

La valoración de la prueba electrónica en los procesos judiciales ecuatorianos: desafíos y garantías procesales

The Assessment of Electronic Evidence in Ecuadorian Judicial Proceedings: Challenges and Procedural Guarantees

Autores:

Luis Alfredo Ponce Cañarte, ORCID: <https://orcid.org/0009-0006-3174-2738>. Correo: luisalfredo.ponce@unesum.edu.ec

Vilma Veronica Manrique Merchan, Correo: verito2074@hotmail.com

Afiliación institucional: Universidad Estatal del Sur de Manabí

***Autor, correo para correspondencia:** luisalfredo.ponce@unesum.edu.ec

Resumen

La progresiva digitalización de las relaciones sociales, económicas y jurídicas ha provocado que una parte creciente de los hechos sometidos a conocimiento judicial se encuentre documentada mediante mensajes de datos, correos electrónicos, conversaciones mantenidas a través de aplicaciones de mensajería instantánea, archivos digitales, fotografías, videos, registros informáticos y otros contenidos generados o almacenados electrónicamente. Esta transformación plantea dificultades particulares para el derecho probatorio, pues el reconocimiento jurídico de un documento electrónico no determina, por sí mismo, su fuerza probatoria en un caso concreto. El presente artículo analiza el régimen jurídico aplicable a la valoración de la prueba electrónica en Ecuador, con especial atención a las condiciones de licitud, autenticidad, integridad, fiabilidad, contradicción y motivación judicial. La investigación se desarrolló bajo un enfoque cualitativo, mediante un diseño documental y jurídico-dogmático, basado en el análisis de la Constitución de la República del Ecuador, el Código Orgánico General de Procesos, el Código Orgánico Integral Penal, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la jurisprudencia y los criterios institucionales relevantes, así como la literatura jurídica especializada. Los resultados evidencian que el ordenamiento ecuatoriano reconoce ampliamente la prueba electrónica, pero distribuye su regulación entre distintos cuerpos normativos y establece tratamientos diferenciados entre los procesos sometidos al Código Orgánico General de Procesos y al proceso penal. Se concluye que la valoración de la prueba electrónica no puede reducirse a la mera visualización de una captura de pantalla o de un archivo digital, sino que exige examinar conjuntamente su licitud, procedencia, autenticidad, integridad, contexto, fiabilidad técnica y posibilidad efectiva de contradicción. En materia penal, estas exigencias se intensifican mediante las reglas sobre técnicas forenses digitales y la cadena de custodia.

Palabras clave: Prueba electrónica; prueba digital; valoración probatoria; debido proceso; autenticidad; integridad; cadena de custodia

Abstract

The progressive digitalization of social, economic, and legal relations has resulted in an increasing number of facts submitted to judicial proceedings being documented through data messages, emails, instant messaging conversations, digital files, photographs, videos, computer records, and other electronically generated or stored content. This transformation poses particular challenges for evidence law because the legal recognition of an electronic document does not, by itself, determine its evidentiary weight in a specific case. This article analyzes the legal framework for assessing electronic evidence in Ecuador, with particular attention to legality, authenticity, integrity, reliability, adversarial examination, and judicial reasoning. The research followed a qualitative approach and a documentary and legal-dogmatic design based on the analysis of the Constitution of the Republic of Ecuador, the General Organic Code of Proceedings, the Comprehensive Organic Criminal Code, the Electronic Commerce, Electronic Signatures and Data Messages Act, relevant case law and institutional criteria, as well as specialized legal literature. The findings show that Ecuadorian law broadly recognizes electronic evidence but distributes its regulation among different legal instruments and treats proceedings governed by the General Organic Code of

Proceedings and criminal proceedings differently. Assessing electronic evidence cannot be reduced to merely viewing a screenshot or digital file. Courts must jointly examine its legality, provenance, authenticity, integrity, context, technical reliability, and the opposing party's effective opportunity to challenge it. In criminal proceedings, these requirements become stricter under rules governing digital forensic techniques and the chain of custody.

Keywords: Electronic evidence; digital evidence; evidence assessment; due process; authenticity; integrity; chain of custody

Información del manuscrito:

Fecha de recepción: 10 de julio de 2026

Fecha de aceptación: 21 de julio de 2026

Fecha de publicación: 29 de julio de 2026

Introducción

La utilización cotidiana de tecnologías digitales ha modificado sustancialmente la forma en que las personas producen, transmiten y conservan información. Una conversación contractual puede desarrollarse mediante WhatsApp; una relación laboral puede documentarse a través de correos electrónicos; una transferencia bancaria deja registros informáticos; una cámara de seguridad registra acontecimientos relevantes para un proceso penal; y una fotografía o video captado mediante un teléfono móvil puede constituir posteriormente un elemento determinante dentro de una controversia judicial. El proceso judicial contemporáneo se enfrenta, por tanto, a una realidad en la que los hechos ya no se documentan exclusivamente mediante soportes físicos.

La prueba electrónica presenta características que la distinguen de la documentación tradicional. Puede ser copiada sin pérdida aparente de calidad, modificada mediante herramientas informáticas, almacenada simultáneamente en

distintos dispositivos, transmitida a terceros, sincronizada con servicios remotos o acompañada de información técnica que no resulta perceptible mediante la simple observación del archivo. Tales particularidades obligan a distinguir entre la información visible para el usuario y los elementos técnicos que pueden contribuir a establecer su procedencia, integridad y autenticidad.

