado. Bajo esa tesitura, se formula el siguiente planteamiento: ¿De qué manera la desmaterialización de la fe pública en el servicio notarial ecuatoriano, mediante el protocolo digital y los servicios telemáticos, incide en la seguridad jurídica, la autenticidad documental y la ciberseguridad?

La desmaterialización no debe entenderse únicamente como la digitalización de documentos físicos. Implica trasladar determinados componentes del proceso notarial a un entorno digital, en el que intervienen mecanismos de identificación, firma

electrónica, almacenamiento seguro y verificación de la integridad documental (Dolynska, 2023). En ese marco, la digitalización puede consistir tanto en la reproducción electrónica de documentos originalmente físicos como en la configuración de procedimientos notariales que nacen, circulan y se conservan dentro de sistemas electrónicos (Rizkianto et al., 2022).

El debate doctrinal latinoamericano en torno a la función notarial en la era digital ha transitado desde la discusión inicial sobre el principio de equivalencia funcional hacia la gobernanza del riesgo tecnológico en la fe pública. El autor Sabando (2019) coincide en que la fe pública conserva su naturaleza garantista en el entorno digital únicamente cuando la arquitectura del sistema asegura la autoría, la integridad y la inalterabilidad mediante esquemas de firma electrónica y la Infraestructura de Clave Pública (PKI). Por su parte, la doctrina notarial clásica y contemporánea (Sabando M, 2019) enfatiza que la función del fedatario excede la mera autenticación formal, exigiendo un juicio de capacidad y libertad de consentimiento que, en el ámbito telemático, requiere herramientas biométricas y sellado de tiempo (*timestamping*) para evitar vicios en el otorgamiento.

No obstante, investigaciones recientes en el contexto nacional Dueñas et al. (2024); Lozano et al. (2025) advierten que la legislación ecuatoriana ha priorizado la rapidez del trámite sin consolidar un marco integral de ciberseguridad, lo que evidencia insuficiencias reglamentarias y técnicas relacionadas con la inmutabilidad de los repositorios digitales, los estándares de ciberseguridad y la distribución de responsabilidades ante incidentes informáticos. De esta literatura se desprende que, si bien la norma consagra la validez del acto telemático, todavía falta profundizar en las garantías cibernéticas que sustentan el protocolo digital. A este debate se suman aportes comparados que amplían la mirada sobre la digitalización notarial: en el ámbito indonesio, Maengkom (2021) y Susilawati et al. (2024) documentan la implementación de sistemas de seguridad de la información y de transacciones electrónicas para actas notariales, mientras que Ngadino (2021) examina la responsabilidad del notario por el almacenamiento electrónico de los protocolos.

Desde una perspectiva más crítica, Latorre (2024) analiza la función notarial como engranaje del Estado en la gestión de arreglos materiales y jurídicos. En el contexto ecuatoriano, Toscano Broncano y Mayorga Almeida (2026) profundizan en la eficacia probatoria del instrumento público, y Vélez Tumbaco y Delgado Alcívar (2026) analizan el impacto concreto de la digitalización en el servicio notarial del país; estos aportes refuerzan la pertinencia de examinar el caso ecuatoriano con el rigor que aquí se propone.

En virtud de lo expuesto, el objetivo general de la presente investigación es analizar la incidencia de la desmaterialización de la fe pública en el servicio notarial ecuatoriano sobre la seguridad jurídica, la autenticidad documental y la ciberseguridad, en el marco del ordenamiento jurídico nacional y de su articulación con estándares técnicos de seguridad de la información y ciberseguridad aplicables a la preservación, integridad y autenticidad del protocolo digital.

Materiales y Métodos

Para abordar esta problemática, la investigación se desarrolla bajo un enfoque cualitativo de carácter dogmático-jurídico y descriptivo-analítico. El método analítico-sintético se aplica sobre la Ley Notarial, la Ley de Comercio

Electrónico, Firmas y Mensajes de Datos y las Resoluciones del Consejo de la Judicatura, en particular la Resolución No. 305-2022, con el fin de descomponer sus disposiciones sobre equivalencia funcional, custodia del protocolo digital y responsabilidad del notario, para luego integrarlas en una lectura conjunta sobre la fe pública desmaterializada. Mediante la exégesis normativa se examinan puntualmente las categorías jurídicas de autenticidad documental, inalterabilidad y trazabilidad contenidas en dichas normas, estableciendo su alcance literal y su compatibilidad con los estándares técnicos vigentes.

