

La prueba digital en la investigación de delitos contra la administración pública

Digital evidence in the investigation of crimes against public administration

Alex Paúl Martínez Once*
Universidad Bolivariana del Ecuador
Riobamba - Ecuador
a_p_m11@hotmail.com
<https://orcid.org/0009-0000-2418-3487>

Hillary Patricia Herrera Avilés
Universidad Nacional de Chimborazo
Riobamba - Ecuador
hillary.herrera@unach.edu.ec
<https://orcid.org/0009-0003-1514-2247>

Juan Fernando Tapia Sanchez
Función Judicial
Riobamba - Ecuador
juan.tapias@funcionjudicial.gob.ec
<https://orcid.org/0009-0006-8582-0762>

***Correspondencia:**
a_p_m11@hotmail.com

Cómo citar este artículo:
Martínez, A., Herrera, H., & Tapia, J. (2026). La prueba digital en la investigación de delitos contra la administración pública. *Esprint Investigación*, 5(2), 94-107. <https://doi.org/10.61347/ei.v5i2.352>

Recibido: 1 de junio de 2026
Aceptado: 9 de julio de 2026
Publicado: 17 de julio de 2026

Copyright: Derechos de autor 2026 Alex Paúl Martínez Once, Hillary Patricia Herrera Avilés, Juan Fernando Tapia Sanchez.



Esta obra está bajo una licencia internacional Creative Commons Atribución-NonComercial 4.0.

Resumen: La incorporación de la tecnología en las actividades sociales, institucionales y jurídicas ha transformado los mecanismos mediante los cuales se generan, almacenan y utilizan los datos, convirtiendo la información digital en un elemento relevante dentro de los procesos judiciales. En este contexto, la prueba digital se ha consolidado como un elemento probatorio fundamental para la investigación y acreditación de hechos delictivos, incluidos aquellos relacionados con la administración pública. El presente estudio tuvo como objetivo analizar la relevancia jurídica y probatoria de la prueba digital en la investigación de delitos contra la administración pública mediante una revisión documental de enfoque jurídico y cualitativo, orientada a examinar las principales conductas delictivas, las fuentes de evidencia digital y el marco normativo aplicable en Ecuador. Los resultados evidencian que delitos como peculado, cohecho, concusión, prevaricato y enriquecimiento ilícito generan rastros digitales susceptibles de análisis mediante correos electrónicos, comunicaciones electrónicas, registros institucionales, documentos digitales y otros recursos tecnológicos. Sin embargo, la eficacia probatoria de estos elementos depende de garantizar su autenticidad, integridad, trazabilidad y adecuada cadena de custodia durante las etapas de obtención, preservación y valoración. El análisis normativo demuestra que Ecuador cuenta con disposiciones constitucionales, legales y técnicas que permiten sustentar el uso de evidencia digital; no obstante, persisten desafíos relacionados con la ausencia de procedimientos específicos y uniformes para su tratamiento. Se concluye que la prueba digital constituye una herramienta indispensable en la investigación de delitos contra la administración pública, siempre que su aplicación combine criterios jurídicos y técnicos que aseguren su confiabilidad y respeto a las garantías procesales.

Palabras clave: Cadena de custodia, corrupción pública, evidencia electrónica, justicia penal, transparencia institucional.

Abstract: The incorporation of technology into social, institutional, and legal activities has transformed the mechanisms through which data are generated, stored, and used, making digital information a relevant element within judicial proceedings. In this context, digital evidence has become a fundamental evidentiary element for the investigation and substantiation of criminal acts, including those related to public administration. This study aimed to analyze the legal and evidentiary relevance of digital evidence in the investigation of crimes against public administration through a documentary review with a legal and qualitative approach, focused on examining the main criminal offenses, the sources of digital evidence, and the applicable regulatory framework in Ecuador. The results show that crimes such as embezzlement, bribery, extortion by public officials, judicial misconduct, and illicit enrichment generate digital traces that can be analyzed through emails, electronic communications, institutional records, digital documents, and other technological resources. However, the evidentiary effectiveness of these elements depends on ensuring their authenticity, integrity, traceability, and proper chain of custody throughout the stages of collection, preservation, and assessment. The regulatory analysis demonstrates that Ecuador has constitutional, legal, and technical provisions that support the use of digital evidence; nevertheless, challenges remain regarding the absence of specific and uniform procedures for its handling. It is concluded that digital evidence constitutes an essential tool in the investigation of crimes against public administration, provided that its application integrates legal and technical criteria that ensure its reliability and respect for procedural guarantees.

Keywords: Chain of custody, criminal justice, electronic evidence, institutional transparency, public corruption.

1. Introducción

Los servidores públicos, en el ejercicio de las atribuciones y competencias conferidas por el ordenamiento jurídico, están sujetos a diferentes tipos de responsabilidades cuando sus actuaciones se apartan de las disposiciones legales y reglamentarias vigentes. Estas conductas pueden generar consecuencias de naturaleza fiscal, penal, administrativa-disciplinaria y civil, dependiendo de la gravedad del incumplimiento y del perjuicio ocasionado (Ortega, 2020). En este marco, los mecanismos de control institucional, transparencia y rendición de cuentas adquieren especial relevancia para prevenir irregularidades y garantizar una gestión pública orientada al interés colectivo, conforme a los principios establecidos en la Ley Orgánica de la Contraloría General del Estado (2002) y el Código Orgánico Administrativo [COA] (2017).

