Universidad Andina Simón Bolívar

Sede Ecuador

Área de Derecho

Maestría en Derecho Penal

El papel de la prueba digital en los procedimientos penales en Ecuador

Segundo Medardo Herrera Zapata

Tutor: Christian Rolando Masapanta Gallegos

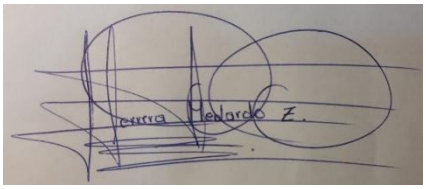
Quito, 2025

Cláusula de cesión de derecho de publicación

Yo, Segundo Medardo Herrera Zapata, autor del trabajo intitulado “El papel de la prueba digital en los procedimientos penales en Ecuador”, mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno 6 de los requisitos previos para la obtención del título de Magister en Derecho Penal en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo, por lo tanto, la Universidad utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en formato virtual, electrónico, digital u óptico, como usos en red local y en internet.
2. Declaro que, en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

27 de marzo de 2025

Firma: 

Resumen

La creciente digitalización de la sociedad ha transformado el panorama jurídico, en particular en el ámbito de los procesos penales, donde la prueba digital se ha vuelto indispensable. Este estudio examina el papel de la prueba digital en los procedimientos penales en Ecuador, centrándose en su marco legal, los desafíos y la necesidad de modernización. La investigación destaca la evolución de la prueba desde los formatos físicos tradicionales a los digitales, enfatizando la importancia de la prueba digital en los procesos judiciales contemporáneos. Explora los fundamentos legales y el marco regulatorio que rige la prueba digital en Ecuador, incluyendo el COIP y el COGEP, a la vez que aborda las lagunas y limitaciones de la legislación vigente. El estudio identifica desafíos significativos, como la falta de regulación específica, las limitaciones técnicas y operativas, y la capacitación insuficiente de los operadores judiciales. La investigación propone la implementación de un protocolo nacional para la gestión de la evidencia digital, enfatizando la necesidad de procedimientos estandarizados, capacitación continua e inversión tecnológica para garantizar la autenticidad, integridad y admisibilidad de la evidencia digital en los tribunales. Al comparar las prácticas de Ecuador con los estándares internacionales, el estudio subraya la necesidad de alinear la normativa local con las mejores prácticas globales, particularmente en el contexto de la ciberdelincuencia y las investigaciones transnacionales. Los hallazgos abogan por un enfoque integral para la integración de la evidencia digital en el sistema judicial ecuatoriano, garantizando la equidad, la transparencia y la eficiencia en los procesos penales.

Palabras clave: evidencia digital, procesos penales, Ecuador, marco legal, desafíos judiciales, ciberdelincuencia, estándares internacionales, modernización judicial

Mi tesis la dedico con todo mi amor y cariño a mis amados hijos, por ser mi inspiración y fortaleza en este apasionante reto académico.

A mi familia, que constituyen el pilar fundamental en mi vida, por su amor incondicional, su apoyo constante y su paciencia infinita. Sin ustedes, este logro no habría sido posible.

A mis docentes y mentores de la Universidad Andina Simón Bolívar, por su invaluable enseñanza y compromiso con la excelencia académica. Gracias por inspirarme a profundizar en el estudio del Derecho Penal con un enfoque crítico y humano.

A mis compañeros de esta apasionante maestría, por compartir este viaje lleno de desafíos y aprendizajes, por las conversaciones enriquecedoras y el apoyo mutuo en cada etapa de este proceso.

A todas aquellas personas que, desde el ejercicio del Derecho Penal, luchan por la justicia y la dignidad de cada ser humano. Que este trabajo contribuya, aunque sea en pequeña medida, a la construcción de un sistema más justo y equitativo.

Con gratitud y respeto,

Agradecimientos

Al concluir este arduo pero gratificante reto académico, deseo expresar mi más sincero agradecimiento a todas aquellas personas que, de una u otra manera, han sido parte fundamental en este logro.

A Dios, por darme la fuerza, la paciencia y la sabiduría para afrontar cada reto que este proceso conllevó.

A mis hijos, por su amor incondicional, su comprensión y su apoyo constante. Su confianza en mí ha sido mi mayor motivación para seguir adelante y superar cada obstáculo.

A mis docentes de la Universidad Andina Simón Bolívar, por su invaluable orientación, su entrega y su compromiso con la excelencia académica de manera especial al Dr. Christian Rolando Masapanta Gallegos por haberme brindado la oportunidad de nutrirme de su conocimiento científico, así como también por haberme guiado durante el desarrollo de mi trabajo de titulación. Gracias por compartir su conocimiento y por fomentar en mí un pensamiento crítico y reflexivo en el campo del Derecho Penal.

A mis compañeros de estudio, con quienes compartí largas horas de aprendizaje, debates enriquecedores y momentos de esfuerzo conjunto. Su apoyo y compañerismo hicieron que este recorrido fuera más llevadero y significativo.

A mis amigos, por su aliento en los momentos difíciles y por recordarme siempre la importancia del equilibrio entre la dedicación académica y la vida personal.

A todos aquellos profesionales del Derecho Penal, cuya labor diaria en la defensa de la justicia y los derechos fundamentales inspira la necesidad de seguir investigando, aprendiendo y contribuyendo a un sistema penal más justo y equitativo.

Este trabajo es reflejo del esfuerzo conjunto de muchas personas, y a cada una de ellas les estaré eternamente agradecido.

Con gratitud,

Tabla de contenidos

Introducción

En un mundo donde la digitalización se ha vuelto omnipresente, cada aspecto de la vida social, política y económica está intrínsecamente afectado por la evolución tecnológica. Esta transformación no es ajena al ámbito del derecho, el cual se encuentra en un proceso constante de adaptación y reconfiguración para poder afrontar los nuevos retos y oportunidades que plantea la revolución digital.

Resulta necesario establecer un diálogo acerca de la naturaleza y el impacto de la prueba digital dentro de los procedimientos penales en Ecuador, una temática que está ganando relevancia en discusión y análisis jurídicos a nivel global. Al respecto, la investigación pretender establecer que la prueba digital debe ser entendida como un elemento central del proceso judicial moderno, especialmente dado que se ha convertido en la esencia de la recolección y presentación de evidencias en los casos penales contemporáneos.

Las innovaciones tecnológicas han generado nuevas formas de recopilación de datos, ya sea a través de dispositivos móviles, redes sociales, correos electrónicos o incluso sistemas de vigilancia que generan grandes cantidades de información digital susceptible de ser utilizada como evidencia legal. Sin embargo, este avance también plantea serias interrogantes sobre la protección de los derechos fundamentales, la autenticidad de la evidencia y la cadena de custodia, aspectos que deben ser cuidadosamente abordados en un marco normativo adecuado.

El análisis propuesto se sumerge en los fundamentos teóricos que sustentan la prueba digital, así como en el marco normativo vigente en Ecuador. El autor no solo considera las leyes y regulaciones nacionales, sino que también se adentra en los estándares internacionales que orientan el tratamiento de la prueba digital. Este enfoque, que combina la perspectiva local y global, es clave para comprender cómo el derecho ecuatoriano se puede alinear con las mejores prácticas internacionales en la gestión de evidencias digitales. La obra resalta la necesidad de que los operadores de justicia —incluidos jueces, fiscales y abogados defensores— estén adecuadamente capacitados y preparados para lidiar con las complejidades y particularidades que presenta la prueba digital.

Un marco fundamental que se establece en el documento es el análisis del desarrollo histórico y la evolución de la prueba penal a través de las diferentes eras de la humanidad. Este análisis introduce al lector en el contexto en el que la prueba penal ha transitado desde

enfoques místicos y religiosos en la antigüedad, donde la intervención divina era vista como la única forma de determinar la culpabilidad o inocencia, hasta llegar a un enfoque más racional y científico en el presente.

Mediante este recorrido histórico, el autor establece que la evolución de la prueba penal refleja tanto los cambios culturales como la transformación del pensamiento humano en la búsqueda de la verdad. A lo largo del tiempo, se han desarrollado diversas metodologías y enfoques para la recopilación y validación de pruebas, lo que culmina en el reconocimiento de la prueba digital como un recurso primordial en el proceso penal del siglo XXI.

En este contexto histórico, es imprescindible entender la relevancia de la prueba digital, no solo como un medio para alcanzar la verdad material, sino también como un factor que impacta directamente en los derechos de las partes procesales. La dignidad de los ciudadanos debe ser protegida durante el manejo de estas pruebas, lo que incluye asegurar que los procesos respecten criterios de objetividad, imparcialidad y debido proceso. La introducción enfatiza que la prueba digital, al igual que cualquier otra forma de evidencia, debe ser tratada con la misma rigurosidad y seriedad, con el fin de garantizar que las decisiones judiciales sean justas y fundamentadas en evidencias claras y verificables.

A medida que el autor desarrolla su argumento, también advierte sobre los desafíos éticos y técnicos que surgen con la digitalización del sistema de justicia. Al tratarse de información que puede ser fácilmente manipulada, alterada o eliminada, el manejo y custodia de la prueba digital se convierten en aspectos cruciales para la integridad del proceso penal. Esto hace evidente la importancia de establecer protocolos claros de actuación que regulen cómo deben almacenarse, manejarse y presentarse las pruebas digitales en el ámbito judicial. Debe destacarse que la cadena de custodia y la preservación de la autenticidad de los datos digitales son elementos que deben ser cuidadosamente considerados y normados para asegurar su validez legal.

Otro aspecto destacado en la introducción es la necesidad de inversión en capacitación y formación especializada para los operadores de justicia. La revolución digital ha transformado la manera en que se procesan y presentan las evidencias, y los jueces, fiscales y defensores deben estar equipados con el conocimiento técnico y jurídico necesario para enfrentarse a estos retos. Esto no solo incluye comprender las herramientas tecnológicas disponibles, sino también estar actualizados sobre las mejores prácticas y protocolos relacionados con el manejo de la evidencia digital. La falta de capacitación

puede conducir a un manejo deficiente de la prueba digital, comprometiendo así los derechos de los acusados y la búsqueda de la verdad en los procedimientos judiciales.

La investigación también pone de manifiesto los impactos de la digitalización en el sistema judicial ecuatoriano y las posibilidades que ofrece para mejorar la eficiencia y transparencia en la administración de justicia. La implementación de tecnologías de información y comunicación ha permitido una mayor accesibilidad y agilidad en los procesos legales, pero también exige la creación de un ambiente regulador que fomente la confianza pública en el uso de estas herramientas. A medida que el sistema legal se moderniza, es imperativo que haya un marco normativo que acompañe esta transformación, asegurando que se respeten los derechos civiles y el debido proceso en todas las etapas del procedimiento penal.

De tal manera que se presenta, entonces, no solo como un análisis de la situación actual, sino también como una propuesta que invita a la reflexión sobre el futuro del derecho penal en un entorno digital. Se busca fomentar un diálogo constructivo en torno a la implementación de la prueba digital en Ecuador, analizando sus repercusiones y proponiendo estrategias para su inclusión efectiva en los procesos judiciales. La obra aboga por la urgente necesidad de adaptar las leyes, desarrollar protocolos claros y formar adecuadamente a los operadores de justicia, todo ello en un esfuerzo conjunto por construir un sistema legal más robusto, equitativo y eficiente.

Capítulo primero
Fundamentos y marco normativo de la prueba digital en Ecuador

La evolución tecnológica ha transformado profundamente el ámbito jurídico, especialmente en la manera en que se recopilan, presentan y valoran las pruebas dentro de los procesos legales. En este contexto, la prueba digital ha adquirido un rol protagónico al convertirse en una herramienta clave para la administración de justicia en el siglo XXI. Este capítulo aborda los fundamentos teóricos y el marco normativo que regulan la prueba digital en Ecuador, ofreciendo una visión integral de los principios legales, las disposiciones constitucionales y los instrumentos internacionales aplicables. Además, se analizan las particularidades del entorno jurídico ecuatoriano, destacando las oportunidades y desafíos que surgen en la implementación de estas normativas en un contexto de acelerada transformación digital.

1.1. La prueba en materia penal

La prueba penal es un elemento medular del proceso judicial, cuyo objetivo principal es garantizar la correcta determinación de la culpabilidad o inocencia de un acusado, al respetar principios fundamentales como la objetividad, la imparcialidad y el debido proceso. Su relevancia no solo radica en la búsqueda de la verdad material, sino también en la protección de los derechos de todas las partes involucradas, al asegurar que las decisiones judiciales sean justas y fundamentadas en evidencias claras y contundentes.[1]

La evolución de la prueba penal refleja la transformación de las sociedades y sus sistemas judiciales, al pasar de enfoques místicos y religiosos a métodos racionales y científicos. En su etapa inicial, conocida como la era de la intervención divina, la prueba penal estaba profundamente arraigada en creencias religiosas. Se consideraba que la divinidad era la única capaz de determinar la culpabilidad o inocencia de un individuo. Los juicios se realizaban a través de rituales como ordalías o pruebas de fuego y agua, donde se buscaba una supuesta manifestación divina que revelara la verdad. Este enfoque, aunque congruente con las cosmovisiones de la época, carecía de fundamentos racionales y frecuentemente conducía a decisiones arbitrarias e injustas.[2]

---

[1] Daniela Zapata, "La prueba en material penal y el debido proceso" (tesis de maestría, Uniandes, 2016), https://dspace.uniandes.edu.ec/handle/123456789/5413.

[2] Ibíd.

Con el tiempo, este sistema dio paso a la era del razonamiento judicial, un cambio paradigmático que marcó el inicio de la modernización de la justicia penal. En este nuevo contexto, los jueces asumieron un rol activo en la valoración de las pruebas, al utilizar su capacidad intelectual para formar un juicio basado en hechos objetivos y verificables. Esta transición no solo consolidó el aspecto racional del proceso penal, sino que también estableció las bases para el desarrollo de principios jurídicos esenciales, tales como la presunción de inocencia y el derecho a la defensa.

En el marco del sistema acusatorio oral, la prueba penal adquiere una dimensión aún más significativa. Este sistema, caracterizado por su estructura pública, contradictoria y concentrada, prioriza la inmediación entre los jueces y las partes, así como la transparencia en la valoración de las pruebas. La prueba en este contexto no solo tiene la función de acreditar los hechos, sino también de equilibrar la relación procesal entre acusación y defensa, lo que garantiza así un juicio justo.[3]

Los principios de inmediación y contradicción son esenciales en este sistema. La inmediación implica que los jueces estén presentes en la recepción de las pruebas, lo que les permite observar directamente la actuación de los testigos y la presentación de los medios probatorios. Por otro lado, el principio de contradicción propicia que las partes tengan la oportunidad de confrontar las pruebas expuestas por su contraparte, al fortalecer el carácter equitativo del proceso.

En el ámbito penal, las pruebas pueden clasificarse según su naturaleza y función dentro del proceso. En primer lugar, las fuentes de prueba corresponden a la información inicial obtenida al momento de descubrir un delito. Estas pueden incluir objetos, como un arma utilizada en el crimen, o evidencias físicas, como un cadáver, que proporcionan indicios sobre lo ocurrido.

Los medios de prueba, por su parte, son las herramientas mediante las cuales las fuentes de prueba se incorporan formalmente al proceso judicial. Entre estos medios se encuentran los documentos escritos, los testimonios de personas relacionadas con los hechos y los informes periciales elaborados por expertos en diversas disciplinas. A través de los medios de prueba, se busca transformar los indicios en elementos probatorios válidos y confiables. Finalmente, los elementos de prueba representan las convicciones que se derivan de la valoración de los medios durante la etapa de juicio. Estos elementos son

[3] Vicente Arias y Luis Cedeño, "Análisis de la confiabilidad en la incorporación de los medios de prueba en materia penal en el Ecuador", *Religación* 9, n.° 41 (2024): e2401306, doi: 10.46652/rgn.v9i41.1306.

fundamentales para que los jueces puedan fundamentar sus decisiones y emitir un veredicto que refleje la realidad de los hechos.

Un aspecto crítico en la valoración de las pruebas es la distinción entre pruebas ilícitas y pruebas ilegales. Las pruebas ilícitas son aquellas obtenidas mediante la violación de derechos fundamentales, como torturas, allanamientos sin orden judicial o interceptaciones de comunicaciones privadas sin autorización. Este tipo de pruebas carece de validez probatoria, ya que su obtención contraviene principios básicos del estado de derecho. En cambio, las pruebas ilegales presentan defectos formales en su obtención, como la omisión de procedimientos establecidos, pero pueden ser subsanadas y admitidas en ciertos casos, siempre que no se haya vulnerado ningún derecho fundamental.

En Ecuador, el Código Orgánico Integral Penal (COIP) establece que las pruebas obtenidas en contravención a la Constitución o la ley no deben ser valoradas por el tribunal penal. Sin embargo, la ausencia de directrices claras sobre los criterios para la exclusión de pruebas puede generar discrecionalidad en los jueces, lo que a su vez podría comprometer la garantía del debido proceso y abrir espacio a interpretaciones subjetivas que afecten la justicia.

El avance de la tecnología ha introducido nuevos retos en el manejo de las pruebas penales. La evidencia digital, como correos electrónicos, registros de cámaras de seguridad y datos almacenados en dispositivos electrónicos, ha ganado protagonismo en los procesos judiciales. Sin embargo, su manejo requiere un alto grado de especialización y protocolos estrictos para garantizar su autenticidad e integridad.[4]

La incorporación de la inteligencia artificial (IA) en el análisis de evidencia penal representa otro desafío significativo. Aunque la IA tiene el potencial de identificar patrones y actividades sospechosas con gran precisión, su uso plantea cuestiones éticas y legales, como la transparencia en los algoritmos y el respeto a los derechos de los procesados. Asimismo, la manipulación de la escena del crimen continua como un problema recurrente que puede comprometer la calidad de las pruebas y la confiabilidad de las investigaciones. En el ámbito internacional, la cooperación entre países es esencial para enfrentar la delincuencia organizada transnacional. En regiones como la Unión Europea, la armonización de normas y procedimientos para la obtención y reconocimiento de pruebas facilita la lucha contra delitos complejos, como el tráfico de drogas y la trata de personas.

[4] Klever Basantes y Danny Sánchez, "La exclusión de la prueba en materia penal frente al debido proceso", *Polo del Conocimiento* 9, n.° 3 (2024): 2873-94, doi: 10.23857/pc. v9i3.6822.

1.2. Definición de prueba

La administración de justicia sobre las controversias conocidas por la jurisdicción implica un proceso meticuloso de correlación entre los hechos alegados por las partes y las normas jurídicas aplicables al caso en discusión. Al respeto hay que señalar que los hechos alegados requieren un soporte probatorio que permita al juez o tribunal confirmar su veracidad y relevancia dentro del contexto del proceso. En este marco, Román conceptualiza las pruebas en los siguientes términos, destacando su naturaleza y trascendencia en el ámbito judicial:

Se trata de un acto procesal que tiene la finalidad es generar certidumbre en el juzgador sobre los hechos alegados, los cuales sustentan las presunciones formuladas por las partes, y frente a los cuales el juzgador debe emitir una respuesta razonada conforme al derecho. Esta conceptualización, de carácter general, es aplicable a las distintas clases de procesos —administrativos, penales, laborales, entre otros— y responde al principio *da mihi factum*, *dabo tibi ius*, que expresa, en gran medida, la esencia de la función jurisdiccional.[5]

La prueba es un componente esencial del proceso, ya que otorga al titular del órgano jurisdiccional, es decir, al juez, la posibilidad de verificar la objetividad de las afirmaciones realizadas por las partes en la defensa de sus pretensiones legítimas y derechos. De igual manera, la prueba se estructura a partir de principios y mecanismos específicos que se ajustan a las particularidades y dinámicas de cada proceso, así como a cada tipo de medio probatorio. Todo ello ha dado cuerpo a una rama jurídica autónoma: Derecho Probatorio. A partir de esos criterios, Coloma (2019), citado por Soárzano (2023), apunta que:

> Una característica relevante en la actividad procesal probatoria lo constituye el afianzamiento de los aspectos que sustentan o apuntalan lo que se quiere dar por probado. Penetrando aún más, se puede señalar que los actos encaminados, sea estos que respalden o contradigan los hechos alegados y que están en pugna. De allí que, los medios probatorios permiten puntualizar la vinculación entre lo alegado y la realidad de los hechos.[6]

---

[5] Luis Román, "La prueba en el proceso penal", *Aldaba,* n.° 24 (1995): 47-80, doi: 10.5944/aldaba.24.1995.20334.

[6] Rodrigo Coloma, "La prueba y sus significados", *Revista chilena de derecho 46,* n.° 2 (2019): 427-49, doi:10.4067/S0718-34372019000200427, p.68, citado por Erika Estefanía Solórzano León, "La valoración de las pruebas en las sentencias emitidas por los Jueces de la Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito de la Corte Provincial de Justicia de Pichincha, frente a casos de abuso sexual en el periodo de enero hasta diciembre del año 2019" (tesis de maestría, Universidad Central de Ecuador, 2023), https://www.dspace.uce.edu.ec/server/api/core/bitstreams/9508a225-607e-46a8-bb10-50c22916c3f0/content, p.56.

A partir de este análisis se colige la necesidad de establecer claras distinciones entre los conceptos de prueba, dato de prueba, medio o fuente de prueba y objeto de prueba. Como apunta Revelez, la prueba es un proceso mental en el cual se arriba a la correspondencia de un hecho alegado con la realidad. Un dato de prueba es una referencia, una información que se aporta para localizar fuentes de pruebas, como lugares, objetos, etc. El medio o fuente de prueba es aquella que permite reconstruir los hechos siguiendo ciertas formalidades procesales o procede la información, el medio que la proporcionará o del cual se podrá tomar[7]. El objeto de prueba es aquel fenómeno que, por su relevancia procesal, debe ser probado, es decir, es el *thema probandum* de un proceso[8].