Asimismo, se aplica el método comparativo-conceptual, mediante el cual se contrastan los requisitos jurídicos de la fe pública, autoría, integridad e inalterabilidad, con estándares técnicos de ciberseguridad, tales como la norma ISO/IEC 27001 (*International Organization for Standardization* [ISO] e *International Electrotechnical Commission* [IEC], 2022) y los protocolos de criptografía asimétrica; este contraste se entiende como un ejercicio metodológico entre exigencias jurídicas y soluciones técnicas; no propiamente como derecho comparado entre ordenamientos, con el objetivo de identificar la brecha existente entre la prescripción legal y la resiliencia cibernética de las notarías.

El corpus documental de la investigación estuvo integrado por la normativa ecuatoriana directamente vinculada con la prestación del servicio notarial telemático, particularmente la Ley Notarial, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y la Resolución No. 305-2022 del Consejo de la Judicatura, complementadas con la norma ISO/IEC 27001:2022 como referente técnico, y con doctrina especializada y literatura científica reciente sobre digitalización notarial, seguridad jurídica y ciberseguridad. La selección de las fuentes respondió a criterios de pertinencia temática, actualidad y relación directa con el problema de investigación. Para el análisis se establecieron como categorías principales la seguridad jurídica, la autenticidad documental, la identificación del compareciente, la conservación del protocolo digital, la integridad de los archivos, la gestión de riesgos de ciberseguridad y la responsabilidad frente a incidentes tecnológicos. Estas categorías permitieron organizar la revisión normativa y doctrinal: para cada una se identificaron las disposiciones que regulan el aspecto correspondiente, se determinó qué elementos quedan sin regulación expresa y se contrastó ese resultado con la doctrina consultada, lo que permitió estructurar posteriormente los resultados y su discusión.

Resultados y Discusión

El análisis documental y dogmático-jurídico desarrollado permite exponer los resultados organizados por categorías, contrastando la normativa vigente con la doctrina examinada y precedidos, en cada caso, por las disposiciones concretas de las que se deriva cada hallazgo. En materia de seguridad jurídica, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos reconoce a los mensajes de datos igual valor jurídico que a los documentos escritos (art. 2), atribuye a la firma electrónica la misma validez y efectos jurídicos que a la firma manuscrita (art. 14) y admite ambos como medios de prueba (art. 52).

A su vez, la Ley Notarial dispone que los servicios notariales pueden prestarse de manera física o telemática (art. 5) y regula la comparecencia telemática y la suscripción de los instrumentos con firmas electrónicas (arts. 18.1 y 29, numeral 10), mientras que la Resolución No. 305-2022 aprueba el protocolo

operativo del servicio notarial telemático. Sin embargo, del análisis de estas disposiciones no se identifica una regulación específica que establezca estándares técnicos obligatorios para garantizar la preservación a largo plazo del protocolo matriz electrónico: el artículo 8, literal d, de la Ley de Comercio Electrónico condiciona la conservación de los mensajes de datos a que «se garantice su integridad por el tiempo que se establezca en el reglamento», y el artículo 22 de la Ley Notarial encarga al notario la conservación de los protocolos, sin que ninguna de estas normas precise formatos, soportes o condiciones técnicas de preservación digital. En consecuencia, la insuficiencia detectada no recae sobre la validez jurídica del acto telemático, sino sobre las condiciones técnicas y reglamentarias necesarias para asegurar su conservación, disponibilidad e integridad en el tiempo.

Este resultado dialoga con el planteamiento de Toscano Broncano y Mayorga Almeida (2026) sobre la relación entre fe pública y eficacia probatoria del instrumento público. En el entorno telemático, esa eficacia ya no descansa únicamente en la intervención del notario, sino también en la capacidad del sistema para demostrar que el documento no ha variado desde su otorgamiento. Por ello, a juicio de los autores, el reconocimiento normativo del documento electrónico es condición necesaria, pero no suficiente, para la seguridad jurídica del acto notarial desmaterializado.

En cuanto a la autenticidad documental y la identificación del compareciente, el artículo 15 de la Ley de Comercio Electrónico exige que la firma electrónica permita «verificar inequívocamente la autoría e identidad del signatario» y que su método de creación y verificación sea «confiable, seguro e inalterable» (literales b y c). El artículo 18.1 de la Ley Notarial, por su parte, dispone que la plataforma del Consejo de la Judicatura debe permitir al notario ver, escuchar e interactuar con los comparecientes y constatar su capacidad, conocimiento y voluntad.