En este contexto, los delitos contra la administración pública representan una problemática de especial relevancia, debido a que afectan la transparencia institucional, debilitan la confianza ciudadana y generan impactos negativos en la gestión estatal y el desarrollo económico (Risco & Herrera, 2025). Por ello, los sistemas de control público y acceso a la información constituyen herramientas esenciales para fortalecer la vigilancia ciudadana y la prevención de prácticas contrarias a la integridad administrativa (Ley Orgánica de Transparencia y Acceso a la Información Pública [LOTAIP], 2004).

Dentro del proceso judicial, la prueba constituye un elemento esencial para demostrar la existencia de hechos jurídicamente relevantes y proporcionar al juzgador fundamentos objetivos para la toma de decisiones. Su eficacia depende del cumplimiento de principios relacionados con la legalidad, pertinencia, admisibilidad y respeto al debido proceso, garantizando el derecho a la defensa de las partes involucradas. Sin embargo, la evolución tecnológica ha transformado las formas tradicionales de producción probatoria, incorporando nuevas fuentes digitales que plantean desafíos respecto a su autenticidad, integridad y valoración jurídica (Iglesias et al., 2025).

El desarrollo tecnológico ha ampliado las fuentes de obtención de información mediante dispositivos electrónicos, plataformas digitales, sistemas informáticos, correos electrónicos, registros audiovisuales y bases de datos, cuyos contenidos pueden adquirir relevancia probatoria dentro de investigaciones penales. En este escenario, la evidencia digital se ha convertido en un elemento frecuente dentro de los procesos judiciales, debido a que permite identificar responsables, reconstruir hechos y sustentar acusaciones. Según Miller (2022), su utilización requiere procedimientos especializados debido a la volatilidad de la información, la posibilidad de alteración y la complejidad técnica asociada a su tratamiento.

Los delitos tradicionales, incluidos aquellos relacionados con corrupción pública, generan con mayor frecuencia rastros digitales que pueden contribuir al esclarecimiento de los hechos. Comunicaciones electrónicas, registros de sistemas institucionales, documentos digitales y transacciones electrónicas pueden constituir elementos determinantes para demostrar conductas ilícitas. No obstante, su valor probatorio depende de procesos adecuados de identificación, preservación, análisis y valoración dentro del procedimiento penal (Llugsha et al., 2025).

La incorporación de tecnologías en la administración de justicia ha generado la necesidad de actualizar los mecanismos de investigación penal para responder frente a modalidades delictivas cada vez más complejas. La prueba digital adquiere relevancia tanto en delitos cometidos mediante tecnologías de la información como en conductas ilícitas tradicionales, donde los registros electrónicos permiten fortalecer la identificación de responsables y la acreditación de los hechos investigados

(Martínez, 2023). En particular, dentro de los delitos contra la administración pública, los registros digitales asociados a sistemas institucionales, comunicaciones electrónicas y documentos administrativos pueden contribuir al esclarecimiento de actuaciones irregulares y procesos sujetos a investigación.

No obstante, aunque la prueba digital representa una herramienta estratégica para la investigación de actos de corrupción, su incorporación dentro del sistema judicial plantea retos relacionados con la obtención lícita de información, protección de derechos fundamentales, autenticidad de los datos, cadena de custodia y criterios de valoración probatoria. Desde una perspectiva técnica, la confiabilidad de esta evidencia requiere procedimientos estandarizados de identificación, adquisición, recopilación y preservación, como los establecidos en la norma ISO/IEC 27037:2012 (International Organization for Standardization & International Electrotechnical Commission, 2012).

Estos desafíos evidencian la necesidad de establecer criterios jurídicos y técnicos que permitan garantizar la confiabilidad de la evidencia digital dentro de los procesos penales. La articulación entre normas de transparencia, control administrativo, protección de derechos y estándares técnicos resulta fundamental para asegurar que la evidencia electrónica pueda ser utilizada como elemento probatorio válido.

En este sentido, el presente estudio se justifica por la importancia de comprender el papel de la prueba digital como mecanismo de apoyo en la investigación de delitos contra la administración pública, considerando los desafíos asociados a su tratamiento jurídico y técnico. Por ello, el objetivo de esta investigación es analizar la relevancia jurídica y probatoria de la prueba digital en la investigación de delitos contra la administración pública en Ecuador, mediante una revisión documental jurídica y científica orientada a identificar sus principales fuentes, tipos, requisitos de validez y marco normativo aplicable.

2. Metodología

El estudio correspondió a una revisión documental de enfoque jurídico y cualitativo, orientada al análisis e interpretación de literatura científica, normativa y doctrinal relacionada con la prueba digital dentro de la investigación de delitos contra la administración pública. La investigación se fundamentó en la revisión de fuentes bibliográficas, artículos científicos, cuerpos normativos nacionales e instrumentos internacionales, los cuales fueron seleccionados y examinados con el propósito de identificar los principales elementos jurídicos que sustentan la incorporación, valoración y utilidad de la evidencia digital en los procesos penales.

El análisis documental permitió examinar tres ejes principales: en primer lugar, los delitos contra la administración pública y la necesidad de evidencia digital, considerando la importancia de los registros electrónicos para identificar, demostrar y vincular conductas relacionadas con actos de corrupción; en segundo lugar, las fuentes y modalidades de evidencia digital descritas en investigaciones jurídicas y científicas sobre corrupción pública, incluyendo comunicaciones electrónicas, mensajes de mensajería instantánea, registros informáticos, documentos digitales y otros elementos tecnológicos susceptibles de aportar información probatoria.

En tercer lugar, se analizó el marco normativo aplicable a la prueba digital en Ecuador mediante el estudio de disposiciones constitucionales, penales, procesales y técnicas que regularon su obtención, preservación, autenticidad y valoración dentro del sistema judicial. Este análisis permitió establecer la relación existente entre los requisitos jurídicos de la prueba y los desafíos técnicos asociados al tratamiento de la evidencia digital.