Cabe decir que todavía existen criterios encontrados en cuanto al alcance de estos términos. Mientras que para algunos se equipara fuente y medio de prueba, para otros este último se refiere al proceso de otorgar a la fuente, la capacidad legal para ser empleada en un proceso judicial. Otros consideran que el dato de prueba, a medida que avanza el proceso, se convierte en medio de prueba, aspecto que es impugnado por Revelez, posición compartida por Nahuatt.[9]

Por su parte, Zeferín analiza los términos de evidencia y medios de convicción. En el caso del primero explica que se refiere a una entidad material cuya naturaleza le permite ser ocupada, conservada y examinada. En cuanto a los medios de convicción, expone cómo la legislación procesal mexicana asume que se trata de datos de prueba que son suficientes para ser valorados en los procesos abreviados.[10] Según la teoría general del proceso –comenta Zeferín–, toda prueba sigue un camino de ofrecimiento, admisión, desahogo y valoración, pero en el sistema penal acusatorio, la prueba, además, se anuncia y se descubre; o sea, tiene dos fases previas, que consisten en el aviso de su existencia, o sea, las partes

---

[7] Daniel L. Revelez, "Dato de prueba, medio de prueba y prueba: los conceptos que los penalistas se niegan a entender", *Revista Código Jurídico Mx,* S/N (2021). https://codigo-juridico-mx.webnode.es/l/dato-de-prueba-medio-de-prueba-y-prueba-los-conceptos-que-los-penalistas-se-niegan-a-entender/

[8] Diego Valderrama, "Diferencias entre objeto de prueba, fuente de prueba y medio de prueba", *Pasión por el Derecho*, s/n, (2021), https://lpderecho.pe/diferencias-objeto-prueba-fuente-prueba-medio-prueba/

[9] Margarita Nahuatt Javier, "Diferencia entre datos de prueba, medios de prueba y prueba: en el nuevo proceso penal acusatorio", *Revista del Instituto de la Judicatura Federal,* (2014): 161-173, https://codigo-juridico-mx.webnode.es/l/dato-de-prueba-medio-de-prueba-y-prueba-los-conceptos-que-los-penalistas-se-niegan-a-entender/

[10] Iván Zeferín, *La prueba libre y lógica: Sistema penal acusatorio mexicano* (Ciudad de México: Instituto de la Judicatura Federal, 2016), https://archivos.juridicas.unam.mx/www/bjv/libros/11/5263/6.pdf,

declaran disponer de material probatorio y, a continuación, se descubre, es decir, se presenten mutuamente las pruebas.[11]

En el ámbito del derecho procesal, incluyendo el ecuatoriano, la distinción entre los diversos elementos que conforman la actividad probatoria adquiere relevancia constitucional y práctica, dada su incidencia directa en la garantía del debido proceso y la efectiva tutela judicial. La prueba, entendida como el conjunto de actuaciones destinadas a acreditar los hechos controvertidos, se estructura a partir de categorías interconectadas, pero con cierta autonomía conceptual, de ahí que su correcta delimitación evitará confusiones que podrían derivar en lesiones a derechos fundamentales.

En cuanto al dato de prueba (*datum probationis*) representa la información preliminar que aún no ha sido sometida aún a los filtros de legalidad procesal. Según la doctrina contemporánea, este concepto –también aludido como prueba indiciaria—[12], se vincula con los indicios mencionados en el artículo 453 del COIP, que exige su suficiencia para sustentar resoluciones judiciales. La jurisprudencia de la Corte Constitucional ecuatoriana ha precisado que tales datos carecen de valor por sí mismos hasta su incorporación mediante medios lícitos, según lo estipulado al respecto en el artículo 76.4 de la Constitución de 2008[13].

Por su parte, el Código Orgánico General de Procesos (COGEP), en su artículo 158, enfatiza la finalidad persuasiva de la actividad probatoria, destinada a formar convicción judicial mediante el estricto respeto de formalidades *ad solemnitatem*. Investigaciones recientes destacan cómo la reforma procesal ecuatoriana ha reforzado los principios de contradicción e inmediación, particularmente en la práctica testimonial virtual regulada en el artículo 457 COGEP, que exige protocolos de biometría y sellado temporal para preservar la integridad probatoria[14].

Los medios de prueba funcionan como puentes entre las fuentes extraprocesales y el debate judicial. La Ley Orgánica de Garantías Jurisdiccionales en su artículo 89 los define

---

[11] Ibid., 52

[12] Raúl Caballero Laura, "El método de la prueba indiciaria, aplicable para la valoración de indicios y la prueba directa en las sentencias sobre delitos de concusión (colusión), peculado y corrupción de funcionarios (cohecho)", *Revista Oficial del Poder Judicial* 11, n.° 13, (2020): 363-388, doi.org/10.35292/ropj.v11i13.49

[13] Ecuador, *Constitución Política de la República del Ecuador*, Registro Oficial1, 11 de agosto de 1998, arts. 24 y 76

[14] Daniela Alejandra León Ordoñez, Rayza Belén León Ortiz y Armando Rogelio Durán Ocampo, "La prueba en el código orgánico general de procesos", *Universidad y Sociedad*, 11, n. 1 (2019): 359-368,http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000100359&lng=es&nrm=iso

como actos regulados que permiten acceder a realidades fácticas preexistentes.[15] Entre ellos destacan el *testimonium*, *documentum* y *peritia*, todos ellos sujetos a requisitos específicos de licitud y pertinencia. En este sentido Medina y Soria advierten sobre el reto que implica el uso de los medios digitales, particularmente en lo relativo a la cadena de custodia de metadatos y comunicaciones cifradas, aspectos ahora regulados en la Ley de Datos Personales (2021) mediante exigencias de consentimiento expreso y finalidad específica[16].

Las fuentes probatorias representan el sustrato material previo al proceso, donde se agrupan desde testigos hasta dispositivos tecnológicos. La Corte Constitucional, en lo tocante a la información digital y el habeas data ha precisado:

> Se compone de la obtención, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales.[17]

El objeto probatorio delimita, desde el punto de vista teleológico, la actividad jurisdiccional, la cual circunscribe a los hechos sustanciales del caso. La distinción entre *facta probanda* y *facta incidentalia*, desarrollada por la jurisprudencia constitucional en la mencionada sentencia, propende a evitar dilaciones procesales al excluir de la controversia lo notorio o jurídicamente irrelevante. Autores contemporáneos como León, León y Durán, subrayan cómo la prueba de oficio, contemplada en el COGEP, refuerza este objetivo al permitir al juez requerir elementos probatorios esenciales para esclarecer la verdad material.[18]

Ahora bien, la interacción entre estos elementos demanda un análisis específico en contextos tecnológicos. El uso de algoritmos predictivos en investigación criminal exige auditorías externas y mecanismos de explicabilidad para garantizar el derecho a contradicción. Paralelamente, la ratificación del Convenio de Budapest en 2022 insta a los estados partes de este instrumento a adoptar los estándares internacionales para la

---

[15] Ecuador, *Ley Orgánica de Garantías Jurisdiccionales*, Suplemento del Registro Oficial No.52, 22 de Octubre 2009, art. 89.

[16] Vanessa Estefanía Medina Medina y Yudith López Soria, "Los medios telemáticos en el proceso penal frente al debido proceso", Sociedad & Tecnología, 5, no. S1 (2022): 86–99: doi: 10.51247/st.v5iS1.235

[17] Ecuador. Corte Constitucional "Sentencia No. 2064-14-EP/21" sobre juicio No. 2064-14-EP de 27 de enero de 2021, 20

[18] Daniela Alejandra León Ordoñez, Rayza Belén León Ortiz y Armando Rogelio Durán Ocampo, "La prueba en el Código Orgánico General de Procesos"

conservación de datos y para cooperación transfronteriza, con lo cual se da paso a la entrada de nuevos paradigmas en la valoración de pruebas digitales.[19]

1.3. Clases de pruebas

En el ámbito del derecho procesal penal, según Devis Echandia, es posible identificar diversas clasificaciones de las pruebas. Desde una perspectiva elemental, estas pueden dividirse en pruebas de probabilidad o de certeza. Si se aborda la prueba desde un enfoque teleológico, las categorías se amplían a pruebas formales, de cargo, de descargo o sustanciales.[20] Asimismo, según los efectos de la prueba, esta puede ser plena o incompleta.

En el ámbito penal, es fundamental clasificar las pruebas según su naturaleza, distinguiendo entre pruebas personales y materiales. Las pruebas personales son aquellas que provienen directamente de individuos, como la confesión voluntaria del imputado, los testimonios de testigos, del acusado o de la víctima. Por otro lado, las pruebas materiales tienen su origen en objetos o elementos físicos, como fotografías, rastros, huellas u otros objetos relacionados con el caso. Además, es relevante diferenciar entre pruebas directas e indirectas. Las pruebas directas se refieren a aquello que demuestra directamente el delito, como el testimonio de un testigo presencial. En cambio, las pruebas indirectas, aunque no están directamente relacionadas con el hecho delictivo, permiten al juez inferir la comisión del ilícito mediante un proceso racional, como es el caso de los indicios.

La clasificación de las pruebas según las características específicas de cada medio y fuente reviste una importancia particular para el Derecho Procesal y el Derecho Probatorio. Esto se debe a que, en función de dicho conjunto de características, las pruebas se presentarán, argumentarán y refutarán de diversas maneras. Estas actuaciones pueden influir de manera determinante en la determinación de la culpabilidad o inocencia de una persona dentro de un proceso penal, con independencia del contexto jurídico, siempre que este se ajuste a las reglas generales del derecho.[21]

Para determinar el origen de la prueba, se hace referencia al punto o lugar en el cual esta se genera. El término "origen de la información" hace alusión a aquello que ya existe con anterioridad, surgiendo de manera independiente al juicio, por lo que no se inicia con

---

[19] Nelson Vela Andrade, "La prueba ilícita en el proceso penal ecuatoriano: Bases doctrinales y jurídicas" *Journal of business and entrepreneurial sutdies* 4 nº. 2 (2020): 295 – 307: doi.10.37956/jbes.v4i2.107

[20] Hernando Devis Echandia, *Compendio de la Prueba Judicial* (Buenos Aires: Rubinzal-Culzoni Editores, 1984), https://www.salapenaltribunalmedellin.com/images/doctrina/libros01/compendio_de_la_prueba_judicial_i.pdf.

[21] Ibíd., 35.

este, sino que puede existir incluso antes de que se dé inicio al proceso judicial, lo que le confiere un carácter extraprocesal. El Código Orgánico Integral Penal, l[22] en su capítulo tercero, dedicado a los medios de prueba, el artículo 498 establece tres tipos: la documental, la testimonial y la pericial.

De la clasificación contenida en el artículo 498 del COIP[23] sobre los medios de prueba, se deriva una subclasificación que destaca los tres tipos de prueba más relevantes en el ámbito procesal. La prueba documental desempeña un papel crucial al respaldar las alegaciones que las partes presentan en acusación o en defensa. Originalmente, esta prueba se limitaba a la presentación de documentos físicos, pero con el tiempo ha sido ampliada para incluir evidencias derivadas de las tecnologías de la información y la comunicación.

Por otro lado, la prueba testimonial se erige como la prueba esencial en un sistema penal caracterizado por la oralidad, pues permite que los individuos cualificados, bajo juramento, expresen sus observaciones sobre el caso en cuestión. Finalmente, el peritaje ofrece al Derecho el apoyo de las ciencias y técnicas auxiliares, facilitando la clarificación de la veracidad de los hechos en disputa.

1.4. La prueba desde el punto de vista doctrinario

Para Sentís (citado por Solórzano), el término "prueba" viene del latín *probatio o probationis*, derivado de *probus*, que significa "bueno".[24] Se colige entonces que la prueba se emplea para verificar o validar la autenticidad de los elementos en cuestión. Asimismo, se entiende que, desde el punto de vista legal, la prueba constituye el procedimiento, mecanismo y medio a través del cual los tribunales desarrollan la actividad probatoria, y que está definida y regulada por la normativa correspondiente

De la misma forma, el concepto de prueba se entiende como un juicio esencial, conectado con la exigencia intelectual del ser humano de conocer y comprender. En este sentido, la prueba adquiere la función de autenticar, es decir, de corroborar la autenticidad y veracidad de aquello que se pretende conocer o demostrar. Los resultados de la actividad probatoria responden, pues, a la necesidad de demostrar, comprobar o indagar la verdad de las afirmaciones presentadas ante los tribunales[25].

---

[22] Ecuador, *Código Orgánico Integral Penal (COIP)*, Registro Oficial 180, 10 de febrero de 2014, art. 498.

[23] Ibíd.

[24] Santiago Sentis, "Que es la prueba (Naturaleza de la prueba)", *Revista derecho Procesal Iberoamericana* 2, n.° 3 (2013): 259-60, citado por Erika Estefanía Solórzano León, "La valoración de las pruebas en las sentencias", p.65.

[25] Margarita Nahuatt Javier, "Diferencia entre datos de prueba, medios de prueba y prueba"

De lo anterior se colige con claridad que una inspección no se limita a una mera indagación, toda vez que su objetivo es comprobar hechos que ya han sido o deben ser previamente esclarecidos, descubiertos y sometidos a análisis. La investigación precede en el tiempo a la inspección, de modo que determinados hechos deben ser investigados y dados a conocer antes de que pueda formularse una declaración al respecto. Solo tras llevar a cabo estos pasos se procede a la prueba, asegurando así que su corrección ha sido verificada.

De este modo, se consideraba fundamental realizar una investigación previa. Este procedimiento no forma parte del fenómeno experimental como tal. Uno de los clásicos sobre el tema, Eduardo J. Couture, sostenía que las pruebas, en su acepción habitual, se asemejaban a dos actividades dirigidas a resolver incertidumbres, ya que su finalidad es confirmar la verdad de una afirmación que previamente se ha dado por cierta[26]. Este enfoque, aunque inicialmente estaba orientado al Derecho Civil, puso de manifiesto un sesgo al presentar la prueba de concepto como dos actividades diferenciadas: la investigación y la validación de lo ya establecido. Por consiguiente, el término "prueba" debería reservarse para aquellas actividades que tienen lugar una vez concluidos los procesos previos de indagación y verificación.

En este sentido, la doctrina reciente y la normativa vigente en Ecuador hace énfasis en la importancia de los medios probatorios como instrumentos *sine qua non* para la reconstrucción de la realidad procesal, en tanto la verdad judicial no es otra cosa que una aproximación razonada y fundamentada de los hechos controvertidos, sujeta a los límites impuestos por los elementos aportados por las partes. Así, resulta claro que el conocimiento judicial no constituye una copia exacta de la realidad, sino una interpretación que depende de la calidad, suficiencia y legalidad de los medios probatorios presentados. Si el juzgador carece de información relevante o si la evidencia ha sido alterada o manipulada, la decisión puede verse afectada, lo que pone de manifiesto la necesidad de una rigurosa valoración de la prueba conforme a las reglas de admisibilidad y conducencia previstas en el COGEP. De esta forma lo comentan Freire y Mayorga:

> En la prueba la importancia radica no en los hechos, sino más bien en las declaraciones de hecho que realizan las partes procesales. En cambio, para el derecho de la prueba son importantes los hechos y las declaraciones de hecho, principalmente desde una perspectiva previa al juicio, ya que deben evaluarse en primer lugar, como una investigación, esto partiendo del punto de vista procesal,

[26] Eduardo J. Couture, *Fundamentos del Derecho Procesal Civil*, (Buenos Aires, Roque de Palma Editor,1958).

> y el segundo lugar a partir de lo procesal, ya que debe probarse la acusación para que el juez pueda dictar sentencia condenatoria.[27]

Desde una perspectiva procesal, la posibilidad de demostrar un hecho jurídico no depende exclusivamente de la existencia abstracta de los medios probatorios, sino de su adecuada incorporación y valoración conforme a derecho. Eso implica el respeto de los sujetos procesales a los principios de contradicción y legalidad. En este contexto, cualquier error en la aplicación de las normas probatorias puede ser combatida a través de los recursos previstos en el sistema, especialmente en sede de casación, donde se revisa la correcta aplicación del derecho

En definitiva, la valoración de la prueba no solo condiciona el desarrollo del proceso y la legitimidad de los actos jurídicos, sino que también otorga coherencia al sistema de recursos, al permitir la revisión de las decisiones jurisdiccionales cuando estas se apartan de los estándares legales. En el marco del modelo acusatorio adoptado en Ecuador, esta dinámica refuerza el protagonismo de las partes en la producción de material probatorio, situándolas como los principales impulsores del proceso y garantizando la efectividad práctica del principio de contradicción

.

1.3.1. La importancia de la prueba en el proceso penal

Como ya se ha reconocido ampliamente en la doctrina, la prueba desempeña un papel fundamental en el ámbito legal. La prueba constituye uno de los pilares esenciales en cualquier procedimiento judicial, ya que permite al juez alcanzar la convicción necesaria para resolver los hechos controvertidos de manera justa y motivada. En el derecho romano se planteaba "*Iudicium sine probatione non est*", es decir, no hay juicio sin prueba. A través de los medios probatorios legalmente admitidos, las partes pueden fundamentar sus pretensiones y el órgano jurisdiccional dispone de los elementos indispensables para administrar justicia, garantizando el derecho de contradicción y el debido proceso. Sin prueba, la decisión judicial carecería de fundamento objetivo y razonable.

---

[27] Génesis Belén Freire Padilla y Estefanía Cristina Mayorga Mayorga, "Los medios probatorios en los actos de proposición en el ordenamiento jurídico ecuatoriano" *Revista Latinoamericana de Ciencias Sociales y humanidades,* Nº.2 (2024), 777: 196: doi: 10.56712/latam.v5i2.1915, p.182

1.3.2. Prueba testimonial

En consonancia con el párrafo anterior, la prueba testimonial es uno de los medios de prueba de mayor vigencia a lo largo de la historia del Derecho, incluso en su modalidad anticipada, como se evidencia en el siguiente comentario:

> La prueba testimonial anticipada es "una institución que ya existía en el Derecho Romano, en el canónico y en el francés: tienen antecedentes en las leyes de partidas (Ley 2ª Titulo 16, partida 3a), la Ley de Enjuiciamiento Civil Española de 1855, también la establece". Este tipo de prueba ha existido desde el mismo derecho romano, lógicamente que la manera de recepción no estaba normada, a diferencia de que sucede hoy en día que en la mayoría de las legislaciones se ha tratado de establecer parámetros básicos para la recepción de un testimonio anticipado pues esto puede resultar contraproducente para las garantías constitucionales.[28]

La prueba testimonial reviste una importancia capital dentro del sistema penal acusatorio, ya que brinda al tribunal información directa sobre los hechos investigados. Según el COIP, específicamente en su artículo 501, el testimonio consiste en la declaración verbal de quienes tuvieron conocimiento del delito, sea como imputados, víctimas o terceros, convirtiendo al testigo en fuente de prueba y su declaración en el medio para incorporarla al proceso.[29] El artículo 502 amplía la normativa, permitiendo la valoración del testimonio en conjunto con el resto de pruebas y estableciendo criterios especiales para la admisión de declaraciones, incluso de personas que no puedan comparecer físicamente, como quienes sufren graves problemas de salud, discapacidad, residen en el extranjero, o son sujetos pasivos o protegidos.

En tales supuestos, y para evitar la paralización del proceso, se prevén medidas extraordinarias como la recepción anticipada del testimonio, siempre que se respeten los principios de inmediación y contradicción. Asimismo, cuando el testigo reside fuera del país, se recurre a la cooperación internacional o nacional, utilizando medios telemáticos para la declaración[30]. Finalmente, cabe destacar que, salvo en delitos de violencia intrafamiliar, de género o violación, ninguna persona está obligada a declarar contra su pareja formal o no, contra sus familiares hasta el cuarto grado de consanguinidad o segundo

---

[28] Marjorie Yanes, "El testimonio anticipado como medio de prueba en delitos de abuso sexual: estudio de casos" (tesis de maestría, Universidad Andina Simón Bolívar, 2021), https://repositorio.uasb.edu.ec/handle/10644/8202, p. 24.

[29] Ecuador, *Código Orgánico Integral Penal*, art. 502.

[30] Víctor Jaya, "Testimonio sobre el abuso sexual y su efecto jurídico en las sentencias emitidas por tribunales", *Lex: Revista de Investigación en Ciencias Jurídicas* 4, n.° 11 (2021): 48-59, doi: 10.33996/revistalex.v4i11.70.

de afinidad; sin embargo, si voluntariamente desean hacerlo, sus declaraciones serán admitidas y valoradas en el proceso.