La doctrina especializada ha advertido, precisamente, que la evidencia digital presenta dificultades particulares relacionadas con su volatilidad, fragilidad, posibilidad de alteración y la dependencia de procedimientos técnicos adecuados para su recuperación y conservación. En consecuencia, la confiabilidad de esta evidencia se relaciona estrechamente con la forma en que fue obtenida, preservada y examinada (Lone & Mir, 2019). Estudios más recientes insisten en que la cadena de custodia y la trazabilidad continúan siendo componentes relevantes para garantizar que la evidencia presentada posteriormente ante

una autoridad judicial corresponda a la obtenida originalmente (Nath et al., 2024).

El ordenamiento jurídico ecuatoriano reconoce, desde hace más de dos décadas, la eficacia jurídica de la información electrónica. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos estableció expresamente que los mensajes de datos tienen el mismo valor jurídico que los documentos escritos (art. 2) y reguló posteriormente su utilización como medios probatorios (art. 52) (2002). Este reconocimiento fue posteriormente complementado por el Código Orgánico General de Procesos (COGEP), que incorporó reglas específicas sobre los documentos digitales, y por el Código Orgánico Integral Penal (COIP), que reguló el contenido digital y estableció condiciones particulares para su recuperación, conservación, análisis y valoración.

Sin embargo, reconocer jurídicamente un documento electrónico no equivale a afirmar que cualquier representación digital aportada al expediente acredita automáticamente los

hechos que contiene. Este constituye uno de los problemas centrales de la prueba electrónica. Una captura de pantalla, por ejemplo, puede permitir visualizar una conversación, pero de ella no necesariamente se desprende, sin elementos adicionales, quién controlaba determinada cuenta, si la conversación está completa, si fue modificada, de qué archivo procede o si la información fue obtenida respetando derechos fundamentales.

En consecuencia, es necesario distinguir tres dimensiones que con frecuencia se confunden: admisibilidad, autenticidad y valoración. La primera se relaciona con la posibilidad jurídica de incorporar un determinado elemento al proceso; la segunda, con la correspondencia entre lo que se presenta y lo que se afirma que representa; y la tercera, con la fuerza que razonablemente puede atribuirse al elemento probatorio al momento de reconstruir los hechos controvertidos.

Esta distinción encuentra fundamento constitucional. El artículo 76 numeral 4 de la

Constitución de la República (2008) dispone que las pruebas obtenidas o actuadas con violación de la Constitución o de la ley carecen de validez y eficacia probatoria. Paralelamente, el numeral 7, literal h, del mismo artículo garantiza el derecho de las partes a presentar pruebas y a contradecir las formuladas en su contra, mientras que el literal l establece la garantía de motivación de las decisiones públicas (Asamblea Constituyente del Ecuador, 2008). De esta manera, el tratamiento de la prueba electrónica se encuentra directamente vinculado al debido proceso.

La dimensión constitucional adquiere una importancia aún mayor cuando la obtención de evidencia tecnológica afecta comunicaciones privadas o información personal. El artículo 66 numerales 19, 20 y 21 de la Constitución (2008) reconoce, respectivamente, los derechos a la protección de datos personales, a la intimidad personal y familiar y a la inviolabilidad y al secreto de la correspondencia física y virtual. El numeral 21 determina que esta

última no puede ser retenida, abierta ni examinada sino en los casos legalmente previstos, previa intervención judicial, protegiendo, además, cualquier otra forma de comunicación (Asamblea Constituyente del Ecuador, 2008). La utilidad probatoria de una comunicación electrónica no elimina, por tanto, los límites constitucionales existentes respecto de su obtención.

En el ámbito procesal no penal, el COGEP contiene una regla especialmente importante. En el artículo 202 (COGEP, 2015) determina que los documentos producidos electrónicamente con sus respectivos anexos son considerados originales para todos los efectos legales y reconoce igual fuerza probatoria a las reproducciones digitalizadas o escaneadas incorporadas al expediente electrónico, sin perjuicio de la obligación de conservar determinados originales y presentarlos cuando sean requeridos. La misma disposición permite admitir como medio de prueba contenido digital conforme a las normas del Código (Asamblea Nacional del Ecuador,

2015).

En materia penal, las exigencias son más específicas. Los artículos 456 y 457 del COIP (2014) relacionan la valoración de determinados elementos con su autenticidad, legalidad y cadena de custodia, mientras que el artículo 500 establece reglas expresas para el contenido digital. Esta disposición exige que el análisis, la recuperación, la valoración y la presentación del contenido almacenado en dispositivos o sistemas informáticos se realicen mediante técnicas digitales forenses y dispone medidas específicas destinadas a preservar su integridad.

La existencia de estas disposiciones demuestra que el ordenamiento ecuatoriano no parte de un vacío absoluto. El problema radica más bien en la articulación de normas provenientes de distintos cuerpos jurídicos y en la necesidad de establecer criterios coherentes para determinar qué debe comprobar el juzgador antes de otorgar fuerza probatoria a un elemento electrónico.

Investigaciones recientes

realizadas en Ecuador coinciden en identificar dificultades prácticas. Imaicela Revilla y Alvarado Ajila (2024) señalan que la incorporación de la evidencia digital plantea retos en materia de seguridad jurídica y de tratamiento procesal. Quichimbo Roman et al. (2024) destacan la necesidad de analizar cuidadosamente los criterios de admisibilidad y valoración establecidos por el COGEP. En el ámbito penal, Ortiz-Nivela et al. (2025) identifican dificultades relacionadas con la autenticación y seguridad de la prueba digital. Asimismo, Arteaga Yepez et al. (2026) sostienen que, aunque el artículo 202 del COGEP (2015) constituye un reconocimiento normativo importante, continúan existiendo problemas relacionados con la verificación y valoración de la evidencia digital.