Desde un enfoque cualitativo, la información recopilada fue sometida a un proceso de análisis jurídico interpretativo, orientado a establecer relaciones entre la normativa vigente, los criterios doctrinales y la aplicación práctica de la evidencia digital en investigaciones de corrupción. Este procedimiento permitió identificar los principales desafíos asociados a la admisibilidad, cadena de custodia y confiabilidad de la prueba digital, así como determinar su relevancia como herramienta para fortalecer la investigación y persecución de delitos que afectan a la administración pública.

3. Desarrollo

Delitos contra la administración pública y necesidad de evidencia digital

Los delitos contra la administración pública constituyen conductas que afectan la transparencia institucional, el correcto funcionamiento del Estado y la protección del patrimonio público. Debido a su impacto en la gestión estatal, la Constitución de la República del Ecuador establece medidas reforzadas para combatir actos de corrupción, incluyendo la imprescriptibilidad de determinados delitos como peculado, cohecho, concusión y enriquecimiento ilícito.

La investigación y sanción de estas conductas requiere la intervención coordinada de instituciones como la Contraloría General del Estado y la Función Judicial, encargadas del control, investigación y juzgamiento conforme a sus competencias (Vázquez-Vázquez et al., 2020). En este contexto, la obtención de elementos probatorios confiables resulta fundamental para determinar responsabilidades y garantizar procesos judiciales ajustados al debido proceso.

Entre las principales manifestaciones de corrupción pública se encuentra el cohecho, entendido como una conducta basada en la utilización indebida de la función pública mediante la entrega, solicitud o aceptación de beneficios a cambio de realizar u omitir actos relacionados con las competencias del servidor público. Esta conducta presenta una naturaleza bilateral, debido a que involucra tanto al funcionario que recibe o solicita el beneficio como a la persona que lo ofrece o entrega (Montoya et al., 2016).

Por otra parte, el peculado representa una de las conductas más lesivas contra la administración pública, debido a que implica la apropiación, disposición irregular o administración inadecuada de recursos estatales por parte de servidores públicos que tienen acceso a ellos debido a sus funciones. La identificación de estas conductas puede requerir registros financieros, documentos electrónicos y otros elementos digitales que permitan reconstruir las actuaciones investigadas (Risco & Herrera, 2025).

La concusión se configura cuando un servidor público, aprovechando su posición institucional, exige o recibe beneficios económicos o de otra naturaleza a cambio de ejecutar, omitir o facilitar actuaciones vinculadas con sus funciones. Esta conducta refleja un abuso del poder público para obtener ventajas indebidas y se encuentra tipificada en el artículo 281 del Código Orgánico Integral Penal (Ulloa-García et al., 2024).

Dentro del ámbito de la administración de justicia, el prevaricato constituye una conducta atribuida a jueces o árbitros que actúan contra una norma expresa durante la sustanciación de una causa. Conforme al artículo 268 del Código Orgánico Integral Penal, su configuración requiere una vulneración manifiesta del ordenamiento jurídico, sin que toda interpretación jurídica controvertida pueda considerarse delito (Ruiz-Sandoval & Aguilar-Chamorro, 2026).

El enriquecimiento ilícito se relaciona con el incremento injustificado del patrimonio de un servidor público cuando existe una desproporción entre los bienes adquiridos y los ingresos legítimos

declarados. Esta figura penal busca preservar los principios de transparencia, probidad y responsabilidad en el ejercicio de la función pública (Montoya et al., 2013).

La complejidad de estos delitos radica en que frecuentemente se desarrollan mediante mecanismos poco visibles, acuerdos informales y procedimientos administrativos que generan rastros electrónicos. Por esta razón, la evidencia digital constituye una fuente relevante para identificar relaciones entre los involucrados, reconstruir actuaciones administrativas y aportar elementos objetivos dentro de las investigaciones penales.

Fuentes y tipos de evidencia digital en investigaciones de corrupción pública

La evidencia digital utilizada en investigaciones de corrupción pública puede provenir de diversas fuentes tecnológicas, principalmente de comunicaciones electrónicas, dispositivos informáticos, sistemas institucionales y registros generados mediante plataformas digitales. Estos elementos permiten reconstruir hechos, identificar relaciones entre los involucrados y verificar actuaciones administrativas, siempre que su obtención, preservación y valoración se desarrollen bajo criterios jurídicos y técnicos que garanticen su autenticidad, integridad y confiabilidad (Armenta, 2018).

Entre las principales fuentes de evidencia digital se encuentran los correos electrónicos institucionales, debido a que constituyen mecanismos oficiales de comunicación dentro de las entidades públicas. Estos registros pueden contener mensajes, documentos adjuntos, imágenes y otros archivos intercambiados entre servidores públicos y dependencias administrativas, aportando información relevante sobre decisiones, instrucciones o acuerdos relacionados con la gestión estatal (Ribeiro, 2022).

Para su incorporación dentro de un proceso judicial, resulta necesario verificar elementos asociados a su autenticidad, como la identificación del remitente y destinatario, fecha de emisión y recepción, origen del mensaje, conservación del contenido original y ausencia de modificaciones que puedan afectar su valor probatorio. Estos criterios permiten establecer la correspondencia entre la información digital presentada y la fuente de origen.

Las comunicaciones digitales y servicios de mensajería instantánea representan otra fuente relevante en investigaciones de corrupción, debido a que permiten documentar interacciones directas entre funcionarios públicos, particulares u otros actores involucrados en posibles actos ilícitos. Aplicaciones de mensajería, redes sociales y otros medios electrónicos pueden revelar solicitudes, acuerdos, negociaciones o coordinaciones relacionadas con conductas investigadas.