Es necesario considerar que, según la práctica internacional, ninguna persona está obligada a emitir su testimonio en una audiencia penal contra sí mismo o contra familiares que se encuentran en el cuarto grado de consanguinidad o segundo de afinidad. Sin embargo, cuando el testigo tenga la intención de declarar es admitida las afirmaciones potestativas de los sujetos pasivos de un delito o de sus familiares independientemente del grado de filiación, de esta forma tabíen aparece concebido enel COIP:

> 5. Las niñas, niños y adolescentes declararán sin juramento, pero con la presencia de sus representantes o un curador que será nombrado y posesionado en la misma audiencia de juicio.
> 6. La o el juzgador nombrará y posesionará en el mismo acto a un traductor, cuando el declarante no sepa el idioma castellano.[31]

A tenor con dicha disposición legal, el sistema penal ecuatoriano en atención al principio de igualdad jurídica garantiza la participación de las personas en el sistema de justicia sin discriminación, aunque la ley prevé determinadas dispensas para los testimonios emitidos por menores. También, en atención a los preceptos del debido proceso, cuando la persona que atestigua es discapacitado auditivo, el juez recogerá el testimonio por escrito; si es iletrado, se le asignará un intérprete o, en su defecto, un sujeto habituado a comprender al declarante, el cual tomará su lugar como interprete en el mismo acto. Este caso particular puede determinar la subjetividad e injerencia del intérprete por lo que será preferencial un ente neutral.

La declaración de los testigos en el proceso penal solo puede verse limitada por razones de procedimiento, cuando existan objeciones fundadas y debidamente motivadas por las partes. Quienes sean llamados a declarar y aquellos que se encuentren en situación de riesgo tienen derecho a la protección que ofrece el Sistema Nacional de Protección y Asistencia a Víctimas, Testigos y Otros Participantes en el proceso penal (SPAVT), el cual prevé la adopción de medidas de seguridad para resguardar su integridad y la de sus familiares.

En este marco, incluso los agentes policiales pueden comparecer como testigos, asegurándose mediante recursos técnicos o protocolos especiales, la protección de su identidad y el desarrollo seguro de su testimonio. La presentación de la prueba testimonial

[31] Ecuador, *Código Orgánico Integral Penal*, art. 502

debe realizarse preferentemente durante la audiencia de juicio, en forma presencial o a través de medios telemáticos, garantizando siempre los principios de inmediación y contradicción. [32]

En casos excepcionales, los funcionarios con fuero pueden rendir su testimonio mediante informe juramentado, mientras que los testigos protegidos, informantes o agentes encubiertos pueden hacerlo en condiciones de aislamiento y seguridad, sin que se revele su identidad y asegurando que sus declaraciones no sean condicionadas por otros testigos

En todos los casos, antes de declarar, los testigos son advertidos sobre la obligación de decir la verdad y las consecuencias penales del falso testimonio o perjurio, lo que refuerza la seriedad y la legalidad del proceso probatorio.

Las partes tienen el derecho de interrogar a los testigos y de formular objeciones, las cuales deben ser valoradas por el juez, quien debe asegurar que las preguntas no sean impertinentes, sugestivas, incriminatorias o artificiosas, salvo en el contra examen, donde se admiten preguntas sugestivas para contrastar la versión del testigo. En el caso de víctimas en situación de vulnerabilidad, como niños, niñas, adolescentes, adultos mayores o personas que han sufrido delitos de violencia sexual o de género, se prevén medidas especiales para evitar la revictimización y garantizar condiciones de seguridad durante su declaración.[33]

El juez debe velar por la correcta identificación del testigo y adoptar todas las medidas necesarias para prevenir actos de intimidación, hostigamiento o cualquier forma de violencia durante el proceso judicial, especialmente en casos de delitos graves contra la integridad personal o la dignidad humana.

En relación con ello, la figura de la prueba testimonial anticipada en el Derecho Penal ecuatoriano presenta características especiales que permiten recoger el testimonio de la víctima con anterioridad al juicio, en condiciones que resguarden su integridad emocional, física y psicológica. Al respecto, Flores, citado por Tulcanaza et al. señala:

> El testimonio anticipado lo que pretendería en realidad es por una parte tratar de asegurar la autenticidad en el mayor grado que resulte posible en lo concerniente a la verdad procesal; mientras que por otra parte se trata de evitar que la víctima tenga que posteriormente rendir nuevas declaraciones o testimonios reproduciendo o recordando nuevamente los hechos relacionados con el ultraje a su integridad y a otros bienes

[32] Israel Emiliano Montenegro Bósquez, Diego Francisco Granja Zurita, Mario Ramiro Aguilar Martínez y Diego Patricio Gordillo Cevallos, "Las aclaraciones a testigos por parte de los jueces penales en las audiencias de juicio, un análisis desde el estándar de prueba", *Revista Universidad y Sociedad* 14, nº.2 (2022): 51-56, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000200051&lng=es&tlng=es.

[33] Ibid

> jurídicos subjetivos que tendrían una protección especial por parte del derecho penal, es decir, se busca evitar la revictimización" [34].

Se puede inferir que el testimonio podrá ser aprobado únicamente cuando el sujeto pasivo lo solicite o lo apruebe de oficio, y siempre que sea acompañado por un profesional capacitado o perito especializado en atención a víctimas, como trabajadores sociales, psicólogos, psiquiatras o terapeutas, entre otros. Es relevante señalar que esta modalidad de prueba testimonial anticipada igualmente se encuentra presente en diversos ordenamientos jurídicos de América Latina la región, fundamentándose en un principio que busca preservar la seguridad jurídica

Esta normativa se aplicará principalmente en procesos donde el sujeto pasivopertenezce a grupos especialmente protegidos en la Ley Suprema o sean testigos dentro de una causa penal, o se encuentren custodiados por la Policía Nacional, con el objetivo de garantizar su seguridad, proteger su testimonio y garantizar su participación en el proceso judicial. Esto se logrará permitiendo que los testigos comparezcan mediante tecnologías que resguarden su seguridad.[35] De igual manera, el Código Orgánico Integral Penal, en su artículo 503, establece la posibilidad de promover el testimonio de terceros cuando, debido a las particularidades del proceso, su testimonio sea indispensable para el esclarecimiento del delito.

Según las disposiciones procesales actuales en Ecuador, los medios de prueba obtenidos a través de declaraciones están sujetos a un conjunto de más de diez normas (art. 502) que regulan tanto la forma de su práctica como su valoración, lo que incide directamente en la formulación de la decisión judicial. En este contexto, el testimonio se evalúa en función de su coherencia con otros elementos probatorios del expediente.

Si bien la regla general establece que el testimonio debe rendirse de manera presencial durante la audiencia de juicio, existen excepciones en las cuales este puede ser anticipado, tales como en el caso de personas enfermas, con discapacidad, fuera del país, testigos protegidos, o aquellos que demuestren la imposibilidad de comparecer, así como

---

[34] Flores, F, "El testimonio anticipado como medio de prueba en los procesos penales", (Tesis de posgrado Universidad Católica de Santiago de Guayaquil, 2022), citado por Edward Andrés Tulcanaza Ruiz, Elias Alberto Herrera Peñafiel, Yudith López Soria y Holger Geovanny García Segarra, "Restricciones procesales para la realización del testimonio anticipado en el proceso penal ecuatoriano", *Revista UGC*, 3 Núm. 1 (2025): 147–155. https://universidadugc.edu.mx/ojs/index.php/rugc/article/view/83. p.149

[35] Carlos Ramírez, *Apuntes sobre la prueba en el COGEP* (Quito: Corte Nacional de Justicia, 2017), https://www.cortenacional.gob.ec/cnj/images/Produccion_CNJ/La%20prueba%20en%20el%20COGEP.pdf.

en circunstancias en las que se realice por medios telemáticos (como en el caso de personas residentes en el extranjero o en situaciones de riesgo bajo el SPAVT)[36].

Vista la norma *ut supra*, resulta como a su vez explica respecto al testimonio de terceros sujeto a las siguientes reglas, los terceros que no estén sujetos o sean parte del proceso de conocimiento de la violación deben testificar en persona. El uso del poder público podrá ejercerse en presencia de testigos que incumplan esta obligación. No se admitirá los testimonios de los sujetos depositarios de un secreto debido a su profesión, oficio o función, cuando se trate de la materia del secreto. Cuando se hayan emplazado, están en la obligación de asistir con el objeto de exponer la razón por la cual se origina la obligación de omitir su exposición, solo cuando se refiera al secreto o reserva del hecho.[37]

A la luz de dicha concepción, Almeida expone las particularidades del testimonio de terceros:

> Los hechos pueden percibirse por medio de los cinco sentidos. Si bien la doctrina se ha concentrado en la percepción de tipo visual, es útil conocer las distintas experiencias sensoriales que ha experimentado la persona que es llamada a declarar en el proceso. En muchos casos será relevante conocer las palabras que ha pronunciado una persona, los sonidos que ha emitido un animal (por ejemplo, los aullidos de un perro en el marco de un proceso en el que se persigue el delito de maltrato animal), o los ruidos que ha producido un objeto (por ejemplo, los provenientes de una alarma en el marco de un proceso en el que se cuestiona el cumplimiento de las obligaciones asumidas por una empresa de seguridad). En tales supuestos, el testigo declarará con base a su conocimiento personal, no habiéndose verificado un enlace comunicacional por medio del cual haya circulado la información, lo que caracteriza, esto último, a todos los testigos de referencia.[38]

Un testigo o perito proporcionará su declaración repetidamente conforme a las instrucciones del juez durante el proceso judicial. En casos en los que se cuente con la participación de veinte testigos o peritos, el juez, en colaboración con las partes en conflicto, determinará cuántos y quiénes asistirán en cada sesión. Si se presenta una multiplicidad de testimonios o peritajes en un mismo procedimiento, estos se recibirán de

---

[36] Anahí Verónica Briceño Ruiz y Diego Adrián Ormaza Ávila, "Régimen Normativo del Sistema Nacional de Protección y Asistencia a Víctimas, Testigos y Otros Participantes en el Proceso Penal en el Ecuador", *Revista Multidisciplinaria Arbitrada de Ciencias Sociales* 8, no. 3 (2024) 4675–4705:doi:10.56048/MQR20225.8.3.2024.4675-4705

[37] Yuli Llerena Pincay Rodríguez, "Testimonio anticipado en el ámbito de los delitos sexuales en el Ecuador", *Revista Científica de Educación Superior y Gobernanza Interuniversitaria Aula* 24, n.° 6 (2024): 41-54, doi: 10.56124/aula24.v6i9.004.

[38] Rodrigo Almeida Idiarte "La prueba testimonial y los testigos de oídas" (tesis de maestría, Universitát de Girona, 2022.) 4, Https://dugi-doc.udg.edu/bitstream/handle/10256/21614/Almeidaidiarte.TFM.pdf

manera individual, asegurando que los testigos no puedan comunicarse entre sí, ubicándolos en distintos lugares.[39]

En lo que respecta a los testigos o sujetos pasivos que requieren protección especial, podrán solicitar condiciones particulares que garanticen su seguridad al presentarse ante el juez o el fiscal, adaptándose a las circunstancias particulares de cada uno. Con el fin de asegurar la protección adecuada, se implementarán recursos tecnológicos, tales como circuitos cerrados de televisión, conferencias en línea u otros métodos similares, los cuales serán utilizados exclusivamente en una única ocasión. Posteriormente, el testimonio mecanizado que contenga la declaración realizada en la audiencia judicial será presentado como medio probatorio.[40]

Por su parte, la prueba testimonial, dadas sus implicaciones, no está exenta de responsabilidades, como la propia solemnidad del juramento previo hace ver, lo cual surge por una razón concreta, y es que, vulnerar el juramento testimonial, deriva en la responsabilidad penal del testigo que perjure. Sobre esto, García, Pérez y Guevara[41] comentan que la regla para juzgar a los testigos por falso testimonio y perjurio, el juez decretará el arresto de un testigo motivado al engañador testimonio o perjurio, el cual será consignado al fiscal correspondiente con el objeto de su indagación.

Finalmente, resulta pertinente citar la jurisprudencia de la Corte Nacional de Justicia en los casos de abuso sexual respecto al testimonio anticipado. En ese marco, el órgano, en su resolución n.° 1972-2018 establece:

> Por lo dicho, nuestra legislación ha establecido aquello, es decir un carácter excepcional para la recepción de testimonios urgentes o anticipados, en casos específicos, entre los que se encuentran a las víctimas del delito de abuso sexual. En estas infracciones, la prueba madre será el testimonio, pues permitirá esclarecer los acontecimientos suscitados, porque la víctima en muchos casos, sino en todos, es la única que conoce los sucesos, por tanto, se deben brindar todos los mecanismos que permitan a los sujetos procesales intervinientes en la causa penal ejercer sus derechos, y en el caso contradecir en el momento procesal oportuno, esto es, durante la práctica del testimonio anticipado.[42]

---

[39] Echandia, *Compendio de la Prueba Judicial*.

[40] Rafael Ayala, "Credibilidad testimonial en el proceso penal", *Revista Brasileira de Direito Processual Penal* 6, n.° 1 (2020): 453-80, https://www.redalyc.org/articulo.oa?id=673971418015.

[41] Ramiro García, Agustín Pérez y Alba Guevara, *El proceso penal: Derechos y garantías en el proceso penal*, t. 1 (Lima: Ara Editores, 2014).

[42] Ecuador Corte Provincial de Justicia Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito, "Resolución Nro. 1972-2018", en *Juicio n.° 03282-2017-00133*, 13 de noviembre de 2018, citada por Martha Elizabeth Jimbo Granda, "Principio de igualdad de armas en relación con el testimonio anticipado en víctimas de delitos sexuales en el contexto ecuatoriano y peruano" (tesis de maestría Universidad Técnica Particular de Loja, 2020), 63, https://bibliotecautpl.utpl.edu.ec/cgi-bin/abnetclwo?METS=61044333737

Teniendo en cuenta este antecedente de la jurisprudencia, se puede deducir que, pese a que la regla general establece que el testimonio debe ser presentada presencialmente a través de la asistencia del testigo en el juicio, cuando se trata de delitos sexuales se prevé el testimonio anticipado de modo excepcional. Esto se fundamenta en el hecho de que, dado que en tales casos la prueba testimonial tiene un carácter predominante sobre los demás medios probatorios, su realización resulta esencial para el juzgamiento de los delitos contra la integridad sexual. En este contexto, considerando los elementos de tipicidad y los efectos perjudiciales para la sobre la víctima, junto con la integración de tecnologías, el testimonio anticipado se presenta como recurso adecuado para proteger a las víctimas, prevenir su victimización secundaria y contribuir a esclarecer los hechos.

1.3.3. Prueba documental

La prueba documental, que reviste gran relevancia en cualquier procedimiento, sigue las pautas generales establecidas. El reconocimiento de documentos y firmas contenidos en ellos solo procede de forma voluntaria, estando prohibido el reconocimiento bajo coacción.[43] Tanto el representante de la Fiscalía como el letrado de la defensa, pueden solicitar informaciones relacionadas que reposen en los archivos públicos o privados, los cuales podrán ser evaluados en la vista oral. Se consideran medios de prueba las cartas y todos los demás materiales documentales incorporados al juicio, siempre que sean necesarios para esclarecer los hechos, las circunstancias y la autoría de estos.

Cuando el material documental forma parte de otro proceso o están archivados en algún expediente, es necesaria una reproducción fidedigna de este, sin que sea preciso adjuntar el original, salvo que se precise para acreditar la veracidad de los hechos. En tales casos, la copia permanecerá en el registro, proceso o archivo correspondiente, y, cuando sea necesario, se devolverá el original, continuando con la copia certificada. En cuestiones no procesales, los datos contenidos en la documentación no podrán ser utilizados ni procesal ni extraprocesalmente. Asimismo, cualquier contenido digital que cumpla con los estándares establecidos podrá ser aceptado como prueba, conforme a lo dispuesto en el COIP.

Con el avance tecnológico, se vuelve indispensable la existencia de normas que regulen la prueba en formato digital. Este tipo de contenido constituye un medio técnico que permite su procesamiento mediante herramientas informáticas, incluidos programas

[43] Devis Echandia, *Compendio de la Prueba Judicial*, 18.

destinados al aislamiento, interconexión o uso de equipos conectados. La información digital puede almacenarse, procesarse y vincularse de manera eficaz. En el marco de una investigación, resulta crucial seguir directrices específicas para su análisis, evaluación, recuperación y visualización, empleando técnicas propias de la tecnología forense digital aplicadas a dispositivos o sistemas informáticos.

Cuando el contenido se encuentra almacenado en soportes volátiles y el dispositivo donde este se almacena está incorporado a la es parte de la infraestructura tecnológica en sectores públicos o privados, se emplea tecnología forense digital para preservar la integridad del contenido, tanto en el sitio como en tiempo real, facilitando así su posterior evaluación y análisis. Una vez que el contenido digital se guarda en medios no volátiles, se recopila mediante herramientas forenses digitales, asegurando su integridad, acudiendo a la cadena de custodia, con vistas a su evaluación y posterior examen.

En las investigaciones donde se recojan medios de almacenamiento, procesamiento o transferencia de contenido digital, cada elemento debe ser debidamente identificado y catalogado de forma separada, y su ubicación debe ser determinada y protegida, utilizando fotografías y mapas de localización. A través de la tecnología digital y forense, el contenido se traslada a un centro especializado de almacenamiento, siguiendo un proceso cuidadosamente gestionado para este propósito.[44]

1.3.4. Prueba pericial

Según Pabón, la prueba pericial constituye un medio probatorio que implica la presentación de elementos técnicos, científicos o artísticos por parte de un especialista en la disciplina correspondiente, con el fin de esclarecer la controversia, siendo este aporte dependiente de conocimientos especializados.[45] Además, la legislación vigente establece que los peritos deberán exponer verbalmente los resultados de sus evaluaciones y responder tanto al cuestionario como al contrainterrogatorio planteado por las partes procesales. A su vez, se encuentran sujetos a normas generales. Es imprescindible que los peritos sean profesionales con formación técnica, académica o práctica, y cuenten con estudios avanzados, estando acreditados por el Consejo de la Judicatura.

---

[44] José González, "La prueba digital y la cadena de custodia", *Anales de la Facultad de Derecho*, n.° 38 (2021: 43-79), https://www.ull.es/revistas/index.php/derecho/article/view/2425.

[45] Pedro Pabón, *La prueba pericial, sistema acusatorio: Parte general y especial* (Colombia: Librería Jurídica Sánchez R., 2006), 627.

El designado tiene la obligación de presentar una disculpa en caso de encontrarse dentro de alguna de las causales previstas en este COIP para los jueces. No es posible rechazar a ningún experto, pero si este presenta un informe que demuestre de manera fehaciente su incompetencia, dicho informe será considerado nulo. Es imperativo que los informes sean entregados dentro del plazo establecido y que se aclaren o generen nuevos informes según lo solicite la parte interesada. El informe del perito debe contener, como mínimo, los siguientes elementos: la ubicación y fecha del peritaje, la identidad del perito, una descripción y estado del sujeto o persona investigada, la tecnología empleada, la base científica que sustenta el análisis, las ilustraciones pertinentes, así como las conclusiones y las firmas establecidas.

En atención al principio de inmediación, el experto en rol de perito deberá personarse en el juicio oral para exponer verbalmente sus informes y responder al interrogatorio de las partes procesales. Para este fin, se les permitirá utilizar cualquier tipo de dispositivo. En aquellos casos en los que no se cuente con un experto debidamente acreditado en la materia correspondiente, se podrá recurrir a un perito suplente, especialista o con un título que avale su capacidad para realizar el peritaje. En los juicios derivados de presuntas malas prácticas profesionales, la fiscalía solicitará una lista de tres expertos en la materia pertinente al instituto competente. Si en la investigación participan peritos internacionales, sus informes se incluirán como medio de prueba mediante la declaración anticipada, la cual podrá ser captada en videoconferencias conforme a las disposiciones legales vigentes.[46]

1.5. Concepto y características de la prueba digital

La prueba digital, también denominada prueba electrónica, se define como cualquier información que se genera, almacena o transmite mediante dispositivos electrónicos, con el fin de utilizarse en un proceso judicial. Este tipo de prueba abarca una gran variedad de formatos, que incluyen correos electrónicos, mensajes de texto, imágenes, videos, archivos digitales, datos en bases de datos y contenidos almacenados en servicios de nube. La evolución de las tecnologías ha introducido nuevas complejidades, como la

[46] Mirian Escobar, "La valoración de la prueba, en la motivación de una sentencia en la legislación ecuatoriana" (Tesis de maestría, Universidad Andina Simón Bolívar, Sede Ecuador, 2010), https://repositorio.uasb.edu.ec/bitstream/10644/1135/1/T0836-MDP-scobarLa%20valoración%20de%20la%20prueba.pdf.

jurisdicción y el acceso a servidores remotos, que deben ser considerados en su tratamiento judicial.

En el derecho procesal contemporáneo, la prueba electrónica ha cobrado una importancia central, reflejando el creciente papel de lo digital en la vida cotidiana y, por ende, en el ámbito jurídico. En una sociedad cada vez más interconectada, este tipo de evidencia se ha convertido en una herramienta clave al ofrecer registros verificables y precisos de acciones, transacciones e interacciones relevantes para la resolución de disputas legales. Además de modificar las dinámicas del litigio, la prueba digital plantea nuevos retos y oportunidades para los sistemas judiciales.

Con el uso masivo de dispositivos móviles y redes sociales, muchas interacciones que antes ocurrían de forma presencial o por medios tradicionales han migrado al entorno digital. Así, mensajes de aplicaciones como WhatsApp, correos electrónicos, publicaciones en redes sociales, grabaciones de cámaras de seguridad y contenidos generados en plataformas de videoconferencia se han convertido en elementos probatorios esenciales en procedimientos civiles, penales y administrativos. Actualmente, resulta difícil concebir un proceso judicial sin la incorporación de alguna forma de prueba digital.

Entre los formatos más comunes de esta evidencia se destacan las fotografías y videos digitales, que proporcionan representaciones visuales directas de hechos relevantes. En casos de lesiones o accidentes, por ejemplo, una imagen o grabación de una cámara de seguridad podría resultar determinante para definir la secuencia de los acontecimientos o las responsabilidades de los involucrados.