La Resolución No. 305-2022 exige a los solicitantes contar con firma electrónica vigente emitida por una autoridad certificadora autorizada (numeral 9.1) y describe los pasos para la verificación de identidad de los comparecientes (numeral 9.5.4.2). No obstante, esos pasos se formulan en términos facultativos, se podrá seguir los siguientes pasos, de modo que la resolución no fija estándares técnicos mínimos y obligatorios de verificación de identidad, como la validación biométrica o los niveles de aseguramiento, y deja a discreción de cada notaría la robustez del proceso de identificación del compareciente.

Este hallazgo complementa lo sostenido por Sabando Mendoza (2019), quien vincula la autoría del documento notarial digital con el uso de la firma electrónica y de la infraestructura de clave pública. La firma electrónica acredita el vínculo entre el certificado y el mensaje de datos, pero no verifica por sí sola que quien comparece ante la cámara sea el titular del certificado ni que actúe con voluntad libre. Desde esta perspectiva, la eficacia de la fe pública en sede telemática exige que la identificación del compareciente deje de ser una práctica facultativa y se convierta en un procedimiento reglado y verificable.

Respecto de la conservación del protocolo digital, el artículo 22 de la Ley Notarial establece que los protocolos pertenecen al Estado y que los notarios los conservarán «como archiveros de los mismos y bajo su responsabilidad», y el artículo 18.1 ordena archivar en el protocolo digital la

videoconferencia íntegra y completa. En el mismo sentido, el numeral 9.5.4.8 de la Resolución No. 305-2022 enumera los elementos que integran el archivo electrónico, y su Disposición General Segunda establece que, hasta la implementación de la «Plataforma Electrónica Segura para la prestación del servicio notarial telemático», los respaldos digitales quedarán bajo custodia de los notarios conforme a los criterios de la Resolución 202-2021.

Sin embargo, ninguna de estas disposiciones remite a un estándar técnico de gestión de la seguridad de la información, como la norma ISO/IEC 27001 (ISO e IEC, 2022), de cumplimiento obligatorio para las notarías, a diferencia de los modelos comparados en los que la literatura documenta sistemas específicos de seguridad de la información para los actos notariales electrónicos, como el ucraniano (Dolynska, 2023) o el indonesio (Maengkom, 2021; Susilawati et al., 2024). Esta ausencia expone al protocolo digital al riesgo de pérdida de disponibilidad sin que exista una obligación reglamentaria expresa de mitigación. Este hallazgo coincide con lo advertido por Dueñas-Palma et al. (2024) y Lozano-Serrano et al. (2025), quienes identifican dificultades derivadas de la modernización tecnológica del sistema notarial cuando esta no se acompaña de mecanismos suficientes de seguridad y preservación.

No obstante, el análisis realizado permite precisar que la problemática no se encuentra en la inexistencia de reconocimiento jurídico del documento electrónico, sino en la falta de desarrollo reglamentario de obligaciones técnicas específicas de conservación. Desde esta perspectiva, la insuficiencia debe calificarse como reglamentaria y técnica, y no como un vacío absoluto respecto de la validez jurídica del acto. Sobre la integridad de los archivos, la doctrina consultada (Dueñas-Palma et al., 2024) coincide en la necesidad de sellado de tiempo, criptografía asimétrica y módulos de seguridad hardware. La normativa ecuatoriana se aproxima a estas exigencias al requerir que el método de creación y verificación de la firma electrónica sea «confiable, seguro e inalterable» (art. 15, literal c, de la Ley de Comercio Electrónico) y que se conserve todo dato que permita determinar el origen, el destino, la fecha y la hora del mensaje de datos (art. 8, literal c); además, el numeral 9.5.4.5 de la Resolución No. 305-2022 regula la suscripción electrónica de la escritura por los comparecientes y el notario.

No obstante, estas disposiciones fijan resultados exigibles y no mecanismos técnicos concretos: no imponen el sellado de tiempo emitido por un tercero de confianza ni el uso de módulos de seguridad hardware como requisitos para la autorización de actos notariales electrónicos, por lo que su implementación depende de la política interna de cada notaría. A juicio de los autores, esta formulación por resultados es coherente con el principio de neutralidad tecnológica; sin embargo, en ausencia de desarrollo reglamentario, traslada al notario decisiones técnicas que exceden su ámbito profesional y produce niveles de protección heterogéneos entre notarías, lo que resulta difícilmente compatible con la uniformidad que exige la fe pública.