Un ejemplo corresponde a un caso de cohecho pasivo propio analizado por la Fiscalía Especializada en Delitos de Corrupción de Funcionarios de Lima (Carpeta Fiscal N.º 294-2022), donde conversaciones mediante WhatsApp entre la denunciante y la investigada constituyeron elementos de convicción para demostrar una presunta solicitud de dinero a cambio de gestionar un puesto laboral en una institución pública (Alcala, 2022). Este tipo de registros evidencia la capacidad de las comunicaciones digitales para establecer vínculos entre los sujetos investigados y aportar información relevante dentro del proceso penal.

En investigaciones complejas, los dispositivos electrónicos y sistemas informáticos de almacenamiento constituyen fuentes esenciales de información, debido a que pueden contener archivos, bases de datos, registros de actividad y otros elementos susceptibles de análisis forense. La obtención de estos datos requiere procedimientos autorizados de acceso, registro y recuperación que aseguren la legalidad de la actuación investigativa y la preservación de la información recopilada (Armenta, 2018).

Dentro de esta categoría, los correos electrónicos adquieren especial importancia, debido a que contienen tanto el contenido del mensaje como datos asociados de tráfico, tales como fecha, hora, origen y destino. Estos metadatos contribuyen a determinar la procedencia de la información y fortalecer la valoración de su autenticidad dentro del procedimiento judicial.

Los documentos electrónicos y registros administrativos digitales constituyen fuentes relevantes para investigar irregularidades en la administración pública. Según su origen, pueden clasificarse en documentos públicos, administrativos y privados. Los primeros corresponden a aquellos generados mediante mecanismos reconocidos jurídicamente por autoridades con capacidad legal; los documentos administrativos son emitidos por funcionarios públicos en ejercicio de sus competencias; mientras que los documentos privados corresponden a archivos digitales generados fuera de procedimientos administrativos formales (Nazate & Viscarra, 2026).

Esta clasificación permite determinar la naturaleza jurídica del documento digital y establecer los criterios necesarios para valorar su alcance probatorio dentro de una investigación relacionada con actos de corrupción pública.

En este contexto, los registros provenientes de sistemas informáticos estatales, bases de datos públicas y administrativas, contratos electrónicos, metadatos, registros financieros electrónicos y plataformas institucionales representan fuentes fundamentales de evidencia digital. Estos elementos permiten verificar procesos, identificar modificaciones, establecer trazabilidad documental y detectar posibles irregularidades en la gestión pública (Vanegas, 2025). Su análisis permite reconstruir la secuencia de actuaciones administrativas, identificar patrones de comportamiento y aportar elementos objetivos para la determinación de responsabilidades dentro de investigaciones penales.

La importancia de estas fuentes se evidencia en investigaciones relacionadas con corrupción pública, donde correos electrónicos, comunicaciones digitales y registros telefónicos pueden contribuir a identificar posibles actos irregulares vinculados con procesos administrativos y contratación pública. En estos escenarios, la aplicación de técnicas de análisis forense digital permite verificar la integridad de la información y fortalecer su incorporación como elemento probatorio mediante procedimientos de cadena de custodia (Imaicela & Alvarado, 2024).

Además de los registros documentales y comunicacionales, los dispositivos tecnológicos de captura audiovisual, como sistemas de grabación de audio y video utilizados en actividades de control público, constituyen fuentes adicionales de evidencia digital. Estos mecanismos permiten documentar actuaciones realizadas por servidores públicos y generar registros verificables sobre posibles conductas irregulares dentro del ejercicio de funciones estatales (Ulloa-García et al., 2024).

La utilidad probatoria de estas fuentes depende de que la evidencia digital cumpla requisitos de autenticidad, integridad, fiabilidad y disponibilidad, además de haber sido obtenida conforme a la normativa vigente y sin vulnerar derechos fundamentales. Su valoración corresponde al juzgador mediante un análisis integral junto con otros elementos probatorios, considerando las circunstancias de obtención, conservación y presentación dentro del proceso judicial (Bujosa et al., 2021).

Marco normativo sobre la prueba digital

La incorporación de tecnologías digitales en los procesos administrativos y judiciales ha generado la necesidad de establecer mecanismos jurídicos que regulen de manera adecuada la obtención, conservación, tratamiento y valoración de la evidencia digital. En Ecuador, si bien no existe una regulación integral y específica sobre prueba digital, su utilización dentro de los procesos judiciales se

fundamenta en disposiciones constitucionales, legales y técnicas que reconocen la validez de los documentos electrónicos, protegen derechos fundamentales y establecen criterios orientados a garantizar su confiabilidad.

La Constitución de la República del Ecuador establece principios relacionados con la protección de datos personales, la intimidad, el secreto de las comunicaciones y el debido proceso, los cuales constituyen límites jurídicos para la obtención, tratamiento y utilización de información digital dentro de investigaciones penales. A nivel procesal, el Código Orgánico Integral Penal y el Código Orgánico General de Procesos reconocen la incorporación de elementos electrónicos como medios probatorios, regulando aspectos vinculados con su legalidad, cadena de custodia, autenticidad y valoración.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos otorga reconocimiento jurídico a los documentos electrónicos y mensajes de datos, mientras que la Ley Orgánica de Protección de Datos Personales [LOPDP] establece principios relacionados con el tratamiento legítimo, seguro y confidencial de la información digital. Estas disposiciones adquieren especial relevancia en investigaciones relacionadas con delitos contra la administración pública, donde los registros electrónicos pueden constituir elementos determinantes para acreditar actuaciones irregulares.