Por su parte, los correos electrónicos, constituyen una de las formas más extendidas de prueba documental en el ámbito digital. Los correos pueden servir para demostrar comunicaciones entre las partes, la intención detrás de ciertos actos contractuales o incluso la existencia de acuerdos previos. Su autenticidad y contenido pueden ser clave en procesos mercantiles o laborales.

En cuanto a los mensajes de texto y chats de aplicaciones, con el aumento del uso de aplicaciones como WhatsApp, Telegrama o incluso plataformas de mensajería dentro de redes sociales, las conversaciones digitales se han convertido en pruebas comunes, ya que contienen diálogos que pueden ofrecer información detallada sobre las interacciones de las partes. Asimismo, archivos en formatos como Word, Excel, PDF o presentaciones PowerPoint pueden ser prueba documental en casos contractuales, administrativos o laborales. Estos documentos son especialmente valiosos cuando contienen firmas electrónicas que pueden ser verificadas por medio de tecnología especializada.

De acuerdo con la Corte Nacional de Justicia[47], en el contexto de los procedimientos penales en Ecuador, la incorporación de pruebas digitales ha adquirido una relevancia significativa, especialmente en el caso de mensajes enviados por plataformas como WhatsApp. Estos mensajes pueden ser considerados documentos electrónicos, siempre que cumplan con los requisitos establecidos por la ley. Entre los aspectos clave para que dichos mensajes sean admitidos como prueba, se encuentra la autenticidad del contenido, lo cual implica verificar tanto el origen del mensaje como la identidad del titular de la cuenta que lo emitió.[48]

Sin embargo, la aceptación de estas pruebas no es automática, la autenticidad y legitimidad de los mensajes deben ser evaluadas cuidadosamente en cada caso concreto, pues su validez dependerá del análisis probatorio llevado a cabo por las autoridades judiciales.

La evaluación de la autenticidad y legitimidad de pruebas digitales, como los mensajes, es responsabilidad de los jueces, quienes revisan la fuente, integridad de los datos, cadena de custodia y relevancia del contenido. Se consideran indicadores como la consistencia temporal, coherencia del contenido, metadata y testimonios corroborativos, además de posibles análisis por expertos en informática forense, asegurándose que la admisibilidad de la prueba cumpla con la legalidad y el debido proceso en cada caso específico.

Este proceso de valoración busca garantizar que las pruebas digitales sean confiables y puedan sostener el peso necesario en un juicio, sin que se comprometa la justicia debido a posibles alteraciones o fraudes en el uso de estas tecnologías. Por lo tanto, aunque las pruebas digitales como los mensajes de WhatsApp son cada vez más comunes en los procesos penales en Ecuador, su admisión requiere un escrutinio riguroso, en consonancia con las normativas vigentes, para asegurar su fiabilidad dentro del sistema judicial.

El Código Orgánico Integral Penal (COIP), en el artículo 457, establece criterios específicos para la valoración de la prueba, los cuales deben incluir la legalidad y autenticidad de los elementos probatorios, así como su sujeción a la cadena de custodia y el nivel de pertinencia científico-técnica de los principios que respaldan el informe pericial.

---

[47] Ecuador Corte Nacional de Justicia, "Oficio: 171-2020-P-CPJP-YG", 3 de febrero de 2020, https://www.cortenacional.gob.ec/cnj/images/pdf/consultas_absueltas/No_Penales/Civil/127.pdf.

[48] Caros Geovanny Torres Loján, "WhatsApp como herramienta de prueba en litigios por obligaciones financieras: Una mirada al sistema judicial ecuatoriano", *Revista Lex* 7, n.° 25 (2024): 496-511, doi:10.33996/revistalex.v7i25.196.

De esta manera, se garantiza que cada prueba digital presentada en un proceso penal sea evaluada conforme a estos estándares, lo que fortalece la integridad del sistema judicial.

Asimismo, recae sobre la parte que presenta los elementos probatorios, especialmente la evidencia física no sometida a cadena de custodia, la responsabilidad de demostrar su autenticidad. Esto implica que, en aquellos casos en los que se utilicen mensajes digitales como prueba, quien los aporte debe asegurar su veracidad y fiabilidad, con el fin de evitar la vulneración de los derechos de las partes involucradas. En este contexto, el uso de pruebas digitales debe ser acompañado de un procedimiento exhaustivo que asegure su legitimidad y, al mismo tiempo, respete los principios del debido proceso.

Adicionalmente, en casos de fraude o delitos cibernéticos, el análisis de grandes cantidades de datos almacenados en bases de datos puede ser esencial para descubrir patrones de actividad ilegal, identificar usuarios o rastrear el origen de transacciones financieras sospechosas. En tal sentido, a pesar de su creciente relevancia, la prueba electrónica no es automáticamente aceptada en un proceso judicial. Para que sea admitida como evidencia válida, debe cumplir con una serie de requisitos legales. Los códigos procesales de las distintas jurisdicciones establecen normas específicas para asegurar que esta forma de prueba sea confiable, legítima y veraz.

A tales efectos, dentro de los requisitos incluyen que la parte que presenta la prueba debe demostrar que esta es auténtica, es decir, que la información presentada proviene de la fuente que se alega. Esto implica demostrar que el correo electrónico fue enviado por la persona que se indica o que el video es una grabación legítima del incidente en cuestión. Aunado a ello, la evidencia debe estar en su forma original o, en caso de que haya sido modificada (por ejemplo, para compilar diferentes partes de un video), esas modificaciones deben ser explicadas y justificadas. Cualquier alteración injustificada puede llevar a la inadmisibilidad de la prueba o a su cuestionamiento en cuanto a su veracidad.

Del mismo modo, resulta esencial que se garantice una cadena de custodia adecuada para la prueba electrónica. Esto significa que desde el momento en que la evidencia es obtenida hasta su presentación en el tribunal, debe quedar constancia de cómo fue almacenada y manejada para evitar que sea manipulada o dañada. En ese mismo orden de ideas, la prueba debe haber sido obtenida de manera lícita. En muchos países, la obtención de pruebas electrónicas sin autorización judicial o violándose derechos fundamentales, como el derecho a la privacidad, puede resultar en la exclusión de dicha prueba del proceso judicial. Este es un aspecto particularmente importante en casos que involucran escuchas telefónicas, acceso a correos electrónicos o la intervención en redes sociales.

Lo cierto del caso es que, aunque la prueba electrónica ha facilitado en muchos casos la obtención de evidencia crucial, también plantea retos significativos para el sistema judicial. Uno de los mayores desafíos es el riesgo de manipulación o alteración de la evidencia digital. Con las tecnologías disponibles en la actualidad, se ha vuelto factible la falsificación de correos electrónicos, la alteración de imágenes y videos, así como la modificación de documentos digitales. Este fenómeno se ha dado en llamar *deepfake* y constituye en la actualidad una peligrosa tendencia del ciberdelito[49]. En este contexto, se vuelve cada vez más imprescindible la intervención de especialistas en informática forense, quienes son capaces de verificar la autenticidad e integridad de las evidencias presentadas.

Otro reto importante es la protección de los derechos fundamentales, especialmente el derecho a la privacidad y a la protección de datos personales. En muchos casos, obtener pruebas electrónicas implica acceder a información privada de las personas, como sus correos electrónicos o mensajes en redes sociales, lo que puede generar tensiones entre el derecho a un juicio justo y la protección de la intimidad de los individuos.

La creciente importancia de la prueba electrónica ha llevado a los legisladores y tribunales a ajustar sus normativas y procedimientos. Muchos países han incorporado disposiciones específicas en sus códigos procesales para regular la admisión y el uso de la prueba digital, estableciéndose protocolos de autenticación y manejo de datos electrónicos. Asimismo, la capacitación de jueces y abogados en el uso y comprensión de estas tecnologías es un aspecto crucial para garantizar que las decisiones judiciales basadas en pruebas electrónicas sean justas y equilibradas. Según Martínez,[50] en el futuro cercano, se ha vuelto probable que el uso de la inteligencia artificial, el blockchain y otras tecnologías emergentes jueguen un papel importante en la autenticación y gestión de la prueba electrónica, al proporcionar nuevas herramientas para garantizar su integridad y facilitar su manejo en los tribunales.

Importancia de la prueba digital en el proceso penal

El avance de la era digital ha intensificado la necesidad de incorporar pruebas digitales en los procesos penales, tanto en delitos convencionales como en aquellos de

---

[49] Ronald Estiven Endara Chamorro, Juan Sebastián Espinoza Jiménez, Eder Ronaldo López Fuel y Jessica Johanna Santander Moreno, "Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador" *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas* IX. n° 1 (2024)240-252: doi:10.35381/racji.v9i1.3530

[50] Gemma Martínez, "Problemática jurídica de la prueba digital y sus implicaciones en los principios penales", *Revista Electrónica de Ciencia Penal y Criminología*, n.° 24-23 (2022): 1-38. https://reunir.unir.net/handle/123456789/15287

naturaleza cibernética. Martínez enfatiza que esta transformación requiere una profunda revisión de los enfoques clásicos del derecho penal, dado que la incorporación de evidencia digital presenta interrogantes sobre su pertinencia y su compatibilidad con principios fundamentales como la legalidad y la presunción de inocencia.[51] Sobre este asunto, es menester subrayar la necesidad de que todos los operadores jurídicos se adapten a esta nueva realidad tecnológica, cuyo desarrollo acelerado desafía los métodos probatorios convencionales.

Por su parte, González analiza los desafíos que la revolución digital ha impuesto al derecho, particularmente en lo referente a la prueba derivada de delitos informáticos.[52] Su estudio señala que, de acuerdo con la doctrina y jurisprudencia penal española, la licitud de una prueba digital depende de que su presentación se realice bajo condiciones que garanticen su contradicción. En este contexto, el peritaje informático desempeña un rol esencial en la verificación de la validez de las pruebas, constituyéndose en una exigencia esencial dentro del proceso penal.

Adicionalmente, Porras advierte que la evolución tecnológica ha generado un nuevo escenario probatorio que aún carece de procedimientos claramente establecidos para la admisión de pruebas digitales en los procesos judiciales.[53] A pesar de la existencia de normativas que regulan el uso de la tecnología, la falta de lineamientos específicos ha generado dificultades en la valoración de estas pruebas, lo que puede conducir a la violación de derechos básicos y a la exclusión de elementos probatorios determinantes.

El impacto de las TIC ha redefinido el derecho penal, otorgando un papel cada vez más relevante a la prueba digital. Su incorporación en los procedimientos judiciales exige una evaluación rigurosa, en la que los peritos desempeñan un rol fundamental al elaborar informes técnicos detallados que permiten su análisis dentro del proceso penal.[54]

La incorporación de evidencias digitales en el procedimiento penal plantea un grupo de serie de desafíos que demandan un enfoque riguroso y detallado. Entre los dilemas principales se encuentra su obtención, pues en todos los casos es esencial determinar si tal obtención cumplió con las exigencias legales vigentes y fueron respetados derechos de las personas implicadas. Otro asunto crucial consiste en definir si la evidencia digital es

---

[51] Ibíd.

[52] José González, "La prueba digital y la cadena de custodia".

[53] Pablo Porras, "La Incorporación de la Prueba Digital en el Proceso Penal Colombiano" (tesis de maestría, Unilibre, 2023), https://repository.unilibre.edu.co/handle/10901/29366?show=full.

Zander López, "Validez jurídica de la prueba digital en Guatemala", *Revista Ciencia Multidisciplinaria CUNORI* 7, n.º 2 (2023): 203-14; doi.10.36314/cunori.v7i2.238

admisible. Se requiere la determinar criterios sólidos que establezcan cuándo una prueba digital es aceptable en el ámbito penal. Tales criterios deben asegurar que la evidencia sea pertinente, confiable y que su obtención se haya realizado obtenida conforme a la ley, caso contrario será excluida del proceso judicial.[55]

La valoración de la prueba digital constituye un reto importante dentro del proceso judicial. Para que esta sea efectiva, los jueces deben contar con una formación adecuada que les permita analizar de manera integral tanto los aspectos técnicos como los jurídicos. Resulta fundamental que comprendan el origen, el tratamiento y la forma en que se ha presentado la evidencia digital, ya que estos elementos inciden directamente en su autenticidad, fiabilidad y relevancia. Solo así será posible garantizar una interpretación justa y precisa que respete el debido proceso.[56]

1.6. Marco legal vigente

En el marco normativo ecuatoriano, el Código Orgánico Integral Penal (COIP) regula el tratamiento de la prueba digital en los procesos penales, al establecer directrices claras para su obtención, preservación, y valoración como evidencia. El COIP enfatiza la importancia de respetar los derechos constitucionales durante la recolección de pruebas digitales, como el derecho a la intimidad y el debido proceso, garantizándose que los medios tecnológicos utilizados no vulneren garantías fundamentales. Asimismo, se contempla la cadena de custodia como elemento esencial para preservar la integridad de estos elementos probatorios, lo cual es indispensable para garantizar su admisibilidad y confiabilidad en los juicios penales.

Por su parte, el Código Orgánico General de Procesos (COGEP) aborda la prueba digital en el ámbito civil, reconociéndola como un medio idóneo para acreditar hechos relevantes en los procesos judiciales. Este cuerpo normativo establece parámetros para su ofrecimiento y producción en las audiencias, lo que destaca la carga de la prueba y la valoración libre pero motivada por parte del juez. Además, se incorporan disposiciones relacionadas con la incorporación de herramientas tecnológicas que permitan acceder, presentar, y analizar pruebas digitales, al garantizar con ello la eficiencia y transparencia en la resolución de conflictos.

Vicente Magro, "Casuística práctica de la prueba digital en el proceso civil y penal", *Actualidad civil*, n.° 1 (2020), https://www.asambleaex.es/vernumero-8637.

[56] Porras, "La incorporación"

1.7. Análisis del Código Orgánico Integral Penal (COIP)

El artículo 456 del Código Orgánico Integral Penal (COIP) regula la implementación de la cadena de custodia, que incluye los elementos materiales y los contenidos digitales utilizados como evidencia en un proceso judicial. Su finalidad es garantizar la autenticidad e integridad de los elementos probatorios mediante la certificación de su identidad y la preservación de su estado original durante todas las fases del procedimiento, incluyendo su recolección, traslado, manipulación, análisis y conservación. Es imprescindible que cada etapa de este manejo quede debidamente documentada, consignando las condiciones en que se desarrolla y la identificación de las personas responsables, así como cualquier modificación efectuada por los custodios.

La cadena de custodia se inicia exactamente en el sitio donde se descubre o recoge el objeto de prueba y finaliza solamente por disposición expresa de la autoridad actuante. El proceso implica a múltiples actores, incluyendo funcionarios del Sistema Especializado Integral de Investigación, profesionales de medicina forense y criminalística, especialistas en tránsito y otros que participen en la manipulación o análisis de los elementos probatorios. También se contempla al personal sanitario que pueda tener acceso a las evidencias.

El artículo 460 del Código Orgánico Integral Penal (COIP) atribuye al fiscal la responsabilidad de realizar la inspección del lugar de los hechos, asistido por las categorías de personas antes mencionadas. Esta inspección abarca no solo espacios físicos, sino también entornos digitales, como servicios electrónicos, plataformas tecnológicas y dispositivos informáticos que contengan información pertinente para la investigación.

Respecto a la validez de la prueba digital, el artículo 499 del COIP establece que el contenido digital puede ser admitido como prueba documental siempre que cumpla con los requisitos legales. El artículo 500 amplía la definición de contenido digital, aludiéndolo como representaciones informáticas que expresen hechos, datos o ideas susceptibles de ser procesados, almacenados o transmitidos mediante tecnologías informáticas. La obtención y análisis de estos contenidos deben realizarse mediante peritajes forenses digitales, a fin de preservar su integridad y autenticidad.

Cuando la evidencia digital reside en sistemas de almacenamiento volátil o dispositivos esenciales para la operación de instituciones públicas o privadas, es necesario capturarla in situ y en tiempo real utilizando técnicas forenses adecuadas. Esto asegura su integridad dentro de la cadena de custodia. En casos de almacenamiento no volátil, también se aplicarán metodologías forenses para su recolección y conservación, garantizando la validez probatoria del contenido digital.

Asimismo, en el contexto de una investigación, registro o allanamiento, los dispositivos físicos que almacenan procesan o transmiten datos digitales deben ser tratados con especial precaución. Cada uno de estos dispositivos debe ser debidamente identificado y catalogado, asegurando su correcta ubicación mediante registros fotográficos y planos detallados del área. Posteriormente, su traslado a un centro especializado debe realizarse bajo estrictas medidas de seguridad, garantizando así su integridad y disponibilidad para los fines del proceso judicial.

1.8. Análisis del Código Orgánico General de Procesos (COGEP)

El Código Orgánico General de Procesos (COGEP) en Ecuador es una norma que ha sido modernizada dentro del sistema judicial, marcándose un punto de inflexión en la manera en que se manejan las pruebas y las actuaciones procesales, que pueden resultar de utilidad el ámbito penal.[57] La incorporación de medios tecnológicos, como la digitalización de documentos y el uso de sistemas electrónicos para el manejo de expedientes y pruebas, busca transformar la administración de justicia hacia un modelo más eficiente, accesible y transparente.

El artículo 116 señala que las actuaciones procesales pueden llevarse a cabo a través de medios electrónicos, informáticos, magnéticos, telemáticos u otros que la tecnología permita.[58] Esto pone de manifiesto un claro compromiso del sistema judicial ecuatoriano con la modernización y la adopción de herramientas tecnológicas que pueden mejorar considerablemente el manejo de los casos, especialmente en términos de rapidez y accesibilidad. Este tipo de actuaciones incluye desde la presentación de pruebas hasta la comunicación de notificaciones y resoluciones judiciales.

En los procedimientos judiciales, la utilización de medios electrónicos tiene implicaciones profundas. Por ejemplo, se puede acceder a pruebas digitales como correos electrónicos, registros de cámaras de seguridad, comunicaciones de redes sociales o incluso datos extraídos de dispositivos electrónicos, todos los cuales son cada vez más comunes en la era digital. El reconocimiento de estas pruebas digitales como válidas dentro de un proceso penal es esencial para garantizar una justicia que refleje las realidades del mundo

[57] Ecuador, *Código Orgánico General de Procesos (COGEP)*, Registro Oficial 506, Suplemento, 22 de mayo de 2015, https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Orgánico-General-de-Procesos.pdf.

[58] Ibíd., art. 116.

moderno, donde los delitos cibernéticos o los delitos que dejan rastros digitales son cada vez más frecuentes.

El artículo 117 regula el uso de documentos digitalizados en las actuaciones judiciales.[59] En Ecuador, como en muchos otros países, los procesos judiciales han sido históricamente dependientes de documentos en papel, lo que no solo ralentiza los procedimientos, sino que también aumenta la posibilidad de pérdida o deterioro de los archivos. Con la norma del COGEP, las partes están facultadas para acompañar sus peticiones y demás actos procesales con documentos digitalizados, independientemente de su formato (texto, imágenes, sonido, videos). Esto podría resultar especialmente útil en los procedimientos penales, donde las pruebas pueden adoptar formas diversas, como fotografías de la escena del crimen, grabaciones de audio de interrogatorios o incluso imágenes de vigilancia, y donde la rapidez en la presentación y evaluación de la evidencia es crucial.

Sin embargo, el artículo también prevé excepciones para aquellos casos en que la digitalización de ciertos documentos no sea viable, ya sea por el volumen del archivo o por problemas de legibilidad. En estos casos, el sistema permite que dichos documentos se presenten físicamente en la unidad judicial, pero establece un plazo máximo: al día siguiente de la presentación de la petición electrónica. Esto garantiza que la justicia no se vea frenada por limitaciones tecnológicas, al tiempo que mantiene el compromiso con la modernización.

El artículo 118 introduce una disposición clave: todas las actuaciones procesales realizadas por o ante un juez deben ser registradas mediante medios telemáticos instalados en las dependencias judiciales.[60] Esta norma no solo busca garantizar la transparencia en el manejo de los procesos judiciales, sino que también asegura la preservación y la seguridad de la información procesal.

Estos registros se integran en una base de datos que alimenta el expediente electrónico del caso, lo cual permite a las partes involucradas, como los abogados defensores, fiscales y jueces, acceder fácilmente a la información en cualquier etapa del proceso. Este expediente electrónico es un avance significativo frente a los sistemas tradicionales basados en papel, que eran vulnerables a la pérdida, el deterioro o la manipulación. La salvaguarda y preservación de estos registros electrónicos facilitan un acceso más ágil y seguro a la información procesal, lo cual resulta de particular relevancia

[59] Ibíd., art. 117.
[60] Ibíd., art. 118.

en los procedimientos penales, donde es imperativo asegurar la protección de los derechos de las partes involucradas y la integridad de las pruebas con el más alto nivel de rigor.

Otro aspecto importante de este artículo es el derecho que se otorga a cualquier persona a solicitar copias de los registros de las actuaciones procesales, con excepción de aquellos que tienen carácter reservado. Esta disposición refuerza la transparencia del sistema judicial, al permitir un control ciudadano sobre las actuaciones judiciales. Sin embargo, el artículo también establece una medida de protección al limitar el acceso a las grabaciones de audiencias solo a las partes involucradas en el proceso.

La relevancia de la prueba digital en los procedimientos penales no puede subestimarse. Con el creciente uso de tecnología en la vida cotidiana, una parte significativa de la evidencia en los casos penales proviene de fuentes digitales. Esto incluye correos electrónicos, mensajes de texto, redes sociales, registros telefónicos, cámaras de seguridad, y una gran cantidad de datos que se almacenan en dispositivos electrónicos y en la nube.