A partir de estos antecedentes, el objetivo general de esta investigación es analizar el régimen jurídico de valoración de la prueba electrónica en los procesos judiciales ecuatorianos, identificando sus principales desafíos técnicos y jurídicos, así como las garantías procesales

necesarias para asegurar su utilización compatible con el debido proceso.

La hipótesis jurídica que orienta el análisis sostiene que el sistema ecuatoriano contiene bases normativas suficientes para reconocer la prueba electrónica, pero su eficacia probatoria no depende únicamente de su formato digital ni de su incorporación formal al expediente, sino de una valoración integral que considere licitud, autenticidad, integridad, fiabilidad, contexto, contradicción y motivación, con exigencias adicionales de preservación forense y cadena de custodia cuando resulte aplicable el régimen penal.

Materiales y métodos

La investigación se desarrolló con un enfoque cualitativo, ya que su objeto no consistió en medir estadísticamente el uso de la evidencia electrónica, sino en interpretar las normas, principios y criterios jurídicos que regulan su incorporación y valoración en el sistema judicial ecuatoriano. Este enfoque resulta adecuado cuando el propósito de la investigación se orienta a comprender e interpretar fenómenos a partir del análisis de sus características, significados y

contextos, antes que a su cuantificación mediante variables numéricas (Hernández-Sampieri & Mendoza Torres, 2018). En este sentido, la naturaleza del problema investigado exigió examinar el contenido y alcance de las disposiciones jurídicas aplicables a la prueba electrónica y establecer su relación con las garantías procesales reconocidas por el ordenamiento jurídico ecuatoriano.

El diseño de la investigación fue documental y jurídico-dogmático. La investigación documental permitió recopilar, seleccionar y examinar fuentes normativas, jurisprudenciales, institucionales y doctrinales relacionadas con la prueba electrónica. A su vez, el método jurídico-dogmático permitió identificar, interpretar y sistematizar el contenido de las normas aplicables, así como establecer relaciones entre disposiciones constitucionales, procesales y especiales. Este tipo de investigación constituye una de las formas características de producción de conocimiento jurídico, pues parte del análisis del derecho vigente, de sus conceptos, normas y relaciones internas con el propósito de ofrecer una reconstrucción sistemática y jurídicamente fundamentada del

objeto estudiado (Courtis, 2006).

De esta manera, el análisis no se limitó a describir las normas existentes, sino que buscó determinar cómo deben articularse para establecer los criterios jurídicos que orientan la admisión y valoración de la prueba electrónica en los procesos judiciales ecuatorianos.

Las principales fuentes normativas examinadas fueron la Constitución de la República del Ecuador; el Código Orgánico General de Procesos; el Código Orgánico Integral Penal; y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. La selección normativa respondió a su relación directa con la admisibilidad, la práctica, la autenticidad y la valoración de la información electrónica en procesos judiciales.

Se analizaron especialmente los artículos 66 y 76 de la Constitución (2008); 160, 164, 165, 193 y 202 del COGEP (2015); 456, 457, 498, 499 y 500 del COIP (2014); y 2, 7, 8 y 52 a 55 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002). Así como de jurisprudencia complementaria.

La revisión doctrinal priorizó investigaciones jurídicas recientes

sobre prueba digital en Ecuador y estudios especializados sobre integridad, autenticidad y cadena de custodia. La información obtenida fue organizada en categorías analíticas: reconocimiento jurídico, admisibilidad, licitud, autenticidad, integridad, conservación, contradicción, valoración, cadena de custodia y motivación.

El estudio no realizó entrevistas, encuestas ni experimentos técnicos sobre dispositivos electrónicos. Por ello, sus resultados deben interpretarse como conclusiones derivadas del análisis jurídico-documental y no como una medición empírica del comportamiento de todos los órganos jurisdiccionales ecuatorianos.

Resultados

Reconocimiento jurídico de la prueba electrónica en Ecuador

El primer resultado permite establecer que el sistema jurídico ecuatoriano reconoce expresamente la eficacia jurídica de la información generada electrónicamente. El artículo 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos dispone que los mensajes de datos tienen el mismo

valor jurídico que los documentos escritos y que su eficacia, valoración y efectos se rigen por dicha ley y su reglamento (2002).

Esta disposición incorpora un principio de equivalencia funcional: la información no pierde valor jurídico únicamente por encontrarse en formato electrónico. En consecuencia, la ausencia de soporte físico no constituye, por sí sola, una razón suficiente para excluir un contenido determinado.

El artículo 52 de la misma ley (LCEFEMD, 2002) desarrolla esta regla en el ámbito probatorio y reconoce como medios de prueba los mensajes de datos, las firmas electrónicas, los documentos electrónicos y los certificados electrónicos nacionales o extranjeros emitidos conforme a la ley.

La reforma de 2021 actualizó la referencia procesal contenida en esta disposición, vinculando la valoración y efectos legales con el Código Orgánico General de Procesos. Esta actualización resulta jurídicamente relevante porque la redacción original remitía al derogado Código de Procedimiento Civil.

El COGEP consolida este reconocimiento mediante el artículo

202 (2015). Los documentos producidos electrónicamente, con sus anexos, se consideran originales para todos los efectos legales. Adicionalmente, las reproducciones digitalizadas o escaneadas incorporadas al expediente electrónico tienen la misma fuerza probatoria que el original, aunque el titular debe conservar determinados documentos originales para presentarlos en audiencia o cuando sean requeridos judicialmente (Asamblea Nacional del Ecuador, 2015).