Estos instrumentos jurídicos se complementaron con procedimientos técnicos establecidos por la Fiscalía General del Estado y estándares internacionales, como el Convenio de Budapest, su Segundo Protocolo Adicional e ISO/IEC 27037:2012, orientados a fortalecer la identificación, preservación, análisis y transferencia de evidencia electrónica bajo criterios de integridad y confiabilidad.

Aunque el marco jurídico ecuatoriano permitió sustentar la incorporación de evidencia digital dentro de procesos administrativos y judiciales, persistieron desafíos relacionados con la ausencia de procedimientos uniformes para su obtención, tratamiento y valoración. En este sentido, resulta necesario analizar la articulación entre las disposiciones normativas y los estándares técnicos que garantizan la validez probatoria de la evidencia digital.

En la tabla 1 se presenta una síntesis de las principales normas e instrumentos nacionales e internacionales aplicables a la regulación de la evidencia digital en Ecuador, considerando aquellos aspectos relacionados con su reconocimiento jurídico, protección de derechos fundamentales, cadena de custodia y criterios de valoración probatoria.

Tabla 1

Normas e instrumentos jurídicos y técnicos aplicables a la evidencia digital en Ecuador

Norma / instrumento jurídico o técnico	Artículo o apartado relacionado	Contenido aplicable a la evidencia digital
Constitución de la República del Ecuador (2008)	Art. 66, numerales 19, 20 y 21	Reconoce el derecho a la protección de datos personales, la intimidad personal y familiar, así como la inviolabilidad y secreto de la correspondencia física y virtual. Estos derechos establecen límites para la obtención y tratamiento de información digital dentro de investigaciones judiciales.
Constitución de la República del Ecuador (2008)	Art. 75 – Tutela judicial efectiva	Garantiza el acceso a una justicia efectiva, imparcial y expedita, evitando situaciones de indefensión durante los procesos judiciales en los que puede incorporarse evidencia digital.

Constitución de la República del Ecuador (2008)	Art. 76 – Garantías del debido proceso	Establece garantías procesales relacionadas con la validez de las actuaciones judiciales y la obtención de elementos probatorios conforme a la Constitución y la ley.
Código Orgánico Integral Penal [COIP] (2014)	Art. 453 – Finalidad de la prueba	Determina que la prueba tiene como finalidad llevar al juzgador al convencimiento sobre la existencia de la infracción y la responsabilidad de la persona procesada.
Código Orgánico Integral Penal [COIP] (2014)	Art. 454 – Principios de la prueba	Establece principios aplicables a la actividad probatoria, como oportunidad, inmediación, contradicción, libertad probatoria, pertinencia y exclusión de pruebas obtenidas ilegalmente.
Código Orgánico Integral Penal [COIP] (2014)	Art. 456 – Cadena de custodia	Regula la conservación y trazabilidad de los elementos probatorios, incluyendo aquellos de naturaleza digital, garantizando su autenticidad, integridad y preservación.
Código Orgánico Integral Penal [COIP] (2014)	Art. 457 – Criterios de valoración de la prueba	Establece que la valoración probatoria debe considerar criterios de legalidad, autenticidad y aplicación de conocimientos técnicos y científicos.
Código Orgánico Integral Penal [COIP] (2014)	Arts. 498 y siguientes – Medios de prueba	Reconoce los medios probatorios aplicables dentro del proceso penal, incluyendo elementos documentales, testimoniales y periciales relacionados con evidencia digital.
Código Orgánico Integral Penal [COIP] (2014)	Arts. 505 y 511 – Actuación y reglas generales de los peritos	Regula la participación del perito, la presentación del informe técnico, su acreditación y la sustentación mediante interrogatorio y contrainterrogatorio.
Código Orgánico General de Procesos [COGEP] (2015)	Art. 196 – Producción de la prueba documental	Reconoce como medios probatorios documentos, fotografías, grabaciones, elementos audiovisuales, computacionales y otros de naturaleza electrónica.
Código Orgánico General de Procesos [COGEP] (2015)	Art. 202 – Documentos digitales	Reconoce la eficacia probatoria de reproducciones digitalizadas o documentos electrónicos incorporados al expediente judicial, conforme a las condiciones establecidas por la normativa aplicable.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002)	Art. 2 – Reconocimiento jurídico de los mensajes de datos	Reconoce que los mensajes de datos poseen igual valor jurídico que los documentos escritos, permitiendo su utilización como elementos probatorios.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002)	Art. 5 – Confidencialidad y reserva	Establece la protección de la información transmitida mediante mensajes de datos y garantiza su tratamiento conforme a principios de seguridad y confidencialidad.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002)	Art. 6 – Información escrita mediante mensajes de datos	Reconoce que la información electrónica puede cumplir requisitos legales de forma escrita cuando sea accesible y pueda ser consultada posteriormente.
Ley Orgánica de Protección de Datos Personales [LOPDP] (2021)	Principios de tratamiento de datos personales	Establece principios de legalidad, seguridad, confidencialidad y protección aplicables al tratamiento de información personal contenida en registros digitales.

Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital (Fiscalía General del Estado del Ecuador, 2025)	Procedimientos técnicos de recolección, preservación, tratamiento y análisis	Define procedimientos técnicos para la identificación, adquisición, conservación y análisis de evidencia digital dentro de investigaciones penales.
Convenio sobre la Ciberdelincuencia (Convenio de Budapest) (Consejo de Europa, 2001)	Arts. 16, 17, 18, 19 y 20	Establece mecanismos relacionados con conservación rápida de datos informáticos, obtención de información almacenada, acceso a datos y cooperación internacional para la obtención de evidencia electrónica.
Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (Consejo de Europa, 2022)	Cooperación internacional y divulgación de evidencia electrónica	Fortalece los mecanismos de cooperación entre Estados y proveedores de servicios para facilitar el acceso y transferencia internacional de evidencia electrónica.
ISO/IEC 27037:2012	Directrices técnicas internacionales	Proporciona directrices técnicas para la identificación, recopilación, adquisición y preservación de evidencia digital, garantizando procedimientos confiables durante su tratamiento.

La prueba digital dentro del proceso penal ecuatoriano debe cumplir criterios de legalidad, licitud, autenticidad, integridad y trazabilidad que permitan garantizar su eficacia probatoria dentro del proceso judicial. Su obtención debe realizarse conforme a las normas procesales vigentes y respetando derechos fundamentales como la intimidad, la protección de datos personales y el secreto de las comunicaciones, bajo criterios de necesidad y proporcionalidad (COIP, 2014; LOPDP, 2021).

La confiabilidad de la evidencia digital depende de la posibilidad de establecer su correspondencia con la fuente original y demostrar que no ha sido alterada durante las etapas de identificación, adquisición, conservación y análisis. Para ello, pueden aplicarse mecanismos técnicos como copias forenses, códigos hash y registros detallados de intervención que permitan verificar la integridad de la información recopilada.

En este contexto, la cadena de custodia constituye un elemento esencial para preservar la trazabilidad de la información digital desde su recopilación hasta su valoración judicial. Aunque el ordenamiento jurídico ecuatoriano reconoce principios aplicables a la incorporación de evidencia digital, persisten desafíos relacionados con la ausencia de procedimientos técnicos uniformes y criterios especializados para su tratamiento.

Por ello, resulta necesario fortalecer el desarrollo normativo y técnico de la prueba digital en Ecuador, con el propósito de garantizar una gestión adecuada de la evidencia electrónica, proteger las garantías constitucionales y asegurar su utilización confiable en investigaciones relacionadas con delitos contra la administración pública (Avemañay et al., 2025).

4. Discusión

La transformación digital ha generado cambios sustanciales en la forma en que los sistemas de justicia obtienen, analizan y valoran información relevante para la investigación penal. En este escenario, la evidencia digital se ha consolidado como un elemento frecuente dentro de los procesos judiciales, debido a que los hechos delictivos actuales generan rastros electrónicos mediante comunicaciones digitales, registros audiovisuales, datos de localización, sistemas informáticos y archivos electrónicos (Llugsha et al., 2025).

Estos cambios evidencian que la prueba digital dejó de constituir un recurso excepcional para convertirse en un componente necesario dentro de la investigación penal, especialmente cuando las conductas ilícitas generan interacciones o registros almacenados en entornos tecnológicos. En consecuencia, los sistemas judiciales enfrentan el desafío de incorporar estos elementos sin afectar los principios que garantizan un proceso justo.

La incorporación de evidencia digital adquiere especial relevancia en delitos contra la administración pública, debido a que estas conductas frecuentemente involucran comunicaciones privadas, sistemas institucionales, documentos electrónicos y registros administrativos digitales. Sin embargo, la disponibilidad de información tecnológica no determina por sí misma su valor probatorio, ya que su incorporación requiere demostrar que fue obtenida legalmente y conservada bajo condiciones que garanticen su autenticidad e integridad.

En concordancia con Herrera (2025), la admisibilidad de la evidencia digital depende de procedimientos adecuados de identificación, preservación y análisis que permitan establecer la correspondencia entre la información presentada y la fuente original. Por ello, la cadena de custodia adquiere una importancia central, debido a que permite documentar las etapas por las cuales atraviesa la evidencia desde su recopilación hasta su valoración judicial.

Esta necesidad adquiere mayor relevancia debido a que, aunque la tecnología facilita la obtención de información útil para la investigación penal, también incrementa los riesgos asociados con la manipulación, modificación o generación artificial de contenidos digitales. La evolución de herramientas tecnológicas capaces de alterar imágenes, documentos, audios o comunicaciones plantea nuevos desafíos para los sistemas judiciales, que requieren mecanismos especializados de verificación.

En este sentido, Bujosa et al. (2021) sostienen que la evidencia digital debe cumplir criterios de autenticidad, integridad, fiabilidad y disponibilidad, considerando aspectos relacionados con su trazabilidad, conservación y ausencia de modificaciones. Estos criterios evidencian que la valoración de la prueba digital supera el análisis exclusivamente jurídico y requiere conocimientos especializados en informática forense para garantizar una interpretación adecuada de sus características técnicas.

De acuerdo con Nazate y Viscarra (2026), la correcta valoración de la evidencia digital exige una interacción permanente entre operadores jurídicos y especialistas técnicos, debido a que los peritos aportan elementos científicos sobre la integridad de la información, mientras que los jueces determinan su pertinencia y alcance probatorio conforme al marco jurídico aplicable.

En el caso ecuatoriano, aunque existe reconocimiento normativo para incorporar elementos digitales dentro de los procesos judiciales, el desarrollo regulatorio aún presenta limitaciones relacionadas con la ausencia de procedimientos específicos y uniformes para la obtención, preservación, análisis y valoración de evidencia digital. Arteaga et al. (2026) señalan que, si bien el Código Orgánico General de Procesos reconoce la incorporación de elementos electrónicos, todavía existen vacíos respecto a criterios técnicos que permitan garantizar una aplicación homogénea.