El COGEP, al integrar la posibilidad de utilizar medios electrónicos para la presentación y registro de pruebas, refuerza la capacidad del sistema penal para manejar este tipo de evidencias de manera adecuada. En muchos casos, la prueba digital puede ser determinante para demostrar la culpabilidad o inocencia de un acusado. Un correo electrónico enviado en un momento clave, una grabación de una cámara de seguridad, o un mensaje de texto enviado por el sospechoso pueden ser las piezas que cierren un caso. La posibilidad de acceder, presentar y registrar estas pruebas de manera electrónica facilita su evaluación por parte del juez y de las partes involucradas.

De esta forma, el Código Orgánico General de Procesos (COGEP) no solo moderniza la justicia ecuatoriana, sino que también introduce una serie de disposiciones que fortalecen el uso de la tecnología en el ámbito procesal. La digitalización de documentos, la posibilidad de realizar actuaciones a través de medios electrónicos y el registro de estas actuaciones en sistemas telemáticos proporcionan a las partes herramientas más eficaces para el acceso a la justicia, agilizándose los tiempos procesales y garantizar la integridad y seguridad de la prueba. En un mundo donde los delitos dejan rastros digitales, estas disposiciones son fundamentales para que el sistema de justicia pueda adaptarse a las nuevas realidades y asegurar que se haga justicia de manera eficiente y equitativa.

El uso y tratamiento de la prueba digital en los procedimientos penales ha cobrado una importancia creciente en Ecuador, en consonancia con el acelerado desarrollo tecnológico y la expansión del ámbito digital en la vida cotidiana. Aunque el marco legal del país, en particular el Código Orgánico General de Procesos (COGEP), se orienta

fundamentalmente hacia los procesos civiles, sus disposiciones sobre la prueba documental y digital proporcionan pautas que pueden ser útiles en el ámbito penal. Este análisis no solo pone en evidencia la creciente relevancia de las pruebas digitales, sino también cómo su regulación, originalmente diseñada para un contexto civil, puede adaptarse eficazmente para abordar las necesidades del derecho penal en Ecuador.

Posteriormente, el Código[61] regula la producción de prueba documental en audiencias civiles. Si bien el enfoque es principalmente hacia los procedimientos civiles, el lenguaje utilizado, en particular al referirse a las pruebas de naturaleza digital o electrónica, resulta aplicable también al contexto penal. En este artículo, se establece que los documentos, objetos, y pruebas audiovisuales o electrónicas deberán ser exhibidos públicamente durante la audiencia de juicio, garantizándose su reproducción por medios idóneos para que sean perceptibles por los asistentes.

Este procedimiento de lectura pública y exhibición no solo se aplica a documentos escritos o físicos, sino también a fotografías, grabaciones, y otros elementos de prueba de naturaleza electrónica como videos o audios obtenidos de dispositivos móviles o computadoras, los cuales pueden ser reproducidos en su parte pertinente. Aunque esta regulación está pensada para el ámbito civil, en los procesos penales, donde el acceso y manejo adecuado de la prueba digital puede ser decisivo, estas disposiciones resultan altamente relevantes.

Por ejemplo, en casos penales que involucran delitos informáticos o fraudes electrónicos, la exhibición de pruebas digitales es clave para reconstruir los hechos, como en la presentación de correos electrónicos que muestren la planificación de un delito o la reproducción de grabaciones de cámaras de seguridad que capten la ejecución del acto criminal. De manera similar, los mensajes de texto intercambiados entre personas involucradas en un crimen pueden ser determinantes para establecer la culpabilidad o inocencia de un acusado.

Además, el artículo 202 introduce una normativa crucial sobre los documentos digitales.[62] Se establece que los documentos que han sido producidos electrónicamente al igual que sus anexos, son considerados originales para todos los efectos legales. Esta disposición refleja un avance significativo en la adaptación del sistema legal ecuatoriano a la realidad digital, al reconocer la validez jurídica de las pruebas electrónicas y su capacidad para sustituir los documentos físicos. La equiparación de los documentos escaneados o

[61] Ibíd., art. 196.
[62] Ibíd., art. 202.

digitalizados a los originales es un factor determinante, especialmente en el derecho penal, donde la integridad de la prueba es esencial para garantizar un debido proceso.

Capítulo segundo
Análisis comparativo de los procedimientos de prueba digital

La globalización y el avance de las tecnologías de la información han generado la necesidad de adaptar los procedimientos judiciales al manejo de pruebas digitales, cuyo tratamiento plantea desafíos únicos en términos de validez, admisibilidad y seguridad jurídica. Este capítulo se enfoca en el análisis comparativo de los procedimientos aplicables a la prueba digital en diferentes jurisdicciones, destacando similitudes, diferencias y buenas prácticas.

A través de este análisis, se identifican los estándares internacionales y las normativas más avanzadas que regulan este tipo de evidencia, con el objetivo de ofrecer una perspectiva amplia que permita evaluar la posición del Ecuador en este ámbito. Asimismo, se exploran los retos asociados al uso de herramientas tecnológicas, la interoperabilidad de sistemas y el resguardo de derechos fundamentales en los procesos judiciales que involucran pruebas digitales.

2.1.Estándares internacionales para la gestión de evidencia digital

Los estándares internacionales para la gestión de evidencia digital han sido desarrollados para garantizar la autenticidad, integridad y validez de este tipo de pruebas en los procedimientos judiciales. Organismos como la Organización Internacional de Normalización (ISO) y la Red Internacional de Capacitación en Ciberdelincuencia (INTERPOL) han establecido lineamientos técnicos y procedimentales que regulan la recopilación, preservación, análisis y presentación de pruebas digitales. Por ejemplo, la norma ISO/IEC 27037 establece pautas específicas sobre la identificación, la adquisición y la preservación de evidencia digital, asegurándose que estos procedimientos minimicen el riesgo de alteración y mantengan la cadena de custodia. Estos estándares permiten que la evidencia sea aceptada en tribunales nacionales e internacionales, independientemente de su procedencia o jurisdicción, siempre que se cumpla con los requisitos de documentación y trazabilidad.

Un principio fundamental en la gestión de evidencia digital es la preservación de la cadena de custodia, que garantiza que los elementos probatorios no sean manipulados desde su recolección hasta su presentación en juicio. Organismos internacionales como el Consejo

de Europa, a través del Convenio de Budapest sobre Ciberdelincuencia, enfatizan la importancia de procedimientos claros y consistentes para la transferencia de pruebas digitales entre autoridades competentes. Esto incluye el uso de herramientas tecnológicas certificadas para la recolección de datos, así como la designación de personal capacitado en el manejo de este tipo de pruebas. La gestión adecuada de la evidencia digital bajo estándares internacionales no solo fortalece su admisibilidad en procesos judiciales, sino que también refuerza la confianza en los sistemas de justicia que la emplean.

2.2. Normativas internacionales relevantes

El Convenio de Budapest sobre Ciberdelincuencia[63] y su Segundo Protocolo Adicional[64] constituyen instrumentos clave para enfrentar de forma efectiva los delitos informáticos, estableciendo un marco normativo armonizado que facilita la cooperación internacional en materia penal. Este tratado, pionero en su campo, busca dotar a los Estados firmantes de medidas legislativas y operativas adecuadas para combatir las crecientes amenazas digitales que trascienden fronteras.

En el artículo 14 del Título I (Disposiciones comunes), se aborda el alcance de las medidas de derecho procesal aplicables en el procedimiento penal. Establece la obligación de que los Estados adopten normas internas que otorguen a sus autoridades facultades eficaces para investigar delitos informáticos y manejar pruebas electrónicas. Esta necesidad responde al aumento de conductas delictivas cometidas mediante sistemas informáticos, que requieren una respuesta jurídica adecuada y coordinada.

El Convenio no se limita a delitos en específico previstos en sus artículos del 2 hasta el 11 —como el acceso no autorizado a sistemas, la interferencia en datos o redes, o la difusión de material pornográfico infantil—. En cambio, se extiende a todo delito que utilice plataformas digitales como medio de comisión, permitiendo así una cobertura legal amplia. Asimismo, se prevé la recolección de evidencia digital, incluso en casos de delitos comunes, siempre que se requiera garantizar la eficacia del proceso penal.[65]

---

[63] Consejo de Europa, *Convenio de Budapest sobre la Ciberdelincuencia*, Serie de Tratados No. 185 (2001), https://rm.coe.int/1680081561

[64] Consejo de Europa, *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas*, Diario Oficial de la Unión Europea L 63/28 (2023), https://rm.coe.int/1680a83724&ved=2ahUKEwivgsPul8yNAxXVSTABHUz-AM0QFnoECAkQAQ&usg=AOvVaw0hIEEFou2J0gg7J_iZj83v

[65] Ibíd.

El Segundo Protocolo Adicional amplía estas disposiciones mediante el artículo 12, que promueve la colaboración directa entre autoridades nacionales por medio de la conformación de equipos de investigación y la ejecución de investigaciones cooperativas. Esta herramienta resulta esencial ante el carácter transnacional de la ciberdelincuencia, pues permite superar los obstáculos jurisdiccionales mediante mecanismos que faciliten la coordinación entre Estados para el esclarecimiento de los hechos y la recolección de evidencia digital válida.

La cibercriminalidad comprende todos aquellos delitos que se cometen al utilizar las tecnologías de la información y comunicación (TIC), al incluir internet, dispositivos electrónicos y redes digitales. Este fenómeno ha experimentado un crecimiento exponencial a medida que las tecnologías digitales han ganado presencia en casi todos los aspectos de la vida cotidiana. Una de las características más distintivas de la cibercriminalidad es su naturaleza desterritorializada, lo que permite a los perpetradores operar desde cualquier lugar del mundo sin restricciones geográficas. Además, el anonimato que ofrecen las herramientas digitales y la dificultad para rastrear las actividades ilícitas complican significativamente su prevención y persecución.

Este tipo de delitos abarca una extensa variedad de actividades ilegales, que incluyen desde las defraudaciones electrónicas y robo de identidad hasta el acceso violatorio a sistemas informáticos, propagación de software malicioso, acoso en línea, explotación infantil y trata de personas. La diversidad de los cibercrímenes refleja tanto la versatilidad de las tecnologías utilizadas como la creatividad de los delincuentes, quienes aprovechan las vulnerabilidades de los sistemas para sus propios fines. Entre las víctimas más afectadas se encuentran los menores, especialmente vulnerables a crímenes como la explotación sexual en línea. Este hecho resalta la importancia de implementar políticas públicas que prioricen la prevención, la educación y la concienciación, protegiéndose a los grupos más expuestos.

El impacto de la cibercriminalidad no se limita únicamente a las víctimas individuales, sino que tiene consecuencias sociales y económicas significativas. Delitos como el fraude financiero y el robo de identidad generan pérdidas monetarias considerables, tanto para las personas afectadas como para las instituciones involucradas. Los ciberdelincuentes emplean técnicas sofisticadas, como la clonación de huellas dactilares o el acceso a bases de datos personales, para llevar a cabo sus acciones ilícitas, lo que pone en evidencia la urgencia de adoptar medidas más robustas para la protección de datos.

En el ámbito jurídico, los desafíos que plantea la cibercriminalidad son igualmente complejos. Muchos países aún carecen de un marco normativo completamente adaptado para abordar estos delitos, lo que dificulta la regulación, investigación y persecución efectiva de los mismos. Se requiere una actualización legislativa tanto a nivel nacional como internacional, dado que la naturaleza global de estos crímenes supera las capacidades de las jurisdicciones tradicionales. Asimismo, el tratamiento de los delitos cibernéticos exige un enfoque especializado debido a su carácter técnico y su impacto transfronterizo, lo que implica el desarrollo de estrategias específicas tanto para su prevención como para la autoprotección.

En el marco del segundo protocolo adicional al convenio, se promueve la formación de equipos conjuntos para fortalecer la cooperación internacional en la investigación penal. El objetivo es facilitar la coordinación entre Estados en la recolección de pruebas, el intercambio de información y el procesamiento ágil de los responsables. No obstante, para salvaguardar la soberanía de cada Estado y los derechos de las personas implicadas, se establecen restricciones respecto al empleo de la información obtenida mediante estos acuerdos.

El artículo 12 del Protocolo define que la utilización de pruebas e información facilitadas por una de las partes puede limitarse conforme a lo estipulado en el acuerdo de cooperación. En ausencia de condiciones específicas, la información puede utilizarse conforme al fin inicial o, con autorización, para investigar otros delitos. Dicha autorización no será necesaria cuando el uso de la información sea imprescindible para garantizar los derechos del acusado, según los principios jurídicos del Estado receptor. Asimismo, en situaciones de emergencia, se permite el uso inmediato de la información, siempre que se notifique a la Parte que la proporcionó, sin demoras injustificadas. Este marco busca equilibrar la eficacia de la cooperación internacional con la protección de los principios legales y derechos fundamentales.[66]

Esta norma enfatiza una gestión rigurosa desde la identificación de los elementos relevantes, evitando la recolección excesiva o irrelevante que comprometa la privacidad o carezca de valor jurídico. Durante la adquisición de la evidencia, se requieren procedimientos técnicos y legales que aseguren la integridad de los datos, garantizando que estos no se vean alterados ni manipulados. Finalmente, la preservación de la evidencia exige medidas estrictas para su almacenamiento y conservación, de manera que permanezca

[66] Ibíd., art.12

inalterada y segura frente a riesgos tecnológicos. Así, se garantiza que pueda ser admitida y utilizada eficazmente en los procesos judiciales.

En paralelo, la gestión adecuada de la evidencia digital se ha convertido en un componente clave de las investigaciones forenses, dada la expansión de las tecnologías digitales y de los delitos informáticos. Ante este desafío, se requiere un marco normativo sólido que asegure la validez de las pruebas en los procedimientos judiciales. En este contexto, la norma internacional ISO/IEC 27037:2012 ofrece lineamientos para la identificación, adquisición, preservación y análisis de las evidencias digitales.[67]

Esta norma enfatiza una gestión rigurosa desde la identificación de los elementos relevantes, evitando la recolección excesiva o irrelevante que comprometa la privacidad o carezca de valor jurídico. Durante la adquisición de la evidencia, se requieren procedimientos técnicos y legales que aseguren la integridad de los datos, garantizando que estos no se vean alterados ni manipulados. Finalmente, la preservación de la evidencia exige medidas estrictas para su almacenamiento y conservación, de manera que permanezca inalterada y segura frente a riesgos tecnológicos. Así, se garantiza que pueda ser admitida y utilizada eficazmente en los procesos judiciales.

La preservación de evidencias digitales representa un pilar esencial en la informática forense, dado que garantiza que los datos recolectados durante una investigación mantengan su integridad, autenticidad y validez. Este proceso no solo se centra en asegurar que la información sea admisible en los procedimientos legales, sino también en preservar su valor probatorio a lo largo de todas las etapas de análisis y presentación en un tribunal. En un entorno donde la mayoría de las actividades humanas tienen un componente digital, la preservación adecuada de estas evidencias se ha convertido en un desafío técnico y jurídico de gran relevancia, ya que cualquier alteración, por mínima que sea, puede comprometer la credibilidad de los resultados y, en consecuencia, el éxito de una investigación.

El proceso comienza con la identificación de las evidencias digitales, un paso crítico que implica reconocer los dispositivos y fuentes de datos potencialmente relevantes. Esto abarca desde ordenadores personales, teléfonos móviles y discos duros externos hasta servicios en la nube, redes sociales y dispositivos conectados a Internet de las cosas (IoT). En esta etapa, los investigadores deben contar con un conocimiento profundo sobre las

[67] Santiago Roatta, María Eugenia Casco y Martin Fogliatto, "El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012", XXI Congreso Argentino de Ciencias de Computación (Junín, 2015), https://sedici.unlp.edu.ar/handle/10915/50586.

tecnologías actuales y las posibles ubicaciones de los datos, pues cualquier omisión puede llevar a la pérdida de información crucial.

Una vez identificadas las evidencias, se realiza su recopilación, etapa en la que se utilizan técnicas altamente especializadas para extraer los datos sin alterar su contenido original. Este procedimiento puede implicar la creación de imágenes forenses, que son copias exactas de los discos duros o dispositivos de almacenamiento, o la captura de datos en tiempo real, por ejemplo, en servidores o sistemas que están en funcionamiento. Es fundamental que esta extracción se lleve a cabo con herramientas certificadas y siguiéndose protocolos estrictos que aseguren que la manipulación sea mínima, preservándose así la autenticidad de los datos recolectados. Además, en esta fase se documenta cada acción realizada, lo que garantiza una cadena de custodia robusta que respalde la fiabilidad de las evidencias.

Posteriormente, los datos recopilados pasan a la etapa de preservación, donde se adoptan medidas para mantener la integridad de las evidencias durante todo el tiempo que dure la investigación. Esto incluye el almacenamiento en condiciones controladas, como medios de almacenamiento inmutables y entornos seguros que protejan la información contra accesos no autorizados, corrupción de datos o daños físicos. Además, se emplean herramientas y técnicas avanzadas, como el uso de hash criptográficos, que permiten verificar que los datos no han sido alterados desde su recolección. Estos métodos son indispensables para garantizar que cualquier cambio accidental o intencionado pueda ser detectado, lo que refuerza la confianza en la validez de las evidencias presentadas.

El análisis de las evidencias digitales constituye una etapa igualmente crucial. En este punto, los datos recolectados son examinados mediante métodos forenses que permiten extraer información relevante para el caso en cuestión. Este análisis debe ser reproducible y detalladamente documentado, de forma que pueda ser revisado por otros expertos o defendido en un juicio. Aquí, la precisión es clave, ya que incluso los errores más pequeños pueden dar lugar a interpretaciones incorrectas o a la descalificación de las evidencias por parte de las autoridades judiciales.

La calidad del proceso de preservación es un elemento determinante en la admisibilidad de las evidencias digitales en un juicio. Como explica Martínez: “la admisibilidad de la prueba electrónica debe cumplir los requisitos exigidos a cualquier otro medio de prueba: pertinencia, utilidad y licitud.”[68] Desde este punto de vista, los errores en

[68] Gemma Martínez, “Problemática jurídica de la prueba digital”, 23.

cualquiera de las etapas, ya sea durante la identificación, recopilación, almacenamiento o análisis, pueden comprometer la validez de las pruebas y afectar significativamente el resultado de una investigación legal. Por este motivo, es fundamental que los equipos forenses sigan estándares internacionales, como los establecidos por organizaciones como la ISO/IEC, y que se sometan a auditorías regulares para garantizar el cumplimiento de las mejores prácticas en cada procedimiento. Estas normativas no solo aseguran la consistencia y fiabilidad del trabajo forense, sino que también fortalecen la credibilidad de las evidencias frente a posibles cuestionamientos legales.

El avance constante de la tecnología ha transformado la informática forense, al introducir herramientas y metodologías innovadoras que optimizan tanto la preservación como el análisis de las evidencias digitales. La inteligencia artificial, por ejemplo, ha revolucionado el campo al permitir la automatización de procesos complejos, como la identificación de patrones en grandes volúmenes de datos o la detección de anomalías que podrían pasar desapercibidas mediante técnicas tradicionales. Asimismo, la tecnología *blockchain* se ha integrado como un recurso útil para registrar las acciones realizadas sobre los datos en un sistema inmutable y transparente, ofreciéndose una protección adicional contra manipulaciones.

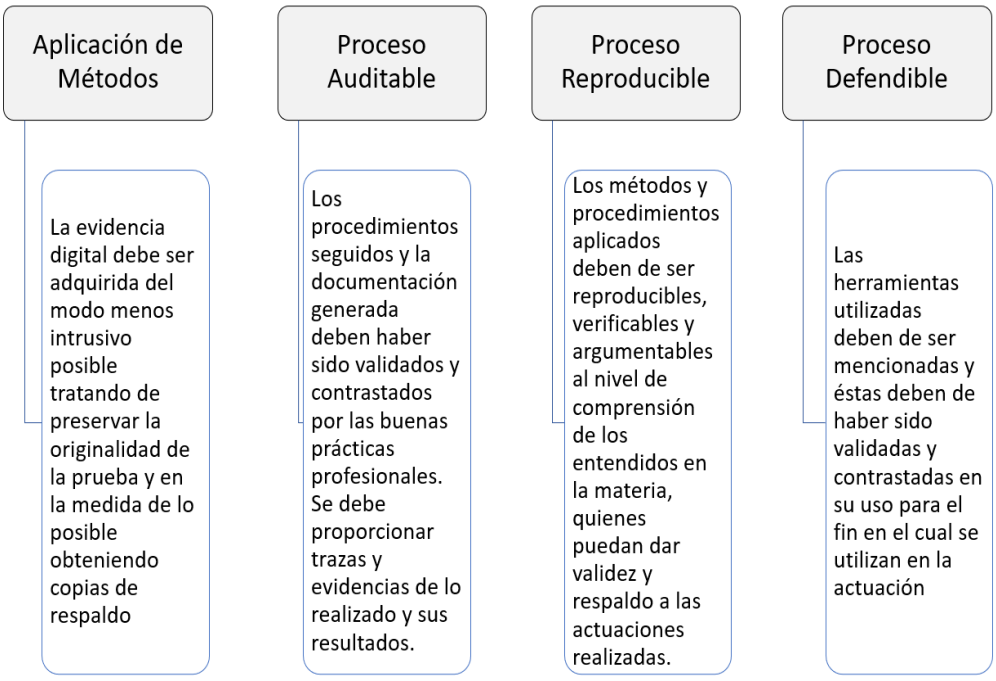
Por otro lado, la creciente adopción de servicios en la nube y dispositivos IoT plantea nuevos retos y oportunidades para la informática forense. Estas tecnologías generan cantidades masivas de datos distribuidos en diferentes ubicaciones y plataformas, lo que requiere enfoques adaptativos para su recolección y análisis. El desarrollo de herramientas específicas para la captura y preservación de datos en estos entornos es fundamental, ya que su complejidad técnica demanda habilidades y conocimientos avanzados por parte de los investigadores.

En este contexto, la norma ISO/IEC 27037:2012 no repercute directamente en el ámbito de las investigaciones forenses, pero también influye en la forma en que los sistemas de justicia incorporan y valoran la prueba digital. Su incorporación en marcos normativos como el Código General del Proceso colombiano, evidencia la necesidad de asumir prácticas internacionales reconocidas para garantizar la correcta recolección, tratamiento y examen de dicha evidencia. La integración de estos protocolos estandarizados permite a jueces y operadores jurídicos evaluar la prueba digital conforme a criterios objetivos de calidad internacionalmente aceptados, fortaleciendo la legitimidad del proceso judicial y

minimizando el riesgo de que la evidencia sea desestimada por vicios en su obtención o manejo.[69]

El estándar desarrollado `por la ISO, exige que las evidencias sean: a) relevancia, porque deben permitir la vinculación del sospechoso con el delito y la víctima; b) confiables, ya que las técnicas utilizadas para la extracción de la evidencia han debido ser probadas previamente y c) suficientes, puesto que el acopio de evidencias debe dirigirse a respaldar y confirmar el resto de presunciones, pruebas y otros indicios del delito, de modo que se debe examinar la totalidad de los dispositivos electrónicos hallados y vinculados con el delito. [70]

En Ecuador, la creciente incidencia de ciberdelitos ha incrementado la relevancia de implementar estándares internacionales en el ámbito de la forensia digital, como la norma ISO/IEC 27037:2012. Esta norma establece líneas esenciales para identificar, recolectar, preservr y analizar la evidencia digital, aspectos críticos en un contexto donde delitos como la ciberextorsión son cada vez más comunes. En estos casos, la investigación forense de dispositivos móviles, particularmente aquellos con sistema operativo Android, ha puesto de manifiesto la urgente necesidad de procedimientos actualizados y estandarizados que respondan a los desafíos específicos que enfrenta el país.



[69] Organización Internacional de Normalización, "ISO/IEC 27041:2015 Tecnologías de la información-tecnologías de la seguridad: Directrices para asegurar la adecuación de métodos de investigación de incidentes", *Amnafzar*, https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027041-2015.pdf.

[70] Gemma Martínez "Problemática jurídica de la prueba digital", 13-14.

Figura 1. Definición de los principios básicos para identificación, recolección, adquisición y preservación de la evidencia digital, según ISO/IEC 27037:2012. Elaboración propia

El desarrollo de un procedimiento forense basado en la norma ISO/IEC 27037:2012 está orientada a garantizar la eficacia en la identificación de evidencia digital, la recolección adecuada de datos de dispositivos móviles, la preservación íntegra de la información recopilada y su análisis conforme a estándares que aseguren su admisibilidad en procesos legales. Esta estandarización no solo mejora la confiabilidad de la evidencia presentada en los tribunales ecuatorianos, sino que también establece una base uniforme que facilita el trabajo de los investigadores forenses en todo el país. Al adoptar estos estándares internacionales, Ecuador fortalece la efectividad de las investigaciones digitales, al tiempo que fomenta la formación continua de especialistas en forensia digital.

La implementación de la norma ISO/IEC 27037:2012 también tiene el potencial de generar múltiples beneficios. En primer lugar, promueve la estandarización de los procesos forenses, lo que asegura un manejo uniforme y riguroso de la evidencia digital, indispensable para garantizar su validez en procedimientos judiciales. En segundo lugar, refuerza la admisibilidad legal de dicha evidencia, incrementándose su aceptación en los tribunales y, por ende, la posibilidad de resolver casos de manera más efectiva. Además, la aplicación de esta norma proporciona un marco sólido para la capacitación de profesionales, al elevar el nivel de preparación técnica en un campo que evoluciona constantemente. Finalmente, facilita la cooperación internacional, al permitir que las agencias ecuatorianas trabajen de manera más eficiente con entidades extranjeras que emplean los mismos estándares, lo cual resulta crucial en la lucha contra el cibercrimen, dado su carácter transnacional.

El constante avance de las tecnologías y la aparición de nuevas modalidades delictivas, como la ciberextorsión y los fraudes electrónicos, han impulsado el desarrollo de procedimientos forenses adaptados a distintos dispositivos y plataformas. En el caso de teléfonos móviles con sistema Android, se han diseñado procedimientos específicos para recolectar datos de aplicaciones, registros de redes sociales, historial de navegación y otros elementos esenciales en investigaciones sobre delitos digitales. Estos procedimientos no solo modernizan las metodologías forenses tradicionales, sino que

también integran herramientas tecnológicas innovadoras que responden a la dinámica cambiante del entorno digital.[71]

Paralelamente, la digitalización creciente de la evidencia —por ejemplo, el almacenamiento en la nube, así como el análisis de amplios volúmenes de información (*big data*)— representa importantes retos para su preservación, análisis e interpretación. Frente a esta realidad, el marco normativo debe actualizarse constantemente para asegurar que las metodologías forenses mantengan su validez jurídica y su eficacia investigativa. En este contexto, normas como la ISO/IEC 27037:2012 y otras afines resultan esenciales, pues fortalecen el trabajo técnico de peritos e investigadores y garantizan que el proceso judicial respete los principios del debido proceso.

Por su parte, la ISO/IEC 27042:2015 se enfoca específicamente en el análisis e interpretación de la evidencia digital.[72] Establece procedimientos claros que orientan a los especialistas desde la identificación inicial de los datos hasta su presentación final en juicio. Esta norma pone especial énfasis en la conservación de la cadena de custodia y en la integridad de la evidencia a lo largo de toda la investigación. Al estandarizar cada fase, se facilita que los resultados sean comprensibles para jueces y abogados, incluso si no cuentan con formación técnica, asegurando así una adecuada utilización de la prueba digital en los procesos judiciales.

La ISO/IEC 27043:2015, en cambio, aborda el proceso integral de la investigación forense digital. Define un marco metodológico que permite estandarizar las actuaciones ante distintos escenarios, incluidos aquellos casos complejos o excepcionales. Esta norma también contempla la transferencia de evidencia entre diferentes jurisdicciones, algo crucial en investigaciones internacionales, en las que se requiere cooperación entre múltiples actores. Su aplicación garantiza no solo la preservación de la evidencia, sino también la eficiencia y coherencia del proceso investigativo, promoviendo así una colaboración fluida entre instituciones y reforzando el acceso a justicia en un contexto cada vez más interconectado.

---

[71] Danilo Banegas y Daniel Andrade, "Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura", *MQRInvestigar* 8, n.° 3 (2022): 4076-97, doi: 10.56048/mqr20225.8.3.2024.4076-4097.

[72] Organización Internacional de Normalización, "ISO/IEC 27041:2015".

2.3. Buenas prácticas en la obtención y manejo de prueba digital

La norma ISO/IEC 27037:2012 se establece como la principal referencia en la gestión de la evidencia digital, siendo la base sobre la cual se sustenta todo el trabajo en este campo. Dicha norma ofrece un conjunto de directrices precisas para la correcta manipulación de la evidencia digital, poniendo énfasis en etapas fundamentales como su identificación, recolección, adquisición y su conservación[73].

La finalidad central de los procesos normativos descritos consiste en asegurar que la evidencia digital se gestione de manera íntegra, siguiendo metodologías aceptadas internacionalmente, lo cual es determinante para su admisión en instancias judiciales. En coherencia con esto, la norma establece tres principios esenciales que deben regir toda investigación digital: relevancia, confiabilidad y suficiencia. Estos principios constituyen el fundamento metodológico que garantiza que la recolección y uso de evidencia digital se realice con formalidad, rigurosidad técnica y dentro de parámetros estandarizados.

La norma ISO/IEC 27037:2012, además, extiende sus lineamientos más allá del ámbito digital, al incluir directrices para la recolección de evidencia no digital que pueda ser clave en el análisis forense.[74] Su orientación está dirigida a diversos perfiles profesionales, entre ellos el *Digital Evidence First Responder* (DEFR), el *Digital Evidence Specialist* (DES), los expertos en respuesta a incidentes y los responsables de laboratorios forenses. Su finalidad es estandarizar las prácticas para que la gestión de la evidencia se desarrolle con imparcialidad, precisión técnica y en resguardo de la autenticidad e integridad de la información recopilada.[75]

Es importante aclarar que esta norma no regula los aspectos legales ni disciplinarios vinculados a un mal manejo de la evidencia digital. En su lugar, remite expresamente al cumplimiento de las leyes y normativas vigentes en cada jurisdicción, dejando en claro que no sustituye los requisitos legales propios de cada país. Aunque no aborda en detalle temas como la admisibilidad o valoración jurídica de la prueba, sí proporciona un marco operativo común que facilita el intercambio transnacional de evidencia digital, permitiendo que sus procedimientos sean adaptados a los marcos normativos locales. De esta manera, se

---

[73] Ibíd.

[74] Ibid.

[75] ONU. *Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020*, *UN,* 6 de abril de 2021, https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101015.pdf

promueve una cooperación internacional eficaz en investigaciones que involucren tecnologías digitales.

El concepto de Cadena de Custodia (Chain of Custody o CoC) es uno de los aspectos más críticos en el manejo de la evidencia digital, pues en esta fase deben cumplirse un grupo de requisitos para garantizar la validez de la prueba. Entre esos requisitos se incluye la asignación de un identificador único para cada pieza, un registro claro y preciso de quién, cuándo y dónde se accede a dicha evidencia, así como del régimen de traslado de un lugar a otro y las acciones realizadas. Absolutamente cualquier cambio en la evidencia digital deberá ser registrado rigurosamente, definiendo los datos identificativos del responsable y la clara justificación clara de las acciones que ejecutó. Todo ello certifica la trazabilidad y autenticidad de la evidencia durante todo el proceso.

La cadena de custodia, más allá de ser un procedimiento técnico, se erige como un pilar fundamental en la garantía del debido proceso dentro del sistema judicial. Su objetivo principal es garantizar que los materiales probatorios presentados durante un juicio sean auténticas, al haberse preservado de toda alteración, contaminación o manipulación en ningún momento de su manejo, almacenamiento o transporte. Esto no solo preserva la integridad de las pruebas, sino que también protege los derechos de las personas involucradas en el proceso, asegurándose que no se dicten sentencias basadas en evidencias que hayan perdido su fiabilidad. En última instancia, la cadena de custodia se convierte en un mecanismo de confianza para el sistema judicial, al validar que los resultados del juicio sean legítimos, justos y respetuosos con los derechos fundamentales de los acusados.

Una de las funciones clave de una cadena de custodia adecuadamente gestionada es garantizar la valoración precisa de las pruebas por parte de los tribunales y la Fiscalía. Esta valoración, que debe basarse en la autenticidad de las evidencias, es un proceso crucial para determinar si las pruebas presentadas en juicio son las mismas que se recolectaron en la escena del crimen. La correcta aplicación de la cadena de custodia permite verificar que las pruebas no han sido manipuladas en ninguna etapa de su recolección, lo que facilita su admisión en el juicio y asegura que la decisión judicial se fundamente en hechos que han sido recolectados y preservados de acuerdo con los estándares legales establecidos. De este modo, se contribuye al mantenimiento de un proceso transparente, en el que las evidencias no puedan ser cuestionadas por su autenticidad o por su manejo indebido.[76]

[76] Mario Guerra Soto, *Análisis Forense Informático*. (Ediciones Ra-Ma.:2021), 60-1, https://www.ra-ma.es/media/rama/files/book-attachment-6367.pdf

La protección de la cadena de custodia también tiene implicaciones directas en la lucha contra la impunidad. Si se permite que la cadena de custodia sea vulnerada o ignorada, existe el riesgo de que las pruebas puedan ser descalificadas, lo que podría resultar en la absolución de acusados que, bajo condiciones normales, podrían haber sido condenados. Este hecho subraya la importancia de mantener una rigurosidad y disciplina en el manejo de las pruebas desde su recolección hasta su presentación ante el tribunal. El cumplimiento estricto de este proceso asegura que, en caso de que una persona sea condenada, la decisión esté basada en pruebas que se hayan mantenido intactas a lo largo del proceso, evitándose que la corrupción o negligencia en el manejo de las evidencias pueda modificar el curso de la justicia.[77]

El papel de la policía en el mantenimiento de la cadena de custodia es igualmente esencial, ya que es la institución encargada de iniciar y supervisar la preservación de las evidencias desde su recolección en la escena del crimen. La policía tiene la responsabilidad de garantizar que los indicios sean protegidos adecuadamente, al registrar cada paso del proceso, desde el momento de su descubrimiento hasta su traslado y almacenamiento. La falta de un registro adecuado o el manejo inadecuado de las pruebas puede poner en peligro todo el caso, ya que cualquier irregularidad podría ser utilizada por la defensa para cuestionar la validez de las pruebas presentadas. Por lo tanto, la policía no solo es responsable de la recolección de las evidencias, sino también de garantizar que su manejo se ajuste a los protocolos establecidos, asegurándose que se cumplan todas las normativas que permiten que las pruebas sean admisibles ante el tribunal.[78]

Para que la cadena de custodia sea realmente efectiva, resulta esencial contar con procedimientos estandarizados y claros que guíen a los agentes encargados del manejo de las pruebas en cada etapa del proceso. Estos protocolos deben definir con precisión las pautas a seguir en la recolección, el transporte, el almacenamiento y la documentación de las evidencias. Asimismo, deben incluir las precauciones necesarias para garantizar que las pruebas no sean contaminadas ni manipuladas, ya sea de forma accidental o intencional. La estandarización de estos procedimientos garantiza que todos los participantes en la cadena de custodia operen bajo un marco normativo común, lo cual disminuye la probabilidad de

[77] María de Lourdes Mendoza Prado, "Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal", *Código Científico Revista De Investigación 5, Nº* E3(2024), 480–498. https://doi.org/10.55813/gaea/ccri/v5/nE3/328

[78] Cléver Tene Lema y Diego Armando xPilco Pucha, "El manejo de la cadena de custodia como requisito fundamental para la legitimidad probatoria de los procedimientos administrativos disciplinarios de la Policía Nacional" (Tesis de maestría, Universidad de Chimborazo, 2023), http://dspace.unach.edu.ec/handle/51000/11333

errores y asegura un manejo consistente y seguro de las evidencias. De este modo, se reducen los riesgos de que cualquier irregularidad en el proceso pueda comprometer la validez de las pruebas y, en consecuencia, la imparcialidad del juicio.

Las implicaciones legales derivadas de una violación de la cadena de custodia son profundas y pueden tener consecuencias significativas en el resultado del juicio. La alteración o pérdida de validez de una prueba crucial puede tener un impacto devastador en una investigación, al invalidar pruebas que podrían ser determinantes para la condena de un acusado. Esta pérdida de credibilidad afecta no solo la integridad del caso en cuestión, sino también la confianza en el sistema judicial en su conjunto. En algunos casos, la violación de la cadena de custodia puede llevar a la desestimación de un caso completo o a la absolución de un acusado, incluso si las pruebas eran suficientes para demostrar su culpabilidad. La posibilidad de que un caso se vea afectado por un manejo inadecuado de las pruebas refuerza la necesidad de mantener una estricta vigilancia y cumplimiento de los procedimientos establecidos, ya que, de no hacerlo, se corre el riesgo de que personas culpables queden en libertad debido a fallos procesales que no tienen relación con el fondo del caso.

Los principios fundamentales que rigen el manejo de pruebas digitales constituyen el pilar de toda investigación forense en entornos tecnológicos. Uno de los más importantes es el principio de mismidad, el cual establece que la evidencia digital recolectada debe ser idéntica a la que será presentada ante el tribunal. Es decir, no puede haber alteraciones ni modificaciones en el contenido desde el momento de su obtención hasta su uso en juicio. Este principio exige una manipulación sumamente cuidadosa de la evidencia, ya que cualquier mínima variación podría comprometer su validez, poner en entredicho los hallazgos del proceso investigativo o incluso derivar en su exclusión como prueba judicial.[79]

Otro principio esencial es la autenticidad, que garantiza que la evidencia digital provenga de una fuente confiable y que no haya sido manipulada. Este principio permite demostrar que la prueba es genuina y que puede asociarse de manera inequívoca con el hecho o la persona investigada. La autenticidad es especialmente relevante cuando se trata de datos obtenidos de dispositivos personales como teléfonos móviles, correos electrónicos o cuentas de redes sociales, que contienen información privada y sensible. Si existe

[79] Orlando J. Pacheco, "Principio probatorio de mismidad en el Código Orgánico Procesal Penal venezolano. Una hermeneusis del derecho probatorio" *Revista Escandalar Investigativa,* No. 2 (2024): 165-177: http://revistas.unellez.edu.ve/index.php/resi/article/view/2581/2299

cualquier sospecha de manipulación o falta de fiabilidad en la fuente, la evidencia podría ser cuestionada, lo que afectaría la credibilidad de toda la investigación.[80]

La originalidad es también un principio central en el tratamiento de evidencias digitales. Este principio establece la importancia de trabajar con la prueba original en lugar de una copia, siempre que sea posible, para evitar dudas sobre su integridad. En casos en que sea necesario realizar una copia, como cuando el dispositivo original es demasiado frágil o valioso, se debe utilizar una metodología que asegure que la copia es exacta, como el uso de herramientas de clonación de discos. El análisis de una prueba digital original proporciona un nivel de certeza más elevado, ya que garantiza que la información no ha sufrido alteraciones ni degradaciones durante el proceso de duplicación.

Los principios fundamentales que regulan la admisión y evaluación de la prueba digital son cruciales para asegurar la justicia y la equidad en los procedimientos judiciales. Uno de los principios más destacados es el de licitud, el cual estipula que cualquier prueba digital debe ser obtenida de manera legal, sin vulnerar derechos fundamentales como la intimidad de las personas, la confidencialidad de las comunicaciones y la preservación de los datos personales. Este principio tiene como objetivo salvaguardar la privacidad de los individuos y garantizar que el proceso judicial se desarrolle de acuerdo con el respeto a los derechos humanos.

Otro principio clave es la pertinencia, que señala que la prueba digital debe ser relevante y útil para acreditar los hechos en disputa dentro de un proceso. Esto implica que solo se podrán presentar aquellas pruebas que tengan una relación directa con los hechos del caso, evitándose la presentación de pruebas que no aporten valor al esclarecimiento de la verdad. A la par, la autenticidad es fundamental, ya que se debe garantizar que la prueba digital es genuina y no ha sufrido alteraciones o manipulaciones que puedan afectar su veracidad y fiabilidad. La autenticidad asegura que la información obtenida refleja de manera fiel los hechos ocurridos.

La integridad desempeña un papel fundamental, dado que establece que la prueba digital debe conservarse en su totalidad, sin alteraciones desde su obtención hasta su presentación ante el tribunal. Esto asegura que la prueba permanezca inalterada y no se vea comprometida a lo largo del proceso judicial. De manera complementaria, el principio de contradicción impone que ambas partes del proceso cuenten con la oportunidad de

[80] William Twinning, *Repensar el derecho probatorio. Ensayos exploratorios,* (Editorial de la Universidad Nacional de Colombia, 2022)

examinar y refutar la prueba digital presentada, lo que salvaguarda el derecho a la defensa y a un juicio equitativo.

El principio de publicidad establece que las pruebas digitales deben ser accesibles a todas las partes implicadas en el proceso, e incluso, en ciertos casos, al público en general, a menos que existan excepciones debidamente fundamentadas. Este principio garantiza la transparencia del proceso judicial. Por otro lado, el principio de inmediación requiere que el juez esté presente en la exposición y el análisis de la evidencia digital, lo que posibilita una valoración directa y objetiva de la misma. Finalmente, el principio de libre valoración concede al juez la facultad de interpretar la prueba digital de acuerdo con su convicción, al tener en cuenta los elementos del caso y los principios de lógica, ciencia y experiencia. Esto otorga al juez la libertad de valorar la prueba en su conjunto, sin estar atado a reglas rígidas, y al ajustar su decisión a las circunstancias específicas del caso[81].

A fin de cumplir con estos principios, es imprescindible seguir una serie de procedimientos rigurosos durante la recolección de la evidencia. La cadena de custodia es uno de los procedimientos más críticos en este contexto y consiste en llevar un registro minucioso de todas las personas que han manejado la evidencia, así como los lugares y momentos en que ha sido almacenada y transferida. Este procedimiento permite demostrar, en cualquier momento, que la prueba ha sido protegida de cualquier tipo de alteración o manipulación no autorizada. Mantener una cadena de custodia bien documentada ayuda a preservar la confianza del tribunal en la evidencia y en el proceso de investigación, y garantiza que la prueba no será desestimada por falta de integridad.[82]

El embalaje adecuado es otro procedimiento clave en la conservación de pruebas digitales. Dado que muchos dispositivos digitales son sensibles a factores externos como el daño físico y la interferencia electromagnética, es fundamental que estos dispositivos sean almacenados en contenedores específicos que los protejan de dichas amenazas. Los discos duros, teléfonos móviles y otros equipos deben ser empaquetados de manera cuidadosa, al evitar que factores externos comprometan la integridad de los datos almacenados en ellos. Además, los protocolos de embalaje exigen que cada dispositivo esté correctamente identificado y que el contenedor esté sellado de forma que cualquier manipulación posterior

[81] Ana Milena Acevedo Silva y Deyanira Castillo, "La tecnología y el carácter de la notificación personal frente al principio de publicidad" (tesis de maestría, Universidad La Gran Colombia, Bogotá, 2022) https://repository.ugc.edu.co/server/api/core/bitstreams/ed008317-c952-4e6b-ab05-9ef83dc4cfbd/content

[82] Fredy Hernando Toscano López, Juan Carlos Naizir Sistac, Luis Guillermo Acero Gallego, Ramiro Bejarano Guzmán, *Derecho probatorio: desafíos y perspectivas,* (Universidad Externado de Colombia, 2021)

sea evidente. Un embalaje defectuoso podría causar la pérdida o alteración de datos esenciales, lo que comprometería gravemente la eficacia de la evidencia en el juicio.