Por tanto, el ordenamiento ecuatoriano supera una concepción exclusivamente material del documento. La condición documental depende de su capacidad para recoger, contener o representar hechos o incorporar derechos, y no exclusivamente del papel utilizado como soporte.

Admisibilidad y valoración no constituyen categorías equivalentes

El segundo resultado consiste en que la normativa obliga a diferenciar la admisión de una prueba electrónica de la fuerza probatoria que posteriormente se le atribuya.

El artículo 160 del COGEP (2015) exige pertinencia, utilidad y

conducencia y dispone que la prueba sea practicada conforme a la ley, con lealtad y veracidad. Además, establece la improcedencia de la prueba obtenida con violación de la Constitución o la ley y niega eficacia probatoria a aquella obtenida mediante simulación, dolo, fuerza o soborno, así como a la prueba actuada sin oportunidad de contradicción (Asamblea Nacional del Ecuador, 2015). En consecuencia, el hecho de que una captura de pantalla, correo electrónico, fotografía o archivo pueda conceptualmente constituir un medio probatorio no significa que deba necesariamente ser admitido ni, una vez admitido, que posea suficiente fuerza para demostrar el hecho controvertido.

El artículo 164 del COGEP (2015) añade que la prueba debe apreciarse conjuntamente conforme a las reglas de la sana crítica y obliga al juzgador a expresar en su resolución la valoración de aquellas pruebas utilizadas para justificar su decisión. La valoración de evidencia electrónica debe insertarse, por tanto, en el razonamiento probatorio general. No existe una regla según la cual el formato digital produzca automáticamente plena prueba. El

documento electrónico debe relacionarse con los demás elementos existentes y someterse al razonamiento judicial.

Autenticidad e integridad como problemas centrales

La autenticidad responde esencialmente a la pregunta de si el elemento presentado corresponde efectivamente a aquello que la parte afirma que es. La integridad, en cambio, se relaciona con la conservación del contenido sin alteraciones relevantes.

La Ley de Comercio Electrónico contiene criterios importantes para resolver ambas cuestiones. Su artículo 7 establece que, cuando la legislación exija información original, el requisito puede cumplirse mediante un mensaje de datos si puede comprobarse que la información ha conservado su integridad desde que fue generada definitivamente (LCEFEMD, 2002). La norma considera íntegro el mensaje cuando su contenido permanece completo e inalterado, exceptuando modificaciones propias del proceso de comunicación, archivo o presentación.

El artículo 8 complementa esta
201

regla al regular la conservación (LCEFEMD,2002). Para que el archivo satisfaga las exigencias legales, la información debe permanecer accesible para consulta posterior, conservarse en su formato original o en uno capaz de reproducirla exactamente y mantener los datos que permitan determinar origen, destino, fecha y hora de creación, procesamiento, envío, recepción y archivo.

Estas disposiciones adquieren particular importancia ante mensajes instantáneos y capturas de pantalla. Una imagen de una conversación muestra determinado contenido, pero puede no contener por sí sola todos los datos disponibles en el dispositivo o sistema original. De ahí que la valoración deba considerar las circunstancias concretas de autenticación. No puede establecerse como regla universal que toda captura sea inválida, pero tampoco puede presumirse automáticamente su autenticidad cuando esta ha sido razonablemente controvertida.

La Corte Nacional de Justicia abordó una cuestión relacionada en su absolución de consulta de 25 de enero de 2021 sobre conversaciones

de WhatsApp utilizadas para acreditar una deuda en procedimiento monitorio en el oficio N.º 0120-AJ-P-CNJ-2021. El criterio institucional reconoció la posibilidad de utilizar documentos electrónicos dentro del régimen probatorio aplicable, vinculándolos con las disposiciones del COGEP sobre documentos electrónicos (Corte Nacional de Justicia, 2021). Por tratarse de una absolución de consulta, el criterio no tiene carácter vinculante, pero demuestra que el soporte tecnológico no excluye por sí mismo la aptitud probatoria.

Firma electrónica y presunción de autenticidad

No toda prueba electrónica presenta el mismo nivel de certeza técnica. La Ley de Comercio Electrónico establece un tratamiento específico para la firma electrónica certificada.

El artículo 53 dispone que cuando se presenta como prueba una firma electrónica certificada por una entidad de certificación de información acreditada se presume que cumple los requisitos legales, que sus datos no han sido alterados desde su emisión y que pertenece al signatario (LCEFEMD, 2002).

Esta presunción diferencia jurídicamente un documento firmado electrónicamente mediante mecanismos legalmente reconocidos de una simple imagen, captura de pantalla o archivo cuya autoría se encuentre controvertida.

El artículo 54 regula además la práctica de esta prueba (LCEFEMD, 2002). Entre otras reglas, contempla la presentación del soporte informático y de los elementos necesarios para lectura y verificación cuando sean requeridos y permite que, ante la impugnación de una firma o certificado electrónico, se obtenga información de la entidad de certificación correspondiente. Por consiguiente, el sistema no trata de manera idéntica todas las manifestaciones de evidencia electrónica. La existencia de mecanismos técnicos verificables puede incrementar razonablemente su fiabilidad.

Fiabilidad técnica como criterio de valoración

El artículo 55 de la Ley de Comercio Electrónico (2002) dispone que la prueba debe valorarse atendiendo a la seguridad y fiabilidad de los medios mediante los cuales fue enviada, recibida, verificada,

almacenada o comprobada, sin excluir otros métodos aconsejados por la técnica y la tecnología.