Esta situación evidencia una brecha entre el avance tecnológico y la capacidad normativa e institucional para responder a las nuevas formas de producción probatoria. Por ello, la incorporación efectiva de la prueba digital requiere fortalecer no únicamente la legislación, sino también las capacidades técnicas de fiscales, jueces, abogados y peritos encargados de intervenir en procesos donde la evidencia electrónica constituye un elemento determinante.

En consecuencia, el principal desafío no consiste únicamente en reconocer la importancia de la prueba digital, sino en garantizar que su utilización combine eficacia investigativa con respeto a los derechos fundamentales de las partes procesales. El fortalecimiento del marco normativo, la capacitación especializada y la aplicación de protocolos técnicos permitirán aprovechar el potencial de la evidencia digital en la investigación de delitos contra la administración pública, reduciendo los riesgos asociados con la alteración, falsificación o interpretación incorrecta de información electrónica.

5. Conclusiones

Los delitos contra la administración pública representan una afectación directa al funcionamiento institucional del Estado, debido a que comprometen principios como la transparencia, probidad y adecuada gestión de los recursos públicos. El análisis realizado permitió determinar que estas conductas requieren mecanismos probatorios capaces de responder a nuevas formas de interacción y generación de información asociadas al entorno digital.

Conductas como peculado, cohecho, concusión, prevaricato y enriquecimiento ilícito pueden generar rastros electrónicos mediante comunicaciones, sistemas institucionales, documentos digitales y registros administrativos. En este contexto, la prueba digital se constituye en un recurso estratégico para reconstruir hechos, identificar relaciones entre los sujetos involucrados y aportar elementos objetivos dentro de investigaciones penales.

Las fuentes de evidencia digital representan herramientas fundamentales para la investigación de actos de corrupción pública, debido a que los sistemas tecnológicos generan diversos registros susceptibles de análisis probatorio. Correos electrónicos institucionales, mensajes digitales, bases de datos administrativas, documentos electrónicos, metadatos, registros financieros y evidencias audiovisuales pueden contribuir a identificar irregularidades y establecer responsabilidades.

No obstante, los resultados evidencian que la existencia de información digital no garantiza por sí misma su valor probatorio, debido a que su eficacia depende de procedimientos adecuados de identificación, preservación, autenticación y valoración técnica. Por ello, la evidencia digital requiere un tratamiento especializado que permita diferenciar información confiable de aquella que pudo haber sido modificada o manipulada mediante herramientas tecnológicas.

El marco normativo ecuatoriano presenta avances importantes en el reconocimiento de elementos digitales dentro de los procedimientos judiciales y administrativos. La Constitución de la República del Ecuador, el Código Orgánico Integral Penal, el Código Orgánico General de Procesos, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Ley Orgánica de Protección de Datos Personales y los instrumentos técnicos institucionales establecen fundamentos jurídicos para garantizar la legalidad, protección de derechos y conservación de la evidencia electrónica.

Sin embargo, el estudio permitió identificar que aún persisten desafíos relacionados con la ausencia de procedimientos específicos y criterios técnicos uniformes para la obtención, tratamiento y valoración de la prueba digital en Ecuador. La rápida evolución tecnológica exige una actualización

permanente del marco regulatorio y una mayor articulación entre operadores jurídicos, peritos informáticos e instituciones encargadas de la investigación penal.

En consecuencia, la prueba digital constituye una herramienta indispensable para fortalecer la investigación de delitos contra la administración pública, siempre que su incorporación se realice bajo estándares jurídicos, técnicos y éticos que garanticen su confiabilidad. El fortalecimiento normativo, la capacitación especializada y la implementación de protocolos de actuación permitirán aprovechar su potencial investigativo sin afectar las garantías fundamentales del debido proceso.

Referencias

- Alcala, V. (2022). *La prueba digital en los delitos contra la administración pública Lima—Metropolitana 2022* [Tesis de pregrado, Universidad Privada Norbert Wiener]. <https://hdl.handle.net/20.500.13053/8043>
- Armenta, M. (2018). Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): Entre la insuficiencia y la incertidumbre. *IDP. Revista de Internet, Derecho y Política*, (27), 67–78. <https://doi.org/10.7238/idp.v0i27.3149>
- Arteaga, E., Cuenca, B., & García, H. (2026). La prueba digital en el proceso civil ecuatoriano: ¿Estamos preparados jurídicamente? *Revista Lex*, 9(32), 351–363. <https://doi.org/10.33996/revistalex.v9i32.460>
- 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
- Bujosa, L., Bustamante, M., & Toro, L. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347–1384. <https://doi.org/10.22197/rbdpp.v7i2.482>
- Código Orgánico Administrativo [COA]. Registro Oficial Suplemento N.º 31, 7 de julio de 2017. <https://n9.cl/tziya>
- Código Orgánico General de Procesos [COGEP]. Registro Oficial Suplemento No. 506, 22 de mayo de 2015. <https://n9.cl/o2op>
- Código Orgánico Integral Penal [COIP]. Registro Oficial Suplemento N.º 180, 10 de febrero de 2014. <https://n9.cl/3iyct>
- Consejo de Europa. (2001). *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. Council of Europe*. <https://n9.cl/yd49tn>
- Consejo de Europa. (2022). *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Council of Europe*. <https://n9.cl/3ahia>
- Constitución de la República del Ecuador [CRE]. Registro Oficial Suplemento No. 449, 20 de octubre de 2008. <https://n9.cl/41evj>
- Fiscalía General del Estado del Ecuador. (2025). *Manual de actuación para la recolección, preservación, tratamiento y análisis del contenido digital*. <https://n9.cl/ynudt>