La documentación meticulosa de cada paso del proceso de recolección de pruebas digitales es igualmente indispensable para asegurar que el procedimiento es rastreable y transparente. Este aspecto de la recolección implica llevar un registro detallado de todas las acciones realizadas desde el primer contacto con la evidencia, al incluir descripciones precisas del entorno en el que fue encontrada, el estado del dispositivo en el momento de su hallazgo, y cualquier intervención llevada a cabo durante el proceso de recolección. La documentación debe capturar todos los detalles, incluso aquellos que podrían parecer irrelevantes, ya que en un tribunal cualquier información adicional puede ser de gran valor para demostrar que la prueba ha sido manejada de manera profesional y cuidadosa.[83]

Además de estos procedimientos específicos, la obtención y manejo de pruebas digitales requieren un alto nivel de competencia técnica y ética por parte de los profesionales involucrados. La manipulación incorrecta de datos o la falta de adherencia a los protocolos podría invalidar la prueba y afectar negativamente la percepción de la investigación en su conjunto. La capacitación continua y el uso de tecnologías avanzadas en el campo de la informática forense son fundamentales para garantizar que las pruebas digitales se manejen adecuadamente en todas las etapas de su recolección y análisis. Asimismo, el respeto por la privacidad de las personas y la confidencialidad de la información recolectada se consideran obligaciones éticas indispensables que deben observarse en todo momento.

El análisis forense en el contexto de las investigaciones digitales y de ciberseguridad es un proceso complejo que requiere de herramientas altamente especializadas para asegurar la precisión y la integridad de los datos obtenidos. Este tipo de análisis se enfoca en recopilar, preservar, examinar e interpretar datos digitales de una manera que sea legalmente admisible y que pueda resistir el escrutinio en un proceso judicial. A propósito de ello, el uso de herramientas de software y hardware forense reconocidas y certificadas es esencial para llevar a cabo un análisis de calidad.[84]

Estas herramientas incluyen tecnologías avanzadas diseñadas para cumplir funciones específicas, como la recuperación de datos eliminados, el análisis detallado de

---

[83] Fredy Hernando Toscano López, Juan Carlos Naizir Sistac, Luis Guillermo Acero Gallego, Ramiro Bejarano Guzmán, *Derecho probatorio: desafíos y perspectivas*

[84] Ronald Estiven Endara Chamorro, Juan Sebastián Espinoza Jiménez, Eder Ronaldo López Fuel y Jessica Johanna Santander Moreno, “Análisis jurídico del deepfake”

archivos y la verificación rigurosa de la integridad de estos datos. La recuperación de datos borrados es especialmente importante en casos donde los involucrados han intentado eliminar o alterar información relevante para el caso, y el éxito de esta recuperación depende en gran medida del uso de programas especializados que pueden acceder a sectores del disco duro que las herramientas convencionales no alcanzan.

Otra función clave en el análisis forense es el análisis de archivos, que implica examinar cada elemento de información en busca de pistas que puedan esclarecer los hechos investigados. Este análisis se realiza mediante un proceso de inspección exhaustiva de metadatos, modificaciones, creaciones, accesos y propiedades de los archivos, lo cual ayuda a identificar la cronología de eventos o la posible manipulación de la información. Además, la verificación de la integridad de los archivos se realiza con herramientas que aplican algoritmos de hash, los cuales crean una "huella digital" del archivo para asegurarse de que no ha sido alterado durante la transferencia o el análisis. Así, los analistas forenses pueden estar seguros de que la información es auténtica y confiable.

En los últimos años, una rama específica de la actividad forense ha tomado auge: el estegoanálisis Conceptualmente se trata del procedimiento de examinar datos electrónicos con el propósito de identificar, extraer y evaluar información oculta o modificaciones no autorizadas en archivos digitales. Esta disciplina involucra el estudio de técnicas y métodos para identificar y desenmascarar la presencia de esteganografía, que es la técnica que permite ocultar datos dentro de otros datos sin ser detectados fácilmente. El estegoanálisis se basa en el principio de buscar patrones, anomalías o alteraciones en los archivos digitales que puedan indicar la presencia de información oculta, que le otorga su carácter de instrumento crucial en la investigación pericial digital.[85]

Tras la recuperación y análisis de los datos, es indispensable documentar los resultados en un informe técnico exhaustivo. Este informe, de carácter formal, debe contener una exposición detallada de los métodos y herramientas empleadas en cada fase del análisis, junto con un resumen de los hallazgos obtenidos y las conclusiones derivadas del estudio. La importancia de este informe radica en que no solo debe ser útil para expertos en el área, sino también comprensible para audiencias con conocimientos técnicos limitados, como abogados, jueces o miembros de un jurado.

---

[85] Mukesh Dalal y Mamta Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide", *Multimedia tools and aplications* 80, nº. 4, (2021), 5723-5771. doi:https://doi.org/10.1007/s11042-020-09929-9

La capacidad del analista forense de traducir términos técnicos a un lenguaje accesible y de organizar la información en un formato lógico y coherente es fundamental para que los hallazgos del análisis forense puedan ser usados efectivamente en el proceso judicial. Para lograrlo, el informe técnico debe estructurarse de tal manera que permita a cualquier lector entender el procedimiento, la relevancia de los datos recuperados y cómo estos sustentan las conclusiones.[86]

Aparte de los aspectos técnicos y metodológicos, el análisis forense requiere de una colaboración estrecha entre distintas entidades para maximizar su efectividad. La naturaleza de una investigación forense, especialmente en delitos informáticos y de alta complejidad, implica que ninguna organización puede abarcar todas las áreas de conocimiento y experiencia por sí sola. En estos casos, es esencial una colaboración interinstitucional que reúna a expertos de diversas áreas, tales como la policía, la fiscalía, expertos en seguridad informática, técnicos forenses y, en algunos casos, representantes de agencias gubernamentales o entidades privadas.

Tal coordinación no solo permite un enfoque integral en la investigación, sino que también optimiza los recursos y reduce el tiempo necesario para alcanzar resultados. Por ejemplo, en una investigación de fraude cibernético que involucre múltiples países, la cooperación entre agencias internacionales permite la obtención de evidencia más rápida y evita que los delincuentes aprovechen las lagunas legales que existen entre jurisdicciones.

Además, los avances en tecnología y el incremento en la sofisticación de los delitos informáticos exigen una actualización constante en los conocimientos y habilidades de los investigadores. La capacitación continua es una necesidad en el campo de la informática forense, ya que nuevas técnicas y herramientas aparecen constantemente en respuesta a la evolución de los métodos de ataque y de los sistemas de seguridad. Los investigadores deben estar familiarizados con tendencias emergentes, tales como el análisis de *blockchain*, la ingeniería inversa de malware y las técnicas avanzadas de análisis en redes. La formación regular en estas áreas permite a los analistas mantenerse al día y aplicar los métodos más efectivos en sus investigaciones, lo cual contribuye a un proceso de análisis forense de alta calidad y adaptable a los desafíos actuales de la criminalidad digital.[87]

---

[86] Edith Pino Icaza, "Informática Forense como medio de prueba en el Ecuador", *Revista Universidad de Guayaquil* 108, Nº. 3, (2020),56-63: https://dialnet.unirioja.es/servlet/articulo?codigo=8368273&orden=0&info=link

[87] Ibid.

El estudio de las investigaciones jurídicas contemporáneas ha permitido sistematizar los aspectos jurídicos y tecnológicos de la gestión de la evidencia digital.

Teniendo en cuenta la experiencia internacional, el desarrollo de un protocolo nacional para el uso de evidencia digital en Ecuador debe considerar varios aspectos fundamentales:

a) la armonización entre los estándares internacionales ISO/IEC y el marco normativo nacional existente, garantizando la compatibilidad técnica y jurídica.

b) la implementación de sistemas de certificación y capacitación para peritos especializados, asegurando competencias técnicas adecuadas para el manejo de evidencia digital.

c) establecer procedimientos específicos para la cadena de custodia digital, adaptando los principios tradicionales a las características particulares de la evidencia electrónica.

d) definir procedimientos de verificación y validación que garanticen la integridad y autenticidad de la evidencia digital en todas las fases procesales.

e) prever mecanismos de actualización periódica, considerando la evolución constante de las tecnologías digitales y la necesidad de mantener la vigencia tecnológica y jurídica de los procedimientos establecidos.

2.4. Comparación entre los procedimientos ecuatorianos y los estándares internacionales

El Código Orgánico General de Procesos establece directrices concretas para la admisión y valoración de la evidencia digital, considerando su creciente protagonismo en los procesos judiciales, tanto civiles como penales. Su regulación responde a la necesidad de garantizar la pertinencia, legalidad y autenticidad de este tipo de prueba, al tiempo que se asegura el respeto al debido proceso, el derecho a la defensa y el acceso efectivo a la justicia, conforme a los principios constitucionales.

El COGEP fija parámetros claros para la admisibilidad de la prueba digital, exigiendo que sea relevante y útil en relación con los hechos debatidos. Esto obliga al juez a verificar que la información presentada esté directamente vinculada con el objeto del litigio, evitando la incorporación de datos ajenos al caso o que comprometan la privacidad de las partes. Además, es imprescindible que la evidencia digital haya sido obtenida legalmente, en respeto a las normas sobre privacidad y protección de datos personales. El uso de pruebas digitales obtenidas de manera ilícita —como el acceso indebido a correos electrónicos o cuentas en redes sociales— conlleva su inadmisibilidad en el proceso, y

puede derivar en responsabilidades legales para quien incurra en tales prácticas, al representar una vulneración de derechos fundamentales.

En la jurisprudencia ecuatoriana, la prueba digital y el derecho a la defensa guardan una estrecha relación, pues se trata garantía constitucional que permite a las partes involucradas acceder a los medios precisos para la protección de sus intereses. Es decir, las partes tienen el derecho de presentar y refutar pruebas digitales, siempre que se asegure su autenticidad e integridad. Tales aspectos resultan esenciales, dado que, por su propia naturaleza, la evidencia digital es susceptible de ser manipulada, lo que podría deformar la realidad de los hechos y comprometer la imparcialidad del proceso judicial. Por tal motivo, la normativa establece que las pruebas digitales han de ser sometidas a procedimientos de verificación rigurosos que aseguren su inalterabilidad desde el momento de su generación hasta su incorporación en el juicio.[88]

El COGEP también estipula que la prueba digital debe cumplir con los principios de comprensibilidad y verificabilidad, requisitos que buscan facilitar su evaluación por parte de jueces y abogados, quienes en muchos casos carecen de conocimientos técnicos en materia tecnológica. La exigencia de comprensibilidad implica que los materiales probatorios en formato digital deben permitir su correcta interpretación. Por otro lado, la verificabilidad es básica para garantizar que la prueba pueda ser sometida a un examen técnico que corrobore su procedencia, autoría y su contenido. Este criterio se orienta a asegurar que cada prueba digital cuente con una trazabilidad permita través de la cual se pueda reconstruir su proceso de creación, almacenamiento y transferencia, garantizando así su autenticidad.[89]

Otro aspecto fundamental en la valoración de la prueba digital radica en la verificación de los medios utilizados para su generación o extracción. El sistema judicial, en muchos casos, exige la presentación del dispositivo original o del sistema que originó la evidencia digital, con el fin de confirmar su autenticidad. Así, por ejemplo, cuando se trata de mensajes de texto o correos electrónicos, no es suficiente aportar únicamente capturas de pantalla; resulta indispensable examinar directamente el dispositivo emisor para constatar que la prueba procede de fuente confiable y que no ha sido manipulada. Tal exigencia obedece a la facilidad con la que los documentos digitales pueden ser alterados,

[88] Ecuador. Código Orgánico General de Procesos (COGEP).
[89] Carlos Ramírez, *Apuntes sobre la prueba en el COGEP*

lo cual, si bien permite su ágil gestión, también representa un riesgo significativo para la integridad y la fiabilidad de la prueba en el contexto judicial.

Pese a estos avances normativos, Ecuador se encuentra ante diversos retos en la aplicación efectiva del COGEP en lo que concierne a la prueba digital. Uno de ellos radica en la insuficiente capacitación de jueces y abogados, quienes requieren conocimientos especializados para evaluar correctamente la autenticidad, trazabilidad y pertinencia de la prueba digital. La vertiginosa evolución tecnológica y la variedad de dispositivos y plataformas que generan este tipo de evidencia demandan una actualización constante de conocimientos y la adopción de nuevas metodologías de análisis, lo cual resulta complejo sin programas de formación continua en esta materia.

Otra limitación relevante en el sistema judicial de Ecuador es la ausencia de metodologías sobre el manejo de la prueba digital. La falta de estándares uniformes en cuanto a la admisibilidad y autenticación de estas evidencias puede generar discrepancias en la interpretación y aplicación de la normativa por parte de diferentes jueces. La elaboración de metodologías, que regulen desde la recolección hasta la incorporación de la prueba digital en el proceso judicial, contribuiría a garantizar su valoración objetiva y equitativa, minimizando el riesgo de manipulaciones y fortaleciendo la transparencia en la administración de justicia.[90]

En el ámbito internacional, diversos instrumentos y normativas buscan estandarizar el tratamiento de la prueba digital, destacándose el Convenio de Budapest, donde se establecen lineamientos para la obtención y preservación de evidencia digital, además de instar a la cooperación bilateral o multilateral en la lucha contra los delitos informáticos. El hecho de que el convenio no haya sido ratificado por parte de Ecuador limita la aplicación de estos estándares internacionales y constituye un obstáculo para abordar eficazmente delitos de naturaleza transnacional, que requieren colaboración internacional y normativas homogéneas. Mientras otras naciones de la región se han adherido al Convenio de Budapest, el país tiene ante sí el roto de fortalecer su marco normativo para alcanzar niveles similares a los de otras naciones.

Tabla 1 Comparación de protocolos sobre el manejo de la prueba digital

[90] Iván Alejandro, Riofrio García, Wagner Guido Morales Román, Johanna Irene Escobar Jara, y Fátima Eugenia Campos Cárdenas, "La prueba electrónica en los procesos penales en Ecuador en concordancia con celeridad y economía procesal." *Serie Científica de la Universidad de las Ciencias Informáticas* 18, Nº. 2 (2025) 49-71, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2306-24952025000200049&lng=es&tlng=es.

Protocolos (origen o jurisdic.)	Principios básicos	Requisitos técnicos	Control de calidad	Ventajas	Limitaciones
SWGDE, Estados Unidos/ NIST	Integridad, competencia, documentación exhaustiva	Laboratorios especializados, protección ESD, identificadores únicos	Revisión técnica/por pares, revisión administrativa	Marco consolidado desde 1998, sólido respaldo institucional	Enfocado solo a los EEUU
ACPO, Reino Unido	Preservación absoluta de datos originales, competencia del personal	Copias forenses bit-a-bit, herramientas especializadas	Competencia certificada del personal	Principios claros y aplicables, amplia adopción internacional	Menos detallado en aspectos técnicos específicos
ENFSI Europa	Calidad, estandarización, competencia	Exámenes priorizados, recuperación sistemática	Aseguramiento de calidad integral	Enfoque europeo armonizado, cobertura comprehensiva	Complejidad de su aplicación
INTERPOL, mundial	Mejores prácticas para primeros respondientes	Preservación en escena, transporte seguro	Directrices específicas para personal no especializado	Aplicabilidad global, enfoque práctico	Limitado a primeros respondientes
Ecuador (COGEP /COIP)	Validez digital sin materialización, testimonio pericial	Almacenamiento en medios ópticos, reproducción en formato original	Testimonio del perito y cadena de custodia	Adaptación a realidad nacional, flexibilidad	Menor detalle técnico, dependencia del criterio pericial

Elaboración propia

Desde una perspectiva de principios generales, los estándares internacionales establecen que la prueba digital debe cumplir con los criterios de: a) cadena de custodia, b) autenticidad y c) integridad. Estos requisitos coinciden en línea general con las disposiciones del COGEP, aunque su implementación puede diferir según la jurisdicción. La cadena de custodiagarantiza la inalterabilidad de la evidencia digital desde su recolección hasta su presentación en juicio, por lo que constituye un pilar esencial para asegurar su fiabilidad. Asimismo, la autenticidad y la integridad son exigencias sine qua non para confirmar que la prueba corresponde efectivamente a los hechos que se pretenden

demostrar, evitando posibles manipulaciones o alteraciones que puedan comprometer su validez.[91]

Al compararse con otras naciones del áreaque han adoptado el Convenio de Budapest y han desarrollado marcos normativos más avanzados en materia de prueba digital, Ecuador mantiene un rezago normativo que puede afectar la calidad del sistema de justicia en casos que conllevan el examen de evidencia digital. Esta situación pone de manifiesto la necesidad de modernizar la legislación nacional en este ámbito y de adoptar estándares internacionales que fortalezcan la seguridad y confiabilidad de las pruebas digitales. De este modo, el sistema judicial ecuatoriano podrá adecuarse a las nuevas realidades de la era digital.

2.5. Casos emblemáticos y su manejo de prueba digital en Ecuador y en el ámbito internacional

La selección de casos emblemáticos para analizar el manejo de pruebas digitales en Ecuador y en el ámbito internacional requiere un enfoque metodológico riguroso que permita destacar ejemplos representativos y fundamentados. Para ello, se priorizan criterios como la relevancia jurídica de los casos, su impacto en la jurisprudencia y la documentación accesible que permita un análisis detallado. Además, es fundamental que los casos seleccionados aborden contextos diversos y reflejen la evolución del tratamiento de las pruebas digitales en diferentes sistemas jurídicos.

Estos casos han sido seleccionados no solo por su impacto en sus respectivos contextos legales, sino también porque permiten analizar distintos aspectos del manejo de pruebas digitales, desde la cadena de custodia hasta la interoperabilidad internacional. Además, su inclusión proporciona una perspectiva comparativa que facilita la comprensión de los retos y avances en la incorporación de pruebas digitales en los sistemas judiciales, destacándose tanto las particularidades del contexto ecuatoriano como las tendencias globales. La elección de estos casos busca establecer una base sólida para explorar la evolución y los desafíos de la prueba digital en el ámbito jurídico contemporáneo.

Casos internacionales

- Investigaciones sobre difusión de imágenes indecentes de niños en Reino Unido (2023)

[91] Carlos Ramírez, *Apuntes sobre la prueba en el COGEP*.

En Reino Unido, al igual que en otras naciones, las fuerzas policiales han enfrentado un aumento exponencial en casos relacionados con imágenes indecentes de niños (IIOC, por sus siglas en inglés). A partir de un grupo de operativos policiales en los que se incautaron dispositivos electrónicos, se acudió al empleo de la inteligencia artificial para el análisis masivo de información. Ante la imposibilidad de procesar esos datos con los métodos tradicionales, los investigadores acudieron a la IA para obtener patrones criminales.

Las experiencias obtenidas de estos procesos han demostrado que la integración de inteligencia artificial en las investigaciones forenses digitales presenta beneficios transformadores, pero también plantean importantes exigencias. Entre los beneficios se encuentran el análisis eficiente y rápido de datos, el reconocimiento de patrones y la toma de decisiones automatizada. Entre tanto, los restos de estos procedimientos se refieren a la elevada capacitación de los forenses, la necesidad de determinar estándares de interpretación de este tipo de pruebas y el desarrollo de procedimientos tecnológicos complementarios para verificar la autenticidad de la información que aporta la IA. [92].

- Revisión global de evidencia digital de Interpol

Los trabajos de investigación realizados por Interpol en el período 2019-2022, se sistematizan en documentos que describen los principales avances en el uso de la evidencia digital. Según el estudio, mediante la evidencia digital se pueden reconstruir las actividades de una persona, incluyendo su movilidad a través del tiempo e interacciones, empleando datos biométricos combinados con análisis contextuales.

La importancia de este reporte reside en demostrar el peso específico de la evidencia digital en una pesquisa policial y en el ulterior procedo penal. Los dispositivos tecnológicos actuales generan trazas digitales únicas, con alto valor identificativo, que permiten establecer vínculos entre personas, lugares y eventos de interés policial de un modo más exacto que los métodos tradicionales de investigación criminal.[93]

- Casos de Divulgación de Evidencia Digital en Procesos Penales

En el año 2021, los tribunales del Reino Unido crearon un precedente denominado "*digital strip-searches*" (registros digitales exhaustivos). Para ello ha sido necesaria la adaptación de la Ley de Procedimiento Penal e Investigaciones de 1996 a los desafíos

[92] Simon Parkinson y Saad Khan, "The role of Artificial Intelligence in digital forensics: Case studies and future directions", *Assesment and development matters* 16, N. 1, 2024, 42-47, https://pure.hud.ac.uk/ws/portalfiles/portal/81261791/accepted_version.pdf

[93] Paul Reedy, "Interpol review of digital evidence for 2019–2022", *Forensic Science International Sinergic*, 6:100313 (2023): doi: 10.1016/j.fsisyn.2022.100313

digitales del siglo XXI, lo cual ha sido particularmente notorio en el manejo de evidencia obtenida de teléfonos móviles y registros electrónicos.