Esta disposición es particularmente significativa porque introduce una dimensión tecnológica dentro del razonamiento judicial. La valoración no se limita al contenido visible del archivo: puede requerir analizar el procedimiento mediante el cual fue generado, conservado o verificado.

Ello no significa que toda prueba electrónica necesite obligatoriamente un peritaje informático. Una regla de esa naturaleza no se desprende del COGEP. La necesidad de intervención pericial dependerá de la controversia concreta y de si el conocimiento técnico especializado resulta necesario para establecer autenticidad, alteración, procedencia u otras circunstancias relevantes. Sin embargo, cuando existe una impugnación técnicamente sustentada sobre manipulación, origen o integridad, la simple observación judicial puede resultar insuficiente para resolver cuestiones que exigen conocimientos especializados.

La contradicción como
garantía indispensable

El artículo 165 del COGEP (2015) reconoce expresamente a las partes el derecho a conocer oportunamente las pruebas, oponerse fundamentadamente y contradecirlas. Esta garantía reproduce, en el plano legal, el contenido del artículo 76 numeral 7 literal h de la Constitución (2008).

En prueba electrónica, la contradicción requiere algo más que permitir a la contraparte observar una imagen durante la audiencia. Debe existir una posibilidad real de cuestionar aquello que fundamenta su credibilidad. Cuando la controversia recaiga sobre la autenticidad, la parte debe poder discutir el origen del archivo, su integridad, la identidad atribuida a sus participantes, el contexto de la conversación, los mecanismos de obtención y, cuando corresponda, las conclusiones de un perito.

La contradicción adquiere especial relevancia cuando únicamente se aporta una selección de mensajes. La valoración aislada de fragmentos puede modificar el sentido de una comunicación. Por

ello, el contexto constituye una variable probatoria relevante.

Licitud y derechos
fundamentales

La obtención de evidencia electrónica presenta un límite constitucional insoslayable. El artículo 76 numeral 4 de la Constitución establece que las pruebas obtenidas o actuadas vulnerando la Constitución o la ley carecen de validez y eficacia probatoria (2008).

Esta regla debe interpretarse conjuntamente con los derechos del artículo 66 (Constitución del Ecuador, 2008). La protección de datos personales, intimidad y secreto de las comunicaciones impide sostener que cualquier información tecnológicamente accesible puede ser utilizada judicialmente sin considerar cómo fue obtenida.

La prueba electrónica obliga así a distinguir accesibilidad tecnológica de licitud jurídica. Que una persona pueda técnicamente ingresar a una cuenta, copiar una conversación, acceder a un dispositivo o recuperar determinado archivo no significa necesariamente que se encuentre jurídicamente autorizada para hacerlo. En materia

penal esta cuestión es particularmente sensible porque las actuaciones investigativas estatales se encuentran sometidas a garantías constitucionales y reglas legales específicas. La búsqueda de la verdad no habilita métodos probatorios contrarios a derechos fundamentales.

Régimen especial de la prueba digital en materia penal

El COIP (2014) desarrolla un sistema más detallado para la evidencia digital, el artículo 498 reconoce como medios de prueba el documento, el testimonio y la pericia, mientras el artículo 499 establece reglas generales para la prueba documental y permite expresamente admitir contenido digital conforme a las normas del Código.

El artículo 456 dispone que la cadena de custodia se aplica a elementos físicos o contenido digital materia de prueba para garantizar su autenticidad, identidad y estado original, documentando las personas y condiciones relacionadas con su recolección, envío, manejo, análisis y conservación (COIP, 2014).

El artículo 457 complementa esta disposición al señalar que la valoración debe considerar la

legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios utilizados en los informes periciales (COIP, 2014). La misma norma establece que la demostración de autenticidad de elementos probatorios o evidencia física no sometidos a cadena de custodia corresponde a la parte que los presenta.

En ese marco, la cadena de custodia no debe interpretarse únicamente como una formalidad documental. Su finalidad es permitir reconstruir el recorrido del elemento y demostrar que aquello examinado y posteriormente presentado conserva una relación verificable con aquello inicialmente obtenido.

El artículo 500 del COIP y las técnicas digitales forenses

El artículo 500 constituye una de las disposiciones más relevantes del régimen ecuatoriano (COIP, 2014). Tras su reforma de 2023, define el contenido digital como todo dato informático que representa hechos, información o conceptos de la realidad, almacenado, procesado o transmitido mediante medios tecnológicos susceptibles de tratamiento informático.

La disposición determina que el análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos debe realizarse mediante técnicas digitales forenses.

También diferencia entre contenido almacenado en sistemas o memorias volátiles y aquel contenido existente en medios no volátiles, pero en ambos casos exige técnicas digitales forenses destinadas a preservar la integridad y contempla la aplicación de cadena de custodia.

Finalmente, cuando durante una investigación, registro o allanamiento se recolecta un medio físico capaz de almacenar, procesar o transmitir contenido digital, el COIP exige identificar e inventariar individualmente el objeto, fijar su ubicación física, protegerlo mediante técnicas digitales forenses y trasladarlo bajo cadena de custodia a un centro especializado (Asamblea Nacional del Ecuador, 2014).

Este tratamiento confirma una diferencia fundamental entre el régimen general del COGEP y el penal: mientras el primero reconoce ampliamente documentos y contenidos digitales bajo las reglas generales de admisibilidad,

contradicción y sana crítica, el segundo establece obligaciones técnicas específicas para la investigación de contenido digital.