- Herrera, S. (2025). *El papel de la prueba digital en los procedimientos penales en Ecuador* [Tesis de maestría, Universidad Andina Simón Bolívar, Sede Ecuador]. <http://hdl.handle.net/10644/10524>
- Iglesias, S., Orbea, L., & Campos, F. (2025). Admisibilidad de la prueba digital en los procedimientos judiciales según la normativa ecuatoriana. *Revista Lex*, 8(30), 1716–1739. <https://doi.org/10.33996/revistalex.v9i30.374>
- Imaicela, J., & Alvarado, L. (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>
- International Organization for Standardization & International Electrotechnical Commission. (2012). *ISO/IEC 27037:2012: Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. <https://www.iso.org/standard/44381.html>
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro Oficial Suplemento No. 557, 17 de abril de 2002. <https://n9.cl/l1srj>
- Ley Orgánica de la Contraloría General del Estado. Registro Oficial Suplemento N.º 595, 12 de junio de 2002. <https://n9.cl/tws30>
- Ley Orgánica de Protección de Datos Personales [LOPD]. Registro Oficial Suplemento No. 459, 26 de mayo de 2021. <https://n9.cl/mv7ow>
- Ley Orgánica de Transparencia y Acceso a la Información Pública [LOTAIP]. Registro Oficial Suplemento N.º 337, 18 de mayo de 2004. <https://n9.cl/6rivv>
- Llugsha, O., Arcos, M., Freire, E., & Castillo, L. (2025). La prueba digital en el proceso penal ecuatoriano: Análisis normativo, probatorio y jurisprudencial. *Reincisol*, 4(8), 1251–1251. [https://doi.org/10.59282/reincisol.V4\(8\)1251](https://doi.org/10.59282/reincisol.V4(8)1251)
- Martínez, G. (2022). Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología*. <https://reunir.unir.net/handle/123456789/15287>
- Miller, C. (2022). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6, 100296. <https://doi.org/10.1016/j.fsisy.2022.100296>
- Montoya, Y., Chanjan, R., Novoa, Y., Rodríguez, J., & Quispe, F. (2013). *Manual de capacitación para operadores de justicia en delitos contra la administración pública*. Pontificia Universidad Católica del Perú. <https://n9.cl/3p03th>
- Montoya, Y., Novoa, Y., Rodríguez, J., Torres, D., & Guimaray, E. (2016). *Manual sobre delitos contra la administración pública*. Pontificia Universidad Católica del Perú, Instituto de Democracia y Derechos Humanos. <http://repositorio.pucp.edu.pe/index/handle/123456789/110641>
- Nazate, M., & Viscarra, R. (2026). El debido proceso y la práctica de la prueba digital: Una lectura crítica desde el derecho procesal civil en Ecuador. *Revista Científica Multidisciplinaria InvestiGo*, 7(19), 225–235. <https://doi.org/10.56519/n97hgx40>
- Ortega, J. (2020). *Delitos contra la administración pública*. Escuela Superior de Administración Pública. <https://n9.cl/pye1oq>
- Ribeiro, D. (2022). *La prueba digital*. En *Teoría crítica do processo: Segunda série*. https://www.academia.edu/82498505/La_prueba_digital

- Risco, E., & Herrera, J. (2025). Delitos contra la administración pública en el Perú: Un análisis comparado con los países de Colombia y Chile. *Aula Virtual*, 6(13). <https://doi.org/10.5281/zenodo.16762082>
- Ruiz-Sandoval, D., & Aguilar-Chamorro, A. (2026). Prevaricato y proceder contra norma expresa en acciones de protección en Ecuador. *Debate Jurídico Ecuador*, 9(2), 279–290. <https://doi.org/10.61154/dje.v9i2.4500>
- Ulloa-García, L., Díaz-Basurto, I., & Ros-Alvarez, D. (2024). Concusión en agentes de tránsito y los medios probatorios tecnológicos en procesos judiciales, Ecuador. *IUSTITIA SOCIALIS*, 9(1), 942–954. <https://doi.org/10.35381/racji.v9i1.4324>
- Vanegas, L. (2025). *Control interno y gestión documental: Una interacción clave para la eficacia y transparencia en la rendición de cuentas de la administración pública* [Tesis de especialización, Universidad de Antioquia]. <https://hdl.handle.net/10495/49257>
- Vázquez-Vázquez, F., Narváez-Zurita, C., Guerra-Coronel, M., & Erazo-Álvarez, J. (2020). La imprescriptibilidad de los delitos contra la administración pública: Caso ecuatoriano. *IUSTITIA SOCIALIS*, 5(8), 208–224. <https://doi.org/10.35381/racji.v5i8.570>

Transparencia

Conflicto de interés

Los autores declaran que no existen conflictos de interés de naturaleza alguna como parte de la presente investigación.

Fuente de financiamiento

Los autores financiaron completamente la investigación.

Contribución de autoría

Alex Paúl Martínez Once: Conceptualización, metodología, software, análisis formal, investigación, gestión de datos, visualización, redacción - preparación del borrador original, redacción - revisión y edición, financiamiento, administración del proyecto, recursos, supervisión.

Hillary Patricia Herrera Avilés: Metodología, validación, análisis formal, investigación, gestión de datos, redacción - preparación del borrador original, redacción - revisión y edición, financiamiento, recursos, supervisión.

Juan Fernando Tapia Sanchez: Conceptualización, metodología, validación, análisis formal, redacción - preparación del borrador original, redacción - revisión y edición, financiamiento, recursos.

Los autores contribuyeron activamente en el análisis de los resultados, revisión y aprobación del manuscrito final.