En materia de riesgos de ciberseguridad, la literatura nacional advierte que la legislación ecuatoriana priorizó la agilidad del trámite telemático sin consolidar un marco integral de ciberseguridad (Dueñas-Palma et al., 2024; Lozano-Serrano et al., 2025). El análisis normativo confirma esta advertencia: el artículo 18.1 de la Ley Notarial se limita a señalar que la plataforma del Consejo de la Judicatura

«garantizará la seguridad del acto notarial», y la Resolución No. 305-2022 no contiene protocolos obligatorios de detección, notificación y respuesta ante incidentes informáticos que afecten al archivo notarial digital.

Este resultado se inscribe en la línea de los estudios nacionales sobre digitalización notarial (Vélez Tumbaco y Delgado Alcívar, 2026), pero permite precisar que el déficit no reside en la ausencia de un mandato general de seguridad, que sí existe en la Ley Notarial, sino en la falta de reglas operativas que conviertan ese mandato en obligaciones concretas y verificables. En lo relativo a la responsabilidad frente a incidentes, el artículo 22 de la Ley Notarial atribuye al notario la conservación de los protocolos «bajo su responsabilidad», mientras que el artículo 18.1 asigna a la plataforma del Consejo de la Judicatura la función de garantizar la seguridad del acto notarial. Ni la ley ni la Resolución No. 305-2022 distribuyen expresamente la responsabilidad entre el notario, el Consejo de la Judicatura —como administrador de la plataforma telemática— y los proveedores tecnológicos externos, pese a que el artículo 8 de la Ley de Comercio Electrónico admite que la conservación de los mensajes de datos se realice mediante servicios de terceros. Esta concurrencia de deberes sin reglas de imputación genera incertidumbre sobre a quién corresponde responder cuando el incidente se origina en la infraestructura institucional o en un proveedor externo.

Este hallazgo guarda relación con lo examinado por Ngadino (2021) respecto de la responsabilidad del notario por el almacenamiento electrónico de los protocolos. En el caso ecuatoriano, la coexistencia de un deber personal de custodia del notario (art. 22) y de un deber institucional de seguridad de la plataforma (art. 18.1) sugiere que la responsabilidad debería graduarse según el origen del incidente, de modo que el notario no responda por fallas de una infraestructura que no controla. En síntesis, el ordenamiento jurídico ecuatoriano reconoce plena validez al acto notarial desmaterializado, de modo que no existe un vacío normativo en cuanto a su eficacia jurídica; la insuficiencia identificada es de carácter reglamentario y técnico, y se concentra en la preservación a largo plazo, los estándares mínimos de ciberseguridad y la distribución de responsabilidades ante incidentes informáticos.

Conclusiones

A partir del análisis jurídico, normativo y técnico desarrollado sobre la desmaterialización de la función fedataria y sus implicaciones en la era digital, se plantean las siguientes conclusiones: La transición del protocolo en papel al entorno telemático no se limita a convertir documentos físicos en mensajes de datos, sino que exige preservar en la comparecencia electrónica las garantías propias de la función notarial, especialmente la correcta identificación del compareciente y la verificación de su capacidad, conocimiento y voluntad. En consecuencia, la digitalización del servicio debe asegurar que estas funciones puedan cumplirse con un nivel adecuado de certeza jurídica en el entorno telemático.

La eficacia probatoria y la integridad del protocolo matriz electrónico dependen, además de su reconocimiento jurídico, de condiciones técnicas adecuadas para su generación, conservación y verificación. En este contexto, mecanismos como la infraestructura de clave pública (PKI), el sellado de tiempo, la criptografía asimétrica y los sistemas seguros de custodia de claves constituyen herramientas relevantes para reforzar la autenticidad,

integridad, trazabilidad y conservación del documento público electrónico. El ordenamiento jurídico ecuatoriano reconoce la equivalencia funcional del mensaje de datos y de la firma electrónica (arts. 2 y 14 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos); por tanto, la insuficiencia identificada no afecta a la validez del acto, sino que es de carácter reglamentario y técnico, y se concentra en la preservación digital a largo plazo, la estandarización de los archivos notariales, los estándares mínimos de ciberseguridad y la distribución de responsabilidades ante incidentes informáticos.

En consecuencia, el fortalecimiento del servicio notarial telemático requiere articular el control de legalidad ejercido por el notario con estándares verificables de seguridad de la información, trazabilidad, auditoría digital y respuesta ante incidentes. Esta articulación contribuiría a reforzar la integridad, confidencialidad, disponibilidad y eficacia probatoria del protocolo digital frente a los riesgos propios de la prestación telemática del servicio notarial.

Referencias Bibliográficas

Consejo de la Judicatura. (2022). *Resolución 305-2022: Protocolo para el uso de plataformas y herramientas para la prestación del servicio notarial telemático*. Registro Oficial No. 232, 18 de enero de 2023. https://www.funcionjudicial.gob.ec/resources/pdf/resoluciones/2022/305-2022.pdf

Dolynska, M. (2023). Evolution of legal regulation of digitalization of notarial activity in independent Ukraine. *Social Legal Studios, 6*(4), 58–68. https://doi.org/10.32518/sals4.2023.58

Dueñas, G., Rey, C., & García, N. (2024). Seguridad jurídica mediante la modernización del sistema notarial y registral. *Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales, 3*(especial 3), 254–262. https://doi.org/10.62574/wyrvta39

International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

Latorre, S. (2024). The place of the public notary: How the engine of the capitalist state operates through material and legal arrangements. *Environment and Planning C: Politics and Space, 42*(3), 401–416. https://doi.org/10.1177/23996544221110040

Ley de Comercio Electrónico, Firmas y Mensajes de Datos [Ley No. 67]. (2002, 17 de abril). Registro Oficial Suplemento 557. Congreso Nacional del Ecuador.

Ley Notarial [Decreto Supremo No. 1404]. (1966, 11 de noviembre). Registro Oficial 158. Texto con reformas hasta el 16 de febrero de 2022. https://www.gob.ec/sites/default/files/regulations/2022-10/LEY%20NOTARIAL.pdf

Lozano-Serrano, L. A., Alfonso-González, I., & Castro-Sánchez, F. de J. (2025). Prestación del servicio notarial telemáticamente y la naturaleza jurídica del notario ecuatoriano. *Noesis. Revista Electrónica de Investigación, 7*(1), 1483–1499. https://doi.org/10.35381/noesisin.v7i1.505

Maengkom, C. R. (2021). Electronic information security system for notarial deeds as national archives. En *Proceedings of the Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2019)*. Atlantis Press. https://doi.org/10.2991/assehr.k.210531.094

Ngadino, N. (2021). Notary responsibility for electronic storage of notary protocols. *Jurnal Pembaharuan Hukum, 8*(1), 60–72. https://doi.org/10.26532/jph.v8i1.15235

Rizkianto, K., Rahayu, K., & Mukhidin, M. (2022). Cyber notary: Kepastian hukum penyimpanan dokumen notaris. *Diktum:*

Jurnal Ilmu Hukum, 10(2), 164–176. https://doi.org/10.24905/diktum.v10i2.105

Sabando Mendoza, M. V. (2019). *La actuación del notario frente a los actos contenidos en medios electrónicos contemplados en la legislación ecuatoriana, y su aporte a la seguridad jurídica* [Tesis de maestría, Universidad Católica de Santiago de Guayaquil]. Repositorio Digital UCSG. http://repositorio.ucsg.edu.ec/handle/3317/12111

Susilawati, T., Asikin, Z., & Suhartana, L. W. P. (2024). Implementation of electronic transactions of notary's deeds in improving legal certainty and data security. *Path of Science, 10*(1), 8024–8033. https://doi.org/10.22178/pos.100-33

Toscano, F., & Mayorga, M. (2026). La fe pública y su eficacia en la prueba documental: Alcances del instrumento público. *VitalyScience Revista Científica Multidisciplinaria, 4*(9), 100–114. https://doi.org/10.56519/sz3jjw71

Vélez, E., & Delgado, C. (2026). Impacto de la digitalización en el servicio notarial en Ecuador. *Ibero Ciencias - Revista Científica y Académica, 5*(2), 378–392. https://doi.org/10.63371/ic.v5.n2.a976

Esta obra está bajo una licencia de Creative Commons Reconocimiento-No Comercial 4.0 Internacional. Copyright © Aarón Stefano Fajardo Rodríguez, Allison Dayana Cruz Gavilanez, Alberto Alexander Alvarado Ajila y Lissette Amelia Alvarado Ajila.

Declaraciones éticas y editoriales del artículo

Contribución de los autores (Taxonomía CRediT).

Aarón Stefano Fajardo Rodríguez: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.

Allison Dayana Cruz Gavilanez: curación y organización de los datos, participación en la recolección de información, validación de los resultados obtenidos y elaboración de representaciones gráficas y visualización de los datos.

Alberto Alexander Alvarado Ajila: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.

Lissette Amelia Alvarado Ajila: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio.

Declaración de conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.

Declaración de financiamiento

La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.

Declaración del editor

El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.

Declaración de los revisores

Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.

Declaración ética de la investigación

Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.

Declaración sobre el uso de inteligencia artificial

Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.

Disponibilidad de datos

Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.