Discusión

Los resultados permiten afirmar que el problema principal de la prueba electrónica en Ecuador no consiste en determinar si jurídicamente puede existir. Esa discusión ha sido superada por la legislación. Tanto la Ley de Comercio Electrónico como el COGEP y el COIP reconocen expresamente información y documentos digitales como posibles medios probatorios.

La cuestión contemporánea es más compleja: determinar bajo qué condiciones un elemento electrónico merece credibilidad suficiente para fundamentar una decisión judicial.

Esta distinción resulta necesaria porque la facilidad con la que actualmente puede generarse, copiarse, editarse o reenviarse contenido digital modifica los riesgos probatorios. Lone y Mir (2019) destacan que la evidencia digital puede ser frágil, volátil y susceptible de alteración, lo que convierte a la autenticidad e integridad en aspectos fundamentales de su tratamiento. Nath et al. (2024) coinciden en señalar que la cadena de custodia

constituye un mecanismo esencial para mantener la confiabilidad de evidencia digital a lo largo de su ciclo de vida.

En el contexto ecuatoriano, la prueba electrónica plantea dificultades que trascienden su simple incorporación al proceso judicial. El problema central se encuentra en determinar bajo qué condiciones un elemento digital puede generar suficiente confianza para ser utilizado como fundamento de una decisión. La facilidad con la que determinados contenidos pueden ser reproducidos, modificados o presentados de manera fragmentada obliga a prestar especial atención a su procedencia, autenticidad e integridad. A ello se suma la necesidad de diferenciar las exigencias aplicables según la naturaleza del proceso, pues el tratamiento de la evidencia digital no es idéntico en materia penal y en los procesos regulados por el COGEP. En consecuencia, el desafío no radica únicamente en admitir estos nuevos medios de prueba, sino en establecer criterios de valoración que permitan aprovechar su utilidad sin disminuir las garantías del debido proceso, especialmente el derecho a la contradicción y la exigencia de una

decisión judicial debidamente motivada.

No obstante, debe evitarse concluir que la existencia de dificultades técnicas equivale automáticamente a una ausencia total de regulación. El ordenamiento ecuatoriano contiene un conjunto significativo de reglas. El verdadero problema es su dispersión y la necesidad de interpretarlas sistemáticamente.

De esta investigación se desprende que la valoración puede estructurarse mediante siete criterios jurídicos interrelacionados:

Criterio	Contenido y aplicación en la valoración de la prueba electrónica	Fundamento normativo
----------	--	----------------------

Licitud Antes de valorar el contenido de la evidencia electrónica debe determinarse si fue obtenida y actuada respetando la Constitución y la ley. La vulneración de derechos o garantías durante su obtención puede afectar su validez y eficacia probatoria. Constitución de la República del Ecuador, art. 76, núm. 4.

Autenticidad Implica determinar si el elemento electrónico corresponde realmente al origen, autor, dispositivo, comunicación o

hecho que se le atribuye. No supone que todo documento electrónico requiera necesariamente certificación notarial o peritaje, pero sí que existan elementos suficientes para sustentar razonablemente su procedencia.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, arts. 7, 8 y 53; COIP, arts. 456 y 457, cuando corresponda.

Integridad Exige determinar si la información se ha mantenido completa y sin alteraciones que afecten su contenido relevante. Su análisis puede considerar la conservación del mensaje y los datos disponibles sobre su origen, destino, fecha, hora y almacenamiento.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, arts. 7 y 8.

Fiabilidad técnica La valoración debe considerar la seguridad y confiabilidad de los procedimientos utilizados para enviar, recibir, verificar, conservar o almacenar la información. En materia penal adquiere especial importancia el empleo de técnicas digitales forenses para el tratamiento del contenido digital. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 55; COIP, art. 500.

Contexto El contenido electrónico debe examinarse atendiendo a las circunstancias en las que fue producido. Un mensaje o fragmento aislado puede adquirir un significado distinto al analizarse dentro de la conversación, secuencia o conjunto documental al que pertenece. COGEP, art. 164: valoración conjunta de la prueba conforme a las reglas de la sana crítica.

Contradicción efectiva
Las partes deben disponer de una oportunidad real para conocer y cuestionar la evidencia electrónica, incluyendo su contenido, procedencia, autenticidad, forma de obtención y, cuando corresponda, los procedimientos y conclusiones técnicas empleados para verificarla.

Constitución de la República del Ecuador, art. 76, núm. 7, lit. h; COGEP, art. 165.

Motivación de la valoración
El juzgador debe explicar las razones por las cuales atribuye determinado valor a la evidencia electrónica y su relación con los demás elementos probatorios. Cuando la prueba digital sea controvertida y resulte relevante para la decisión, la motivación debe permitir comprender las razones que

justifican su credibilidad y peso probatorio. Constitución de la República del Ecuador, art. 76, núm. 7, lit. I; COGEP, art. 164.

Nota. Elaboración propia a partir del análisis de la Constitución de la República del Ecuador (2008), el Código Orgánico General de Procesos (COGEP, 2015), el Código Orgánico Integral Penal (COIP, 2014) y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002). Los criterios expuestos constituyen una sistematización analítica de las disposiciones examinadas y no una enumeración establecida expresamente bajo estas siete categorías por una única norma jurídica.

Otro aspecto que merece discusión es la utilización frecuente de capturas de pantalla. La captura constituye una representación visual y puede ser procesalmente útil, pero su valor dependerá de las circunstancias del caso. No existe fundamento normativo para sostener que toda captura sea automáticamente inválida; tampoco existe base jurídica para afirmar que toda captura demuestra necesariamente la autenticidad del contenido representado.

Cuando no existe controversia razonable sobre su origen y el contenido se encuentra corroborado por otros elementos, puede contribuir al convencimiento judicial. En cambio, cuando se cuestionan específicamente la autoría, integridad o manipulación, puede ser necesario acudir a elementos adicionales de autenticación. Esta aproximación evita dos extremos igualmente problemáticos: un formalismo que excluya toda evidencia electrónica que no venga acompañada de peritaje y una confianza acrítica que considere auténtica cualquier imagen presentada al expediente.

También debe diferenciarse entre procesos sujetos al COGEP y procesos penales. Trasladar automáticamente las exigencias de cadena de custodia penal a cualquier controversia civil, laboral o contencioso-administrativa carecería de sustento normativo. El COGEP utiliza un modelo basado en admisibilidad, contradicción y sana crítica. En cambio, el COIP contiene reglas expresas sobre cadena de custodia y técnicas forenses.

Ello no significa que la integridad carezca de relevancia fuera del ámbito penal. Significa que el mecanismo jurídico para

demostrarla puede variar según la materia. Finalmente, la evolución tecnológica intensifica el problema. Las herramientas de edición digital y generación artificial de contenidos aumentan la necesidad de analizar procedencia y autenticidad. El sistema probatorio no puede responder a este fenómeno mediante una presunción general de falsedad de todo contenido digital, porque ello neutralizaría medios de prueba legítimos. La respuesta jurídicamente adecuada consiste en fortalecer los mecanismos de autenticación y elevar el rigor de la valoración cuando existan motivos concretos para cuestionar la fiabilidad.

Conclusiones

El análisis realizado permite concluir que el ordenamiento jurídico ecuatoriano cuenta con bases suficientes para reconocer y utilizar la prueba electrónica dentro de los procesos judiciales. Sin embargo, su creciente presencia en las controversias judiciales plantea la necesidad de superar una visión centrada únicamente en su admisión y prestar mayor atención a las condiciones que permiten atribuirle un determinado valor probatorio. La naturaleza digital de un elemento no garantiza por sí misma su

confiabilidad, del mismo modo que tampoco constituye una razón suficiente para cuestionar su validez.

Uno de los principales hallazgos de la investigación es que la admisibilidad y la valoración de la prueba electrónica deben entenderse como cuestiones diferenciadas. Que un mensaje, correo electrónico, archivo, fotografía, video o captura de pantalla pueda incorporarse al proceso no significa necesariamente que resulte suficiente para acreditar el hecho discutido. Su fuerza probatoria dependerá de las circunstancias particulares del caso y, especialmente, de la posibilidad de establecer razonablemente su procedencia, autenticidad, integridad y contexto.

Asimismo, se considera que la licitud debe constituir el punto de partida para el tratamiento de cualquier evidencia electrónica. El desarrollo tecnológico amplía las posibilidades de acceder, almacenar y recuperar información, pero estas capacidades técnicas no pueden justificar afectaciones a derechos fundamentales. La obtención de información digital debe mantenerse dentro de los límites del debido proceso y respetar especialmente la intimidad, la protección de datos

personales, el secreto de las comunicaciones y el derecho de las partes a ejercer una defensa efectiva.

La investigación también permite identificar a la autenticidad y la integridad como dos de los mayores desafíos de la prueba electrónica. La facilidad con la que determinados contenidos digitales pueden copiarse, modificarse, reenviarse o presentarse parcialmente obliga a que su valoración no se limite a observar aquello que aparece en una pantalla. Cuando existan cuestionamientos razonables sobre su origen o conservación, será necesario acudir a mecanismos adicionales que permitan verificar su confiabilidad, cuya intensidad dependerá de la naturaleza de la evidencia y de la controversia planteada.

En este sentido, no se considera adecuado establecer como regla general que toda prueba electrónica requiera necesariamente un peritaje informático. Una exigencia de esta naturaleza podría generar formalismos innecesarios y dificultar la utilización de medios probatorios legítimos. No obstante, cuando la controversia se refiera específicamente a una posible alteración, manipulación, autoría o

procedencia del contenido, la intervención técnica especializada puede adquirir especial relevancia para proporcionar al juzgador elementos suficientes para adoptar una decisión razonada.

En materia penal, la preservación de la evidencia adquiere una importancia particularmente elevada debido a las consecuencias que pueden derivarse del proceso. La trazabilidad del contenido digital y la utilización adecuada de procedimientos forenses contribuyen no solamente a fortalecer la investigación, sino también a garantizar que la persona procesada pueda conocer y cuestionar las condiciones en las que la evidencia fue obtenida, preservada y analizada. Por ello, las exigencias técnicas deben entenderse también como garantías procesales y no únicamente como procedimientos propios de la investigación informática.

Respecto de las capturas de pantalla, se concluye que no resulta jurídicamente adecuado atribuirles de manera anticipada un valor absoluto. Su utilización debe analizarse atendiendo a las circunstancias particulares del proceso. Una captura puede constituir un elemento

relevante cuando su contenido resulta coherente con otros medios de prueba y no existen cuestionamientos razonables sobre su procedencia; sin embargo, su fuerza probatoria puede disminuir cuando se presenta de manera fragmentada, carece de contexto o existen objeciones justificadas sobre su autenticidad. La valoración debe evitar tanto la aceptación automática como el rechazo generalizado de este tipo de evidencia.

A partir del estudio realizado, se considera que uno de los principales desafíos del sistema ecuatoriano se encuentra en la dispersión de las reglas aplicables a la prueba electrónica. Existen disposiciones que permiten responder jurídicamente a buena parte de los problemas identificados, pero se encuentran distribuidas entre diferentes cuerpos normativos y responden a las particularidades de distintas materias procesales. Esta situación puede dificultar la construcción de criterios uniformes frente a problemas tecnológicos semejantes. Por ello, una interpretación sistemática basada en licitud, autenticidad, integridad, fiabilidad, contexto, contradicción y motivación puede contribuir a

proporcionar mayor coherencia a su valoración judicial.

La motivación judicial constituye, finalmente, una garantía especialmente relevante frente a este tipo de prueba. Cuando un elemento electrónico resulte determinante para resolver una controversia, no debería ser suficiente afirmar que su contenido acredita determinado hecho. La decisión debe permitir comprender por qué ese elemento fue considerado confiable, qué relación mantiene con las demás pruebas y de qué manera fueron examinadas las objeciones formuladas por las partes. La dimensión tecnológica de la prueba no sustituye el razonamiento judicial; por el contrario, puede exigir una justificación particularmente cuidadosa cuando existan controversias sobre su confiabilidad.

En cuanto a las limitaciones del estudio, debe señalarse que la investigación tuvo carácter jurídico-documental, por lo que se concentró en el análisis normativo, doctrinal e institucional de la prueba electrónica y no incorporó una investigación empírica sobre la totalidad de decisiones emitidas por los órganos jurisdiccionales ecuatorianos. Tampoco se realizaron entrevistas a

jueces, fiscales, abogados o peritos informáticos. Estas limitaciones no afectan los resultados derivados del análisis jurídico realizado, pero delimitan su alcance y permiten reconocer que la aplicación práctica de estas reglas puede presentar particularidades que requieren estudios específicos.

Como futuras líneas de investigación, resulta pertinente profundizar en el análisis jurisprudencial de la prueba electrónica mediante muestras sistemáticas de decisiones judiciales ecuatorianas, con el propósito de determinar los criterios que efectivamente utilizan los juzgadores para establecer su autenticidad y fuerza probatoria. También sería relevante estudiar comparativamente el tratamiento de las capturas de pantalla, conversaciones de WhatsApp, correos electrónicos, publicaciones en redes sociales y registros provenientes de plataformas digitales, pues cada uno presenta problemas técnicos y jurídicos particulares. Finalmente, el desarrollo de contenidos generados o modificados mediante inteligencia artificial abre una línea de investigación especialmente relevante sobre autenticación de

evidencia, deepfakes, trazabilidad digital y estándares probatorios necesarios para diferenciar contenidos auténticos de aquellos creados o manipulados artificialmente.

Bibliografía

Arteaga Yopez, E. V., Cuenca Mina, B. E., & García Segarra, H. G. (2026). La prueba digital en el proceso civil ecuatoriano: ¿Estamos preparados jurídicamente? *Revista Lex*, 9(32).
<https://doi.org/10.33996/revistalex.v9i32.460>

Asamblea Constituyente del Ecuador. (2008). Constitución de la República del Ecuador. Registro Oficial No. 449, 20 de octubre de 2008. Texto reformado.

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Suplemento del Registro Oficial No. 180, 10 de febrero de 2014. Última reforma: Cuarto Suplemento del Registro Oficial No. 275, 29 de abril de 2026.

Asamblea Nacional del Ecuador. (2015). Código Orgánico General de Procesos. Suplemento del Registro Oficial No. 506, 22 de mayo de 2015. Texto vigente consultado con reformas registradas

hasta el Registro Oficial No. 340, 4 de agosto de 2026.

Congreso Nacional del Ecuador. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Suplemento del Registro Oficial No. 557, 17 de abril de 2002. Última reforma: Quinto Suplemento del Registro Oficial No. 525, 27 de agosto de 2021.

Corte Nacional de Justicia. (2021). Absolución de consulta: Prueba por medio de documentos electrónicos (WhatsApp) (Oficio No. 0120-AJ-P-CNJ-2021, 25 de enero de 2021). Presidencia de la Corte Nacional de Justicia.

Courtis, C. (Coord.). (2006). Observar la ley: Ensayos sobre metodología de la investigación jurídica. Editorial Trotta.
<https://dialnet.unirioja.es/servlet/libro?codigo=10654&utm>

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill Education.
<https://bibliotecadigital.uce.edu.ec/s/L-D/item/1946?utm>

Imaicela Revilla, J. A., & Alvarado Ajila, L. A. (2024). La incorporación de la prueba digital en

el derecho procesal ecuatoriano. Revista Lex, 7(27), 1338–1350.
<https://doi.org/10.33996/revistalex.v7i27.247>

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55.
<https://doi.org/10.1016/j.diin.2019.01.002>

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 11–20). IEEE.

Ortiz-Nivela, M. N., Vega-Pila, L. E., & García-Segarra, H. G. (2025). Insuficiente regulación de la prueba digital y su valoración en el proceso penal. 593 Digital Publisher CEIT.
<https://doi.org/10.33386/593dp.2025.4.3399>

Quichimbo Roman, M. A., Mereci Balcazar, L. S., & Ramón Merchán, M. E. (2024). La admisibilidad de la prueba digital en los procesos judiciales incorporados

en el Código Orgánico General de
Procesos. Dominio de las Ciencias,
10(3), 1126–1142.
<https://doi.org/10.23857/dc.v10i3.397>
2mortem en el Ecuador y su
valoración probatoria. *ASCE*
Magazine, 4(3), 2054-2083.