

**VALIDEZ Y CONTRADICCIÓN DE LA PRUEBA DIGITAL EN PROCESOS DE
SOCIEDADES MERCANTILES BAJO EL COGEP**
**VALIDITY AND ADVERSARIAL TESTING OF DIGITAL EVIDENCE UNDER THE
COGEP: PROCEEDINGS INVOLVING COMMERCIAL COMPANIES**

Autores: ¹Andrea Carolina Arce Oñate, ²Gilda Cecilia Herrera Herrera, ³Holger Geovanny García Segarra.

¹ORCID ID: <https://orcid.org/0009-0009-7264-4538>

²ORCID ID: <https://orcid.org/0009-0009-2576-6313>

³ORCID ID: <https://orcid.org/0009-0009-2499-762X>

¹E-mail de contacto: acarceo@ube.edu.ec

²E-mail de contacto: gcherrera_h_a@ube.edu.ec

³E-mail de contacto: hggarcias@ube.edu.ec

Afiliación: ¹*²*³Universidad Bolivariana del Ecuador, (Ecuador).

Artículo recibido: 3 de Octubre del 2026.

Artículo revisado: 15 de Octubre del 2026.

Artículo aprobado: 15 de Octubre del 2026.

¹Contadora Pública Autorizada, graduada de la Universidad de Guayaquil, (Ecuador), con 18 años de experiencia laboral. Magíster en Finanzas de la Escuela Superior Politécnica del Litoral, (Ecuador). Abogada de los Tribunales y Juzgados de la República del Ecuador en la Universidad de Guayaquil, (Ecuador).

²Abogada de los Tribunales y Juzgados de la República, graduada de la Universidad de Guayaquil, (Ecuador), con 23 años de experiencia. Especialista en Derecho Penal y Justicia Indígena por la Universidad Autónoma de los Andes, (Ecuador). Magíster en Derecho Procesal, graduada de la Universidad Bolivariana del Ecuador, (Ecuador). Doctora en Jurisprudencia, graduada de la Universidad Nacional de Loja, (Ecuador). Doctorante en Ciencias Jurídicas de la Universidad de la Habana, (Cuba).

³Abogado de los Tribunales y Juzgados de la República del Ecuador, graduado de la Universidad de Guayaquil, (Ecuador). Magíster en Derecho Procesal de la Universidad Tecnológica ECOTEC, (Ecuador). Doctorante en Derecho Municipal, en la Universidad de la Habana, (Cuba).

Resumen

El artículo examina cómo regula el Código Orgánico General de Procesos (COGEP) la prueba digital en entornos virtuales y qué efecto tiene esa regulación sobre el principio de contradicción, el derecho a la defensa y la seguridad jurídica en los procesos judiciales en que intervienen sociedades mercantiles en Ecuador. Se realizó una investigación cualitativa de tipo jurídico-documental con los métodos dogmático, exegetico y comparado. Las fuentes normativas, jurisprudenciales y doctrinales se seleccionaron por su vigencia, pertinencia y jerarquía, y la comparación con Colombia, China y España se hizo a partir de tres variables comunes. El COGEP reconoce la prueba digital, pero sus reglas de admisibilidad, impugnación y valoración no dicen quién debe aportar el archivo original y sus metadatos, cómo se preserva la evidencia ni cuándo procede el peritaje informático. Ese vacío pesa más sobre la prueba corporativa: actas de juntas generales, correos institucionales y documentos validados con código hash. El marco vigente no asegura una contradicción

efectiva de la prueba digital societaria. Se propone un articulado de reforma al COGEP sobre representaciones gráficas, cadena de custodia digital, impugnación con acceso protegido a metadatos y peritaje informático, validado según su adecuación constitucional, coherencia sistemática, viabilidad institucional y efecto sobre la igualdad procesal.

Palabras clave: Prueba digital, Principio de contradicción, Sociedades mercantiles, Cadena de custodia digital, Validez jurídica.

Abstract

This article examines how Ecuador's Organic General Code of Procedure (COGEP) regulates digital evidence in virtual environments and how that regulation affects the adversarial principle, the right to defense, and legal certainty in judicial proceedings involving commercial companies. A qualitative legal-documentary study was carried out using dogmatic, exegetical, and comparative methods. Legislation, case law, and scholarship were selected for their validity, relevance, and hierarchy, and the comparison with Colombia,

China, and Spain relied on three common variables. The COGEP recognizes digital evidence, but its rules on admissibility, challenge, and assessment do not state who must produce the original file and its metadata, how evidence is to be preserved, or when a digital forensic examination is required. This gap weighs most heavily on corporate evidence: minutes of shareholders' meetings, institutional emails, and documents validated with hash codes. The current framework does not ensure effective adversarial testing of corporate digital evidence. Draft amendments to the COGEP are proposed on graphic representations, digital chain of custody, challenges with protected access to metadata, and digital forensic expertise, validated for constitutional consistency, systemic coherence, institutional feasibility, and effect on procedural equality.

Keywords: Digital evidence, adversarial principle, commercial companies, digital chain of custody, legal validity.

Sumário

O artigo examina como o Código Orgânico Geral de Processos (COGEP) regula a prova digital em ambientes virtuais e que efeito essa regulação tem sobre o princípio do contraditório, o direito de defesa e a segurança jurídica nos processos judiciais em que intervêm sociedades mercantis no Equador. Realizou-se uma pesquisa qualitativa de tipo jurídico-documental com os métodos dogmático, exegético e comparado. As fontes normativas, jurisprudenciais e doutrinárias foram selecionadas por sua vigência, pertinência e hierarquia, e a comparação com Colômbia, China e Espanha foi feita a partir de três variáveis comuns. O COGEP reconhece a prova digital, mas suas regras de admissibilidade, impugnação e valoração não dizem quem deve apresentar o arquivo original e seus metadados, como a evidência é preservada nem quando cabe a perícia informática. Essa lacuna pesa mais sobre a prova corporativa: atas de assembleias gerais, correios eletrônicos institucionais e documentos validados com código hash. O

marco vigente não assegura um contraditório efetivo da prova digital societária. Propõe-se um articulado de reforma ao COGEP sobre representações gráficas, cadeia de custódia digital, impugnação com acesso protegido aos metadados e perícia informática, validado segundo sua adequação constitucional, coerência sistemática, viabilidade institucional e efeito sobre a igualdade processual.

Palavras-chave: Prova digital, princípio do contraditório, sociedades mercantis, cadeia de custódia digital e validade jurídica.

Introducción

Correos electrónicos, conversaciones de mensajería, contratos con firma electrónica y registros de sistemas informáticos forman parte hoy del material probatorio corriente en los juzgados ecuatorianos. En los procesos en que intervienen sociedades mercantiles esta evidencia suele ser la principal, porque la vida de la empresa, desde sus juntas hasta su contabilidad, se documenta casi por completo en soportes electrónicos. Interesa saber si las reglas procesales vigentes permiten a la contraparte examinar esa evidencia y discutirla en condiciones reales.

El Código Orgánico General de Procesos (en adelante, COGEP) admite la prueba digital, pero no fija protocolos técnicos para obtenerla, conservarla, practicarla y contradecirla. Herrera (2025) recuerda que la validez probatoria exige condiciones mínimas de autenticidad, integridad, fiabilidad y posibilidad de contradicción, y Ramírez (2017) insiste en que las partes deben poder conocer, impugnar y controvertir lo que se incorpora al proceso. Si faltan reglas claras, el juez valora con amplia discrecionalidad y la contradicción termina dependiendo más de su criterio que de la ley.

El asunto tiene un perfil propio cuando la parte es una persona jurídica. La compañía genera y custodia correspondencia institucional, actas

societarias, registros contables y documentos con firma electrónica, y su actuación en juicio descansa en sistemas informáticos y en plataformas estatales de validación que, por sí solos, no garantizan la trazabilidad que exige el principio de contradicción. Quien litiga contra ella rara vez tiene acceso a esos sistemas.

De ahí la pregunta que guía el estudio: ¿hasta qué punto la regulación de la prueba digital en entornos virtuales prevista en el COGEP garantiza el principio de contradicción, el derecho a la defensa y la seguridad jurídica en los procesos que involucran a sociedades mercantiles? El objetivo general es analizar esa regulación y su incidencia en dichas garantías en los procesos con sociedades mercantiles. Los objetivos específicos son: (i) examinar el régimen de admisibilidad, impugnación y valoración de la prueba digital en el COGEP, en relación con la Constitución, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y la normativa societaria; (ii) identificar las limitaciones de ese régimen frente a la prueba digital corporativa; y (iii) formular y validar una propuesta de articulado de reforma.

El trabajo es cualitativo y jurídico-documental. Combina el método dogmático, la exégesis de las normas procesales y societarias y una comparación funcional con Colombia, China y España, elegidos porque dan tres respuestas distintas al mismo problema: la valoración indiciaria, la trazabilidad tecnológica y los servicios electrónicos de confianza. Como se verá, la debilidad del modelo ecuatoriano no está en el reconocimiento legal de la prueba digital, sino en la falta de reglas que obliguen a exhibir el archivo original y sus metadatos cuando la prueba se impugna. El propósito es ofrecer a legisladores, jueces y abogados una propuesta de reforma concreta, que concilie la

celeridad de los entornos virtuales con las garantías del debido proceso.

Materiales y Métodos

La investigación es cualitativa, de tipo jurídico-documental y alcance descriptivo-analítico. Siguiendo a Álvarez (2002) se adoptó una perspectiva dogmática que parte del derecho positivo para interpretarlo, sistematizarlo y valorarlo, complementada con la exégesis de las normas y con la interpretación hermenéutica y sistemática propia de la investigación jurídica (Pozo et al., 2022). La selección de fuentes fue intencional. En un estudio de este tipo la representatividad estadística no es un requisito; lo que se exige es que las fuentes sean pertinentes, verificables y suficientes para responder la pregunta.

Se aplicaron cuatro criterios: vigencia, es decir, normativa en vigor a 2025 y, para doctrina y jurisprudencia, el período posterior a la expedición del COGEP en 2015, salvo obras metodológicas y leyes de referencia; pertinencia, porque solo se incluyeron fuentes sobre autenticidad, integridad, impugnación o valoración de la evidencia electrónica; jerarquía, con prioridad para normas de rango legal, decisiones de altas cortes y artículos de revistas arbitradas; y verificabilidad, que llevó a descartar textos sin autoría identificable o sin acceso al texto completo.

El corpus normativo comprende la Constitución de la República del Ecuador (2008), el COGEP (2015), la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002), la Ley de Compañías (1999), la Ley Orgánica de Protección de Datos Personales (2021), el Código Orgánico Integral Penal (2014), como referente de cadena de custodia, y la regulación de juntas generales de la Superintendencia de Compañías, Valores y Seguros (2025). El

jurisprudencial reúne el criterio no vinculante No. 171-2020-P-CPJP-YG de la Corte Nacional de Justicia y decisiones de altas cortes extranjeras sobre capturas de pantalla, correos electrónicos, mensajería y evidencia verificada con hash o blockchain. El doctrinal se compone de artículos científicos, tesis de posgrado y obras especializadas. El análisis se ordenó en seis categorías: autenticidad, integridad, autoría, cadena de custodia, contradicción (entendida como acceso efectivo al soporte original y a los metadatos) y valoración judicial. La comparación siguió el método funcional, que no equipara instituciones por su nombre sino

por el problema que resuelven, y usó tres variables: (V1) reconocimiento y valor probatorio de la evidencia electrónica; (V2) mecanismos de autenticación y trazabilidad; y (V3) reglas de impugnación y prueba pericial. Colombia comparte con Ecuador la tradición continental y adoptó la Ley Modelo de la CNUDMI sobre comercio electrónico; España ha influido en la dogmática procesal ecuatoriana y aplica el régimen europeo de servicios de confianza; China se incluyó como caso de máxima diferencia, por sus tribunales de internet. La Tabla 1 resume la ruta seguida.

Tabla 1. Matriz de coherencia metodológica.

Objetivo específico	Fuentes	Método	Hallazgo
(i) Examinar el régimen de la prueba digital en el COGEP	Constitución (arts. 76, 82, 168); COGEP (arts. 158, 160, 164, 165, 196, 202, 203, 221-227); LCE; criterio CNJ 171-2020	Dogmático y exegético	No hay deber de exhibir el soporte original ni cadena de custodia en materia no penal
(ii) Identificar las limitaciones frente a la prueba corporativa	Ley de Compañías; Resolución SCVS-INC-DNCDN-2025-0001; LOPDP; doctrina	Exegético y crítica doctrinal	Asimetría en el acceso a servidores y metadatos; alcance limitado del hash y de la firma electrónica
(iii) Formular y validar una propuesta de reforma	Normas y sentencias de Colombia, China y España	Comparado funcional y validación argumentativa	Cuatro disposiciones y matriz de validación (Tabla 3)

Fuente: Elaboración propia.

Resultados y Discusión

La prueba digital es el dato o conjunto de datos generados, almacenados o transmitidos por dispositivos o sistemas electrónicos que se incorporan al proceso para acreditar hechos relevantes; su soporte es inmaterial y depende de infraestructura tecnológica para producirse, conservarse y recuperarse (Navas y Vázquez Martínez, 2025, pág. 7). Abarca correos, mensajes, imágenes, audio, video, metadatos, bases de datos y registros de sistemas corporativos (Echavarría et al., 2023, págs. 14-15). Puetate et al. (2021) añaden que su validez depende de la autenticidad, la autoría, la integridad y la accesibilidad, y que el juez la aprecia según la sana crítica. El punto de partida es constitucional. La Constitución de la República del Ecuador (2008) reconoce el

derecho a presentar pruebas y a contradecir las que se presenten en contra (art. 76, numeral 7, literal h), garantiza la seguridad jurídica (art. 82) y somete la sustanciación de los procesos al principio de contradicción (art. 168, numeral 6). El COGEP (2015) desarrolla esas garantías: fija la finalidad de la prueba (art. 158), declara ineficaz la actuada sin oportunidad de contradecir (art. 160), ordena valorarla en conjunto según la sana crítica (art. 164) y reconoce el derecho a conocerla y contradecirla (art. 165). Para la prueba documental regula su producción en audiencia (art. 196), los documentos digitales (art. 202) y la impugnación de firma o autoría (art. 203); para la pericial, la actuación de peritos acreditados por el Consejo de la Judicatura (arts. 221 a 227). En cuanto al soporte electrónico, el artículo 14

de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) equipara la firma electrónica a la manuscrita, y el artículo 202 del COGEP considera originales los documentos producidos electrónicamente y da a sus reproducciones digitalizadas la misma fuerza probatoria. Ninguna de las dos normas acredita por sí sola la autoría, que debe probarse conforme a las reglas procesales. La Corte Nacional de Justicia, en el criterio no vinculante No. 171-2020-P-CPJP-YG, de 25 de enero de 2021, admitió conversaciones de WhatsApp autenticadas ante notario como base de un procedimiento monitorio, siempre que cumplan exigencias de autenticidad, integridad y relevancia, y advirtió que su sola presentación no garantiza su eficacia (Quirola & Carrera, 2025).

Estas reglas permiten impugnar la prueba digital, pero dejan sin resolver cuatro cuestiones de las que depende que la contradicción sea efectiva. Nada obliga a quien aporta un archivo electrónico a conservarlo en su formato nativo y a exhibir sus metadatos si la contraparte lo impugna, de modo que el debate suele girar en torno a impresiones o capturas. La cadena de custodia está regulada en el Código Orgánico Integral Penal (2014, art. 456), pero no existe un estándar equivalente para los procesos no penales, donde son los propios litigantes quienes obtienen y guardan la evidencia.

El artículo 203 del COGEP está pensado para impugnar la firma o la autoría, no la alteración del contenido o de los metadatos, que es el riesgo típico de la evidencia electrónica. Y no se prevé qué ocurre si la parte se niega a entregar el soporte original, ni quién asume el costo del peritaje informático. Las compañías litigan como empleadoras, contratantes y socias, y en cada uno de esos frentes la prueba es electrónica. Los conflictos entre socios por

convocatorias, exclusiones o nulidad de resoluciones se discuten con actas de juntas documentadas digitalmente; los incumplimientos contractuales, con correos y mensajes; los conflictos laborales, con contratos, comunicaciones y actas de finiquito digitales. Si se impugnan los correos institucionales, los contratos electrónicos, los registros contables de un sistema ERP o las actas firmadas electrónicamente, lo procedente es un peritaje sobre servidores, bitácoras de acceso y metadatos.

La reforma al reglamento de juntas generales acentuó esa dependencia. Mediante la Resolución No. SCVS-INC-DNCDN-2025-0001, la Superintendencia de Compañías, Valores y Seguros (2025) permitió que socios y accionistas elijan asistir de forma presencial o virtual, sin que pueda imponerse una modalidad. La prueba de la convocatoria, del quórum y del voto en una junta mixta descansa ahora en registros de conexión, grabaciones y actas electrónicas que conserva la propia compañía. Si un socio impugna los acuerdos conforme a la Ley de Compañías (1999), la información que necesita está en manos de su contraparte.

Abrir esos sistemas puede, a su vez, exponer información reservada de la empresa y datos personales de trabajadores, clientes o proveedores protegidos por la Ley Orgánica de Protección de Datos Personales (2021). La salida no es negar el acceso sino delimitarlo: el examen puede practicarse sobre una copia forense bajo custodia judicial, restringido a los metadatos y registros vinculados con el hecho controvertido, por un perito acreditado que guarde reserva sobre lo ajeno al litigio. Un caso frecuente es el acta de finiquito validada con código hash en el Sistema Único de Trabajo. El hash funciona como una huella: permite

detectar si el archivo cambió después de generado, pero no acredita quién lo elaboró ni si su contenido es veraz (Gobierno del Ecuador, 2026). El blockchain tampoco resuelve la cuestión, porque su registro distribuido asegura la trazabilidad de la información desde que ingresa, no su veracidad previa (Tapscott & Tapscott, 2017). El Tribunal Supremo Popular de China (2018) admite la evidencia verificada con estas técnicas solo si se demuestra la fiabilidad del procedimiento que la generó y la conservó. Trasladado a Ecuador, un código hash no exime al juez de revisar el soporte original, los metadatos y los registros del sistema, ni de ordenar un peritaje si la prueba se impugna.

Para Taruffo (2008, como se citó en Meneses, 2009), una prueba que no ha podido ser refutada carece de valor. En entornos virtuales, refutar exige algo más que mirar una captura de pantalla: hace falta acceder al soporte original y a los metadatos que muestran su procedencia. Ortiz-Nivela et al. (2025) señalan que la captura, por sí sola, carece de metadatos, huellas del archivo, registros del servidor o certificaciones que permitan descartar alteraciones, y por eso no puede recibir el mismo peso que el documento electrónico original.

Nieva Fenoll (2018) cuestiona las reglas tradicionales de carga de la prueba y propone que la decisión se apoye en la prueba efectivamente disponible. La idea encaja aquí, porque con frecuencia una parte no tiene los medios técnicos para impugnar un archivo que controla la otra. Avemañay et al. (2025) y Vines (2023) coinciden en que la sana crítica no basta cuando faltan estándares mínimos de integridad y autenticidad, como la verificación de metadatos, el sellado de tiempo o el uso de funciones hash. En Colombia, los artículos 9 a

11 de la Ley 527 (1999) reconocen la integridad, la admisibilidad y la fuerza probatoria de los mensajes de datos. La Corte Constitucional de Colombia (2020), en la Sentencia T-043 de 2020, dio a las capturas de pantalla de WhatsApp valor de indicio, por la facilidad con que pueden alterarse, y exigió valorarlas junto con los demás medios de prueba. La Sentencia T-238 de 2022 reiteró ese criterio y añadió que el envío de un correo no prueba por sí solo su recepción ni el conocimiento de su contenido (Corte Constitucional de Colombia, 2022). La Corte Suprema de Justicia de Colombia (2019), en la Sentencia SL5246 de 2019, aceptó correos electrónicos que permitían identificar procedencia, destinatario y fecha.

China optó por la verificación tecnológica a través de los tribunales de internet de Hangzhou, Beijing y Guangzhou. El artículo 11 de las disposiciones del Tribunal Supremo Popular de China (2018) admite firmas electrónicas, sellos de tiempo, funciones hash y blockchain para comprobar la integridad de la información, siempre que se acredite la fiabilidad del procedimiento. Según González-García (2025), la contradicción se ejerce allí impugnando tanto el contenido como el procedimiento técnico de captura y conservación.

En España, la Ley 1/2000 de Enjuiciamiento Civil (2000) reconoce en sus artículos 299.2 y 382 a 384 los medios de reproducción de la palabra, el sonido y la imagen y los instrumentos de archivo de datos. La Sala Segunda de lo Penal del Tribunal Supremo de España (2015), en la Sentencia 300/2015, advirtió sobre la posible manipulación de las comunicaciones digitales y sostuvo que, impugnada su autenticidad, corresponde acreditarla a quien pretende valerse de ellas,

normalmente mediante pericia; aunque el criterio es penal, sirve para cualquier proceso. La Ley 6/2020 modificó el artículo 326 de la Ley de Enjuiciamiento Civil para presumir auténticos e íntegros los documentos que usan servicios de confianza cualificados. Ninguno

de los tres modelos resta valor a la prueba por su formato, pero los tres condicionan su eficacia a que pueda verificarse su origen e integridad. Ecuador reconoce la prueba digital y carece todavía de esas reglas de verificación (Tabla 2).

Tabla 2. Comparación según las variables V1 a V3

Variable	Colombia	China	España	Ecuador
V1. Reconocimiento y valor probatorio	Equivalencia funcional (Ley 527, arts. 9-11); capturas con valor de indicio (T-043/20; T-238/22)	Admitida si se acredita la fiabilidad de su generación y conservación	Medios de reproducción y archivo de datos (LEC, arts. 299.2 y 382-384)	Documento electrónico equiparado al original (COGEP, art. 202); sin regla sobre capturas
V2. Autenticación y trazabilidad	Integridad y confiabilidad del mensaje de datos; firma digital	Firmas electrónicas, sellos de tiempo, hash y blockchain	Presunción para servicios de confianza cualificados (Ley 6/2020; LEC, art. 326)	Firma electrónica y hash en plataformas estatales; sin cadena de custodia no penal
V3. Impugnación y pericia	Valoración conjunta; el envío no prueba la recepción (T-238/22)	Se impugna el contenido y el procedimiento técnico	Impugnada, prueba quien aporta; pericial indispensable (STS 300/2015)	Impugnación de firma o autoría (art. 203); sin deber de exhibir el soporte ni regla de costos

Fuente: Elaboración propia.

Manobanda y Cárdenas (2023) ya plantearon la necesidad de reformas que fijen criterios de admisibilidad y práctica de la evidencia electrónica. ¿Por qué no basta con reforzar las reglas de la prueba documental? Porque descansan en la distinción entre original y copia y en la firma como signo de autoría, y ninguna de las dos funciona bien con evidencia electrónica: la copia digital es idéntica al original, la información es volátil y su autenticidad depende de metadatos externos al documento visible. Además, mucha prueba digital no es documental, como las bitácoras de un servidor o los metadatos de una grabación. La propuesta da a la prueba digital reglas propias, pero las inserta a continuación del artículo 202 del COGEP y las remite a las normas generales de admisibilidad, valoración y pericia, sin crear un procedimiento nuevo.

Art. 202.1.- Prueba digital. Es prueba digital todo dato generado, almacenado o transmitido por medios electrónicos que se incorpore al proceso para acreditar un hecho controvertido. Quien la anuncie identificará su fuente y el sistema de origen, y conservará

el archivo en su formato nativo con sus metadatos hasta que concluya el proceso. Las impresiones, capturas de pantalla y transcripciones son representaciones de la prueba digital; si no se acompaña el archivo original o este no puede verificarse, valdrán como indicio y se apreciarán con los demás medios de prueba.

Art. 202.2.- Cadena de custodia digital. Quien aporte prueba digital documentará su obtención, extracción, transferencia y almacenamiento en un registro que incluya el valor hash del archivo y la fecha, hora y responsable de cada actuación. La falta de este registro no excluye por sí sola la prueba, pero se considerará al valorar su integridad.

Art. 202.3.- Impugnación de la prueba digital. La parte contra quien se presente una prueba digital podrá impugnar fundadamente su autenticidad, integridad o autoría en la oportunidad prevista para oponerse a la admisión de la prueba. Admitida la impugnación, quien aportó la prueba pondrá a disposición el soporte original y sus

metadatos. Si no lo hace sin causa justificada, la prueba solo podrá valorarse como indicio.

Art. 202.4.- Peritaje informático y protección de la información. La o el juzgador, de oficio o a petición de parte, podrá disponer un peritaje informático a cargo de perito acreditado por el Consejo de la Judicatura, que se practicará sobre una copia forense bajo custodia judicial, se limitará a los datos necesarios para verificar

el hecho controvertido y guardará reserva sobre la información de terceros y los secretos empresariales. Los honorarios los anticipará quien solicite la pericia y los reembolsará quien aportó la prueba si se comprueba su alteración. Si la parte impugnante acredita falta de recursos, el peritaje podrá practicarse a través del sistema pericial de la Función Judicial. La propuesta se contrastó con siete criterios derivados del análisis normativo, doctrinal y comparado; la Tabla 3 sintetiza los resultados.

Tabla 3. *Validación argumentativa y documental de la propuesta*

Criterio	Justificación y respaldo
1. Adecuación constitucional	Desarrolla el derecho a contradecir la prueba (art. 76.7.h) y el principio de contradicción (art. 168.6); aporta reglas previas y claras (art. 82).
2. Coherencia sistemática	Se inserta tras el art. 202 y remite a los arts. 160, 164, 203 y 221-227; no crea procedimientos ni órganos.
3. Viabilidad institucional	Usa peritos acreditados por el Consejo de la Judicatura y una cadena de custodia ya conocida en materia penal (COIP, art. 456).
4. Igualdad procesal	Obliga a exhibir el soporte a quien controla la información (Nieva Fenoll, 2018; Ortiz-Nivela et al., 2025).
5. Protección de datos	Copia forense bajo custodia judicial, limitada al hecho controvertido y con reserva de datos de terceros (LOPD, 2021).
6. Costos periciales	Anticipo de quien pide la pericia, reembolso si hay alteración y alternativa pública ante falta de recursos.
7. Respaldo comparado	Valor indiciario de las capturas (Colombia); fiabilidad del procedimiento técnico (China); carga y pericial ante impugnación (España).

Fuente: Elaboración propia.

Los resultados confirman que el problema del derecho ecuatoriano no es el reconocimiento de la prueba digital, que existe, sino la ausencia de un régimen técnico para obtenerla, conservarla y discutirla. Esa ausencia no invalida la evidencia, pero deja al juez la tarea de decidir, caso por caso, cuánto exigir.

La comparación muestra caminos distintos (valoración indiciaria en Colombia, trazabilidad tecnológica en China, presunciones ligadas a servicios de confianza en España) con un punto en común: la eficacia de la prueba depende de que pueda verificarse. Coincidimos con Vines (2023) y Avemañay et al. (2025) en que el reconocimiento jurídico es insuficiente sin estándares de preservación e inspección. Ortiz-Nivela et al. (2025) muestran que, sin acceso al

soporte original, surge una asimetría entre quien presenta la evidencia y quien la impugna, y esa asimetría crece si se aplican con rigidez las reglas de carga de la prueba (Nieva Fenoll, 2018). En los procesos societarios el desequilibrio es mayor, porque la compañía controla los servidores, las plataformas de juntas virtuales y los sistemas contables.

Una firma electrónica o un código hash prueban ciertas propiedades del archivo, pero no su autoría ni su veracidad. El riesgo que se identifica no es una supuesta contradicción entre sentencias, sino el margen de valoración que dejan la falta de reglas técnicas y el carácter no vinculante del criterio de la Corte Nacional. Ese margen permite que dos jueces resuelvan de forma distinta casos semejantes, y es

precisamente lo que el articulado propuesto busca acotar.

Conclusiones

El COGEP y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos equiparan el documento electrónico al original y la firma electrónica a la manuscrita, y el COGEP ofrece reglas generales de admisibilidad, contradicción, impugnación y pericia. Falta, sin embargo, el deber de conservar y exhibir el archivo original con sus metadatos, así como una cadena de custodia digital para los procesos no penales. Sin ellos, la autenticidad queda librada a la sana crítica o a soluciones externas al proceso, como la autenticación notarial.

La contradicción se resiente menos en la admisión de la prueba que en la posibilidad práctica de controvertirla. El problema se agudiza con las capturas de pantalla y en los procesos con sociedades mercantiles, cuya evidencia reside en sistemas que controla una sola de las partes. El código hash demuestra que un archivo no cambió desde su registro y la firma electrónica tiene equivalencia legal, pero ninguno acredita por sí solo la autoría o la veracidad del contenido; el blockchain tampoco. Del derecho comparado pueden tomarse tres aportes: el valor indiciario de las capturas (Colombia), la trazabilidad técnica verificable (China) y las presunciones ligadas a servicios de confianza cualificados (España).

Se proponen cuatro disposiciones a continuación del artículo 202 del COGEP sobre la prueba digital y sus representaciones, la cadena de custodia, la impugnación con exhibición del soporte y el peritaje con protección de la información. La validación argumentativa indica que son compatibles con la Constitución y con el COGEP, aplicables con

la estructura pericial actual y favorables a la igualdad procesal.

Referencias Bibliográficas

- Álvarez, G. (2002). Metodología de la investigación jurídica: hacia una nueva perspectiva. Universidad Central de Chile, Facultad de Ciencias Jurídicas y Sociales. Obtenido de <https://bibliotecavirtualceug.wordpress.com/wp-content/uploads/2017/05/doc.pdf>
- Avemañay, S., Avemañay, A., & Duarte, M. (2025). La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica. *Ciencia Latina Revista Científica Multidisciplinar*, 9(5), 17880-17900. https://doi.org/10.37811/cl_rcm.v9i6.21212
- Código Orgánico General de Procesos. (2015). Registro Oficial Suplemento 506, 22 de mayo de 2015. Asamblea Nacional del Ecuador. <https://www.ces.gob.ec/lotaip/2023/Marzo/A2/C%C3%B3digo%20Org%C3%A1nico%20General%20de%20Procesos.pdf>
- Código Orgánico Integral Penal. (2014). Registro Oficial Suplemento 180, 10 de febrero de 2014. Asamblea Nacional del Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/07/COIP_a_ct_jun-2021.pdf
- Constitución de la República del Ecuador. (2008). Registro Oficial 449, 20 de octubre de 2008. Asamblea Constituyente. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
- Corte Constitucional de Colombia. (13 de febrero de 2020). Sentencia T-043/20. <https://www.corteconstitucional.gov.co/relatoria/2020/t-043-20.htm>
- Corte Constitucional de Colombia. (30 de Agosto de 2022). Sentencia T-238/22. Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2022/t-238-22.htm>

- Corte Suprema de Justicia de Colombia. (02 de Diciembre de 2019). SL5246-2019. Bogotá. Obtenido de <https://www.cortesuprema.gov.co/corte/wp-content/uploads/2020/06/SL5246-2019-2.pdf>
- Echavarría, U., Dueñas, L., & Guerrero, N. (2023). Aportación y valoración de la prueba digital desde la garantía de los derechos fundamentales. Obtenido de Universidad Cooperativa De Colombia: <https://repository.ucc.edu.co/server/api/core/bitstreams/7fed225d-2156-4c20-a05a-6f3af542cbcb/content>
- Gobierno del Ecuador. (2026). Registro de actas de finiquito. Ministerio de Trabajo. <https://www.gob.ec/mt/tramites/registro-actas-finiquito>
- González, T. (2025). Implementación de blockchain en el sistema judicial público y en los sistemas de resolución alternativa de disputas. *Revista de los Estudios de Derecho y Ciencia*, 1-12. Obtenido de <https://dialnet.unirioja.es/descarga/articulo/10129993.pdf>
- Herrera, S. (2025). El papel de la prueba digital en los procedimientos penales en Ecuador. Obtenido de Universidad Andina Simón Bolívar, Maestría en Derecho Penal: <https://repositorio.uasb.edu.ec/bitstream/10644/10524/1/T4605-MDPE-Herrera-El%20papel.pdf>
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (2000). Boletín Oficial del Estado, 7, de 8 de enero de 2000. BOE-A-2000-323. <https://www.boe.es/buscar/act.php?id=BOE-A-2000-323>
- Ley 527 de 1999. (1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial No. 43.673, 21 de agosto de 1999. Congreso de la República de Colombia. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276>
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. (2020). Boletín Oficial del Estado, 298, de 12 de noviembre de 2020. BOE-A-2020-14046. <https://www.boe.es/buscar/act.php?id=BOE-A-2020-14046>
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002). Registro Oficial Suplemento 557, 17 de abril de 2002. Congreso Nacional del Ecuador. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf>
- Ley de Compañías. (1999). Codificación. Registro Oficial 312, 5 de noviembre de 1999. Congreso Nacional del Ecuador. <https://www.supercias.gob.ec/portalscv/Institucion/SectorSocietario.php?seccion=ley-de-compa%C3%B1ias>
- Ley Orgánica de Protección de Datos Personales. (2021). Registro Oficial Quinto Suplemento 459, 26 de mayo de 2021. Asamblea Nacional del Ecuador. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf>
- Manobanda, D., & Cárdenas, K. (2023). La prueba documental frente al principio de contradicción en el Código Orgánico General de Procesos, en Ecuador. *Revista Metropolitana de Ciencias Aplicadas*, 6(1), 64-74. <https://www.redalyc.org/articulo.oa?id=721778122009>
- Meneses, C. (2009). La prueba. *Ius et Praxis*, 15(1), 449-452. <https://www.scielo.cl/pdf/iusetp/v15n1/art20.pdf>
- Navas Abad, C., & Vázquez Martínez, D. (2025). La importancia de la prueba digital en los procedimientos penales en Ecuador. *Polo del Conocimiento*, 10(1), 1742-1775. <https://doi.org/10.23857/pc.v10i1.8778>
- Nieva Fenoll, J. (2018). La carga de la prueba: una reliquia histórica que debería ser abolida. *Revista Ítalo-española De Derecho Procesal*, 1, 129-146. Obtenido de <https://www.revistasmarcialpons.es/rivitsproc/article/view/la-carga-de-la-prueba-una-reliquia-historica-que-debeira-ser-abo>

- Ortiz, M., Vega, L., & García, H. (2025). Insuficiente regulación de la prueba digital y su valoración en el proceso penal. 593 Digital Publisher CEIT, 10(4), 1057-1070. <https://doi.org/10.33386/593dp.2025.4.3399>
- Pozo, D., Méndez-Cabrita, C., Jacho-Villalba, M., & Portilla-Obando, P. (2022). La hermenéutica jurídica como instrumento de interpretación de la legislación ecuatoriana. Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, 7(2), 773-783. <https://doi.org/10.35381/racji.v7i2.2166>
- Puetate, J., Coka, D., & Méndez, C. (2021). La prueba digital en procesos judiciales aplicables al Código Orgánico General de Procesos (COGEP), a partir de la pandemia COVID-19. Revista Dilemas Contemporáneos: Educación, Política y Valores, 8(17). <https://doi.org/10.46377/dilemas.v8i.2696>
- Quirola, N., & Carrera, G. (2025). Análisis jurídico de los documentos digitales como medios de prueba en el COGEP y su precisión probatoria. Ciencia y Educación, 6(9.3), 210-226. Obtenido de <https://cienciayeducacion.com/index.php/journal/article/view/zenodo.18125118/2325>
- Ramírez, C. (2017). Apuntes sobre la prueba en el COGEP. Obtenido de Corte Nacional de Justicia: https://www.cortenacional.gob.ec/cnj/images/Produccion_CNJ/La%20prueba%20en%20el%20COGEP.pdf
- Sala Segunda de lo Penal del Tribunal Supremo de España. (19 de Mayo de 2015). STS 300/2015. <https://vlex.es/vid/571257698>
- Superintendencia de Compañías, Valores y Seguros. (2025). Resolución No. SCVS-INC-DNCDN-2025-0001, de 7 de marzo de 2025, que reforma el reglamento sobre juntas generales de socios y accionistas. <https://www.supercias.gob.ec/portalscvs/Noticias/Noticias.php?seccion=noticia-07042025>
- Tapscott, D., & Tapscott, A. (2017). La revolución blockchain: descubre cómo esta nueva tecnología transformará la economía global (J. M. Salmerón, Trad.). Ediciones Deusto.
- https://proassets.planetadelibros.cl/usuarios/libros_contenido/arxius/35/34781_La_revolucion_blockchain.pdf
- Tribunal Supremo Popular de China. (06 de Septiembre de 2018). The Supreme People's Court's Provisions on Several Issues Related to Trial of Cases by the Internet Courts. Obtenido de <https://www.chinalawtranslate.com/en/the-supreme-peoples-courts-provisions-on-several-issues-related-to-trial-of-cases-by-the-internet-courts/>
- Vinces, R. (2023). La aplicación de la cadena de custodia y su incidencia en la prueba digital dentro de los delitos informáticos en la legislación ecuatoriana. Obtenido de Universidad Ecotec, Facultad de Derecho y Gobernabilidad: <https://repositorio.ecotec.edu.ec/handle/123456789/621>



Esta obra está bajo una licencia de Creative Commons Reconocimiento-No Comercial 4.0 Internacional. Copyright © Andrea Carolina Arce Oñate, Gilda Cecilia Herrera Herrera y Holger Geovanny García Segarra.

Declaraciones éticas y editoriales del artículo

Contribución de los autores (Taxonomía CRediT)

Andrea Carolina Arce Oñate: 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.

Gilda Cecilia Herrera Herrera: 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.

Holger Geovanny García Segarra: 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.