Si bien ya era conocida la pertinencia de tales datos, la aplicación de registros digitales exhaustivos ha puesto de manifiesto la capacidad de formar convicciones en los órganos juzgadores debido a la exactitud de la información presentada por los peritos. Sin embargo, este tipo de procedimientos ha llevado a la Corte Británica a definir mediante actos jurisprudenciales los límites de tales procedimientos, así como las formas de revelarlos, en un intento por balancear la protección social contra los delitos y los derechos de las personas sobre su información personal.[94]

Casos emblemáticos en Ecuador

- Caso "Sobornos 2012-2016"

En Ecuador, el uso de pruebas digitales ha emergido como un elemento crucial en la resolución de casos de corrupción de gran envergadura, al aportar transparencia y solidez a las investigaciones. Uno de los casos más destacados fue el denominado "Sobornos 2012-2016", que involucró a una red de sobornos dentro del gobierno ecuatoriano. Este caso no solo destacó por la magnitud del escándalo, sino también por el uso eficaz de la tecnología en el proceso judicial. Los fiscales presentaron pruebas digitales clave, como correos electrónicos y registros de transferencias bancarias, que permitieron trazar la ruta de los pagos ilícitos y el entramado de complicidades entre funcionarios de alto nivel.[95]

Este caso no solo evidenció la magnitud de la corrupción en la administración pública, sino que también planteó interrogantes sobre el manejo de pruebas digitales en la justicia penal y las garantías procesales necesarias para asegurar la transparencia y la imparcialidad del sistema judicial. Su análisis detallado permite comprender la intersección entre la tecnología y el derecho penal, así como la evolución de las normativas y procedimientos frente a los desafíos del siglo XXI.

La investigación se originó con denuncias presentadas por la Fiscalía General del Estado, que señaló la existencia de un esquema de sobornos sistemáticos durante el gobierno del expresidente Rafael Correa. Este esquema habría consistido en la recepción

---

[94] Alexandra Topping, "Police and CPS scrap digital data extraction forms for rape cases Exclusive: case of two complainants funded by Equality and Human Rights Commission forces U-turn" *The Guardian*, 16 de julio, 2020, https://www.theguardian.com/society/2020/jul/16/police-and-cps-scrap-digital-data-extraction-forms-for-cases

[95] Ecuador. Procuraduría General de la República, "Caso Sobornos 2012-2016: Doce funcionarios públicos constan en la acusación particular", Boletín de Prensa, Quito, 20 de noviembre de 2019, http://www.pge.gob.ec/index.php/prensa/boletines-de-prensa/noviembre-2019/caso-sobornos-2012-2016-doce-funcionarios-publicos-constan-en-la-acusacion-particular

de aportes económicos ilegales por parte de contratistas y empresarios privados a cambio de la adjudicación irregular de contratos estatales, configurándose un modelo de corrupción estructurada que, según la Fiscalía, involucraba a altos funcionarios gubernamentales y otras personas relacionadas. La acusación formal se concretó el 3 de enero de 2020, cuando la jueza Daniela Camacho Herold decidió llamar a juicio a 21 personas, entre las que destacaban figuras prominentes como el expresidente Correa y el exvicepresidente Jorge Glas. Este paso procesal marcó el inicio de un juicio que tendría amplias repercusiones políticas, sociales y jurídicas en el país.

El delito imputado a los acusados fue el de cohecho, tipificado en el artículo 286 del Código Penal que se encontraba vigente en ese momento. Este delito, considerado uno de los actos más graves contra la administración pública, implica la recepción de dádivas o beneficios indebidos por parte de funcionarios a cambio de favorecer a terceros en el ejercicio de sus funciones. Según la Fiscalía, 20 de los procesados participaron como autores directos de estos actos, mientras que uno de ellos actuó como cómplice al facilitar las operaciones ilícitas. La estructura delictiva denunciada por la Fiscalía incluía tanto la obtención de fondos a través de sobornos como la posterior distribución de estos recursos para financiar campañas políticas del movimiento oficialista, lo que implicaba una red compleja de acciones y actores.

El tribunal que asumió la tarea de juzgar este caso estuvo compuesto por los jueces Iván León Rodríguez, Marco Rodríguez Ruiz e Iván Saquicela Rodas. La audiencia de juzgamiento, que tuvo lugar entre el 10 de febrero y el 6 de marzo de 2020, se desarrolló bajo un escrutinio público significativo debido al impacto mediático y político del caso. En este escenario, la Fiscalía General del Estado y la Procuraduría General del Estado actuaron como acusadores, al presentar un extenso conjunto de pruebas que buscaban demostrar la existencia del esquema de corrupción y la responsabilidad de los acusados. Tras concluir las deliberaciones, el tribunal emitió su decisión el 7 de abril de 2020, al dictarse una sentencia unánime cuya publicación completa no ha sido accesible en las fuentes revisadas. Sin embargo, se sabe que esta decisión generó controversias y fue objeto de análisis por expertos en derecho y organizaciones sociales.[96]

La validez de estas pruebas fue asegurada mediante peritajes informáticos, realizados por expertos que confirmaron su autenticidad y permitieron que fueran aceptadas

[96] Ecuador. Corte Nacional de Justicia "Tribunal Penal de la CNJ dictó sentencia en el caso Sobornos 2012 – 2016", https://www.cortenacional.gob.ec/cnj/index.php/noticias-2020/128-abril-2020/264-tribunal-pernal-de-la-cnj-dicto-sentencia-en-el-caso-sobornos-2012-2016

sin objeciones en el juicio. Esta autenticidad se convirtió en un pilar fundamental para la condena de los implicados, entre ellos el expresidente Rafael Correa, quien fue señalado como una de las figuras clave dentro de este esquema de corrupción. Así, el empleo de pruebas digitales no solo resultó en el esclarecimiento de los hechos, sino que también consolidó un precedente importante para el sistema judicial del país, demostrándose que la tecnología puede jugar un papel decisivo en la lucha contra la corrupción a niveles gubernamentales.

Concretamente, las pruebas digitales jugaron un papel decisivo para establecer la existencia del esquema de corrupción, incluyéndose correos electrónicos, registros de transferencias bancarias y documentos digitales que trazaban el flujo de sobornos entre contratistas y funcionarios públicos. La Fiscalía General del Estado presentó estas evidencias electrónicas respaldadas mediante peritajes informáticos especializados, los cuales analizaron metadatos para garantizar que no hubieran sido alterados, al validar su origen y autoría. La cadena de custodia fue certificada en cada etapa del proceso, al asegurar su admisibilidad, y los correos electrónicos revelaron comunicaciones clave entre los acusados que detallaban el mecanismo de asignación de contratos a cambio de pagos ilícitos.

En la sentencia, el tribunal destacó la relevancia de estas pruebas como evidencias objetivas que permitieron reconstruir el esquema delictivo, lo que valida su autenticidad y trazabilidad mediante análisis técnicos que les otorgaron un alto grado de credibilidad. Los magistrados subrayaron que los correos electrónicos no solo corroboraron otras pruebas, sino que también ofrecieron una narrativa detallada y respaldaron testimonios clave, al actuar como elementos centrales para las condenas. Este caso marcó un precedente en la justicia ecuatoriana al demostrar la eficacia del manejo de pruebas digitales en delitos complejos de corrupción, y evidenció la necesidad de fortalecer normativas y capacidades técnicas para garantizar su uso adecuado en procesos futuros.

- Caso Petroecuador

Un caso igualmente relevante en la historia judicial de Ecuador es el caso Petroecuador, que involucró a la principal empresa estatal de petróleo del país en una serie de actos de corrupción que incluyeron sobornos y malversación de fondos. La investigación se centró en desentrañar una red de funcionarios y empresarios que se beneficiaban de

contratos millonarios a través de prácticas corruptas. En este caso, las pruebas digitales también jugaron un papel fundamental.[97]

Los fiscales utilizaron una variedad de pruebas electrónicas, tales como correos electrónicos, mensajes de texto y registros de llamadas, para rastrear la comunicación entre los involucrados y desentrañar el modus operandi de los delitos. Con el respaldo de peritajes técnicos que garantizaron la integridad de estas pruebas, los fiscales lograron validar su autenticidad y utilizarlas eficazmente en el juicio. Gracias a este enfoque, se identificaron a los responsables y se dictaron condenas, mientras que también se logró la recuperación de fondos malversados, lo que contribuyó a mitigar los efectos de la corrupción en el sector público. Este caso ejemplifica cómo la correcta aplicación de las pruebas digitales puede ser decisiva no solo para lograr justicia, sino también para fortalecer la confianza en las instituciones judiciales del país.

Un aspecto central que emerge del análisis de este caso es la posible incorporación de pruebas digitales en el proceso penal. Las evidencias incluyeron mensajes de texto, correos electrónicos, registros de llamadas y datos financieros electrónicos recopilados por expertos en informática forense, quienes aseguraron su integridad y autenticidad. Un aspecto destacado fue el uso de software especializado para analizar patrones de comunicación entre los implicados, al permitir mapear las interacciones y establecer roles dentro de la red delictiva.

En las sentencias, los jueces valoraron cómo los mensajes de texto y los registros de llamadas aportaron evidencias directas sobre la coordinación entre los acusados, mientras que los registros financieros respaldaron las acusaciones de malversación de fondos. Además, se señaló que las pruebas digitales cumplieron con los estándares de admisibilidad y que su autenticidad no fue cuestionada, al fortalecer así la posición de la Fiscalía y al ser determinantes para las condenas. Este caso demostró que, aunque las pruebas digitales son herramientas poderosas, su manejo exige altos niveles de especialización técnica, subrayándose la necesidad de formar adecuadamente a peritos y actualizar a los jueces en materia tecnológica como factores clave para garantizar el éxito en este tipo de procesos.[98]

---

[97] El Universo, “Caso Petroecuador: audiencia preparatoria de juicio contra Nilsen Arias y otros 16 acusados por el delito de cohecho sin fecha para reanudarse”, 14 de octubre, 2024. https://www.eluniverso.com/noticias/politica/nilsen-arias-caso-petroecuador-cohecho-audiencia-evaluacion-y-preparatoria-de-juicio-caso-alianza-exgerente-de-comercio-internacional-en-petroecuador-rafael-correa-antonio-pere-icaza-enrique-pere-icaza-raymond-kohut-transnacional-gunvor-corrupcion-suspension-audiencia-fiscalia-ivonne-nunez-juez-giovanni-freire-nota/

[98] Ibid.

La relevancia de las pruebas digitales en casos complejos como este no solo radica en su capacidad para aportar evidencia directa, sino también en los retos asociados a su manejo. Garantizar la admisibilidad de estas pruebas en un proceso penal exige un cumplimiento riguroso de principios como la integridad de los datos, la autenticidad de las evidencias y el mantenimiento de una cadena de custodia confiable. Además, el análisis técnico de los datos debe realizarse bajo estándares especializados para evitar cualquier cuestionamiento sobre su validez. En este contexto, la falta de claridad sobre la utilización de pruebas digitales en el caso "Sobornos 2012-2016" plantea preguntas importantes sobre la capacidad del sistema judicial ecuatoriano para adaptarse a los desafíos tecnológicos contemporáneos.

- Operativo Guardián 5 en el SERCOP

El allanamiento a las oficinas del Servicio Nacional de Contratación Pública (SERCOP) en febrero de 2025, se llevó a cabo luego de un ataque informático que afectó 920 procesos de contratación pública. La evidencia digital ocupada permitió reconstruir el vector de ataque, definiendo que los ciberdelincuentes habían obtenido credenciales de usuario mediante ingeniería social, luego modificaron las contraseñas y eliminaron archivos. La pericia forense permitió identificar patrones de comportamiento digital, incluyendo horarios de acceso y direcciones IP vinculadas a los sospechosos. Aquí se demostró la efectividad de la colaboración interinstitucional, dada la colaboración de la policía con peritos informáticos de la FGN.

El saldo del proceso fue la implementación de protocolos de seguridad reforzados en entidades del sector público y la creación de un sistema de monitoreo proactivo para detectar anomalías en tiempo real. Este y otros operativos han venido a replantear la necesidad de adecuar el marco regulatorio para adaptarlo a las nuevas formas del delito cibernético y llenar los vacíos que usualmente se encuentran en la investigación de estos hechos. [99]

Los casos vistos hasta aquí demuestran que la evidencia digital se ha convertido en un elemento indispensable para la investigación y procesamiento de delitos complejos tanto a nivel internacional como nacional. Las experiencias obtenidas, resaltan la necesidad de formación especializada continua, desarrollo de procedimientos consensuados y la implementación de tecnologías avanzadas como la IA artificial para el procesamiento eficiente de grandes volúmenes de evidencia digital. La evolución continua de las

[99] Iván Alejandro Riofrio, Wagner Guido Morales Román, Johanna Irene Escobar Jara y Fátima Eugenia Campos Cárdenas, "La prueba electrónica en los procesos penales en Ecuador"

tecnologías y el surgimiento de nuevos tipos de delitos informáticos requieren una adaptación constante de los procedimientos forenses y las normas legales.

Capítulo tercero
Deficiencias y desafíos en la aplicación de la prueba digital

3.1. Análisis de las deficiencias identificadas en el manejo de la prueba digital en Ecuador

Ecuador enfrenta una significativa carencia de un marco normativo específico que regule adecuadamente la prueba digital. Aunque existen cuerpos legales como el COIP y el COGEP, estos se enfocan mayoritariamente en las pruebas físicas tradicionales, lo que relega las evidencias digitales a un segundo plano. Esta ausencia de regulación detallada limita la capacidad del sistema judicial para adaptarse a los retos que plantea la creciente digitalización de la sociedad.

En este contexto, el país ha manifestado su intención de adherirse al Convenio de Budapest,[100] el cual establece estándares internacionales para la recolección, manejo y presentación de pruebas digitales. Sin embargo, aunque este paso representa un avance hacia la modernización, aún no se han implementado las regulaciones necesarias para garantizar una aplicación efectiva de los principios establecidos en dicho convenio. Esto genera un vacío normativo que pone en riesgo la adecuada gestión de las pruebas digitales en el ámbito judicial.

A nivel técnico y procedimental, uno de los mayores desafíos radica en la autenticidad e integridad de las pruebas digitales. Sin protocolos claros que regulen su recolección y manejo, los datos digitales corren un alto riesgo de ser manipulados, lo que compromete su validez y confiabilidad como evidencia en los tribunales. Además, la valoración judicial de estas pruebas enfrenta serias dificultades debido a la falta de conocimientos especializados entre jueces y fiscales. La carencia de capacitación sobre cómo manejar y evaluar evidencia digital puede derivar en decisiones judiciales equivocadas o en la exclusión injustificada de pruebas relevantes.[101]

En cuanto a la capacitación del personal judicial, se observa una notable deficiencia en la formación en nuevas tecnologías. Jueces, fiscales y abogados carecen de las herramientas y conocimientos necesarios para abordar eficazmente los retos que conlleva

[100] Consejo de Europa, *Convenio de Budapest sobre la Ciberdelincuencia*, Serie de Tratados No. 185 (2001), https://rm.coe.int/1680081561

[101] Henry Saca, Anthony Márquez y César Arciniegas, "La inviabilidad de la prueba digital por falta de regulación en los delitos informáticos", *593 Digital Publishet CEIT* 8, n.º 4 (2023): 21-34:doi.10.33386/593dp.2023.4.1887

el manejo de pruebas digitales. Este déficit formativo obstaculiza la capacidad del sistema judicial para adaptarse a las demandas del entorno digital y afecta la eficiencia y equidad en la administración de justicia.[102]

Por otro lado, las implicaciones sociales y tecnológicas también representan un obstáculo importante. La brecha digital en Ecuador limita el acceso de muchas comunidades a tecnologías modernas, lo que no solo dificulta la recolección de pruebas digitales, sino que también restringe su participación plena en procesos judiciales que dependen de esta evidencia. Esta desigualdad tecnológica agrava las barreras existentes para garantizar un acceso equitativo a la justicia, especialmente en regiones rurales o de bajos recursos.[103]

3.2.Limitaciones técnicas y operativas

La adopción de pruebas digitales en el sistema judicial ecuatoriano se ve obstaculizada por una serie de barreras que complican su integración efectiva y su aceptación en términos generales. Estas dificultades comprenden tanto aspectos normativos como problemas relacionados con la infraestructura y la formación, lo cual limita la capacidad del sistema para ajustarse a las exigencias de la era digital. Uno de los desafíos más significativos radica en la falta de una legislación específica que regule el manejo y la valoración de las pruebas digitales.

Aunque el COIP contiene disposiciones que abordan de manera general la evaluación de evidencias, estas se centran principalmente en las pruebas físicas, lo que deja un vacío respecto a las digitales. Esta falta de regulación clara genera incertidumbre entre los operadores de justicia, quienes enfrentan dificultades para determinar los procedimientos adecuados y los criterios necesarios para garantizar la validez de estas pruebas dentro del marco legal.

La insuficiencia de capacitación del personal judicial agrava aún más esta problemática. Muchos jueces, abogados y otros actores del sistema no cuentan con el conocimiento técnico necesario para interpretar y analizar pruebas digitales. La formación en técnicas forenses digitales es limitada, y la escasez de expertos en informática forense

---

[102] Sandy Vega, *La prueba electrónica y su aplicación en el Código Orgánico General de Procesos* (Guayaquil: UCSG, 2016). http://repositorio.ucsg.edu.ec/bitstream/3317/7128/1/T-UCSG-PRE-JUR-DER-98.pdf

[103] Ricardo Becerra, "El reconocimiento de la brecha digital para garantizar el acceso efectivo a la administración de justicia civil", Precedente. Revista Jurídica 23 (2023): 11-35. https://doi.org/10.18046/prec.v23.5875

dentro de las instituciones judiciales dificulta el acceso a un tratamiento especializado de este tipo de evidencia. Este vacío de conocimientos y recursos humanos impactan directamente sobre la calidad y celeridad de los procesos judiciales, alargándose los plazos y comprometiéndose la precisión de las decisiones basadas en pruebas digitales.

Además de los desafíos relacionados con la capacitación, la infraestructura tecnológica del sistema judicial presenta serias deficiencias. Muchas instituciones carecen de los equipos y programas necesarios para manejar adecuadamente las pruebas digitales. El hardware y el software disponibles suelen estar desactualizados, lo que limita la capacidad de realizar análisis forenses efectivos y seguros. Esta situación refleja la falta de inversión en tecnología moderna, lo que no solo entorpece los procesos judiciales, sino que también compromete la seguridad de la información y aumenta el riesgo de manipulaciones o errores que pueden afectar la validez de las pruebas.[104]

En el contexto legal y ético, la incorporación de pruebas digitales genera interrogantes complejos, especialmente en lo que respecta a la protección de datos personales y la privacidad. A pesar de que la legislación ecuatoriana reconoce el derecho a la protección de datos, su implementación efectiva en la práctica presenta desafíos considerables. La falta de una cultura sólida sobre privacidad, combinada con limitaciones en las capacidades institucionales, puede resultar en situaciones donde las pruebas digitales sean obtenidas o utilizadas de manera que vulneren derechos fundamentales.[105] Estas tensiones subrayan la necesidad de desarrollar políticas y prácticas que equilibren la utilidad de las pruebas digitales con el respeto a los derechos humanos y las garantías procesales.

Otro ámbito afectado por la falta de regulación en el manejo de pruebas digitales es el comercio electrónico, donde los problemas relacionados con la evasión fiscal y el control tributario se han intensificado. La normativa actual no se adapta completamente a las particularidades de las transacciones digitales, lo que dificulta la identificación y sanción de prácticas fraudulentas. Este vacío legal no solo representa un desafío para la justicia fiscal, sino que también puede impactar la percepción de equidad y eficacia del sistema judicial en su conjunto.

---

[104] Imaicela Jackson y Lissette Alvarado, "La incorporación de la prueba digital en el derecho procesal ecuatoriano", *Revista LEX* 7, n.º 27 (2024): 1338-50. https://doi.org/10.33996/revistalex.v7i27.247

[105] Henry Saca, Anthony Márquez, y César Arciniegas, "La Inviabilidad de la Prueba Digital"

3.3.Vacíos legales y falta de actualización normativa

Tal como se señaló previamente, el COGEP establece un marco normativo destinado a regular la admisibilidad y valoración de las pruebas digitales dentro de los procesos judiciales. Sin embargo, pese a su importancia como herramienta procesal, presenta serias limitaciones que afectan su aplicación práctica. Aunque reconoce la relevancia de los documentos electrónicos y otros medios digitales como pruebas, el COGEP no proporciona una regulación lo suficientemente detallada que aborde todos los aspectos técnicos y jurídicos necesarios para garantizar su correcta utilización en el ámbito judicial.[106] Uno de los problemas más significativos radica en la ausencia de directrices específicas que permitan determinar con claridad la autenticidad y la integridad de estas pruebas. Entre los mecanismos más relevantes se encuentran las funciones criptográficas hash (SHA-256 o MD5)*;* los sellos de tiempo (*timestamp*) que utilizan infraestructuras de clave pública (*public key infrastruture* o PKI) lo cual debe certificarse por una autoridad de sellado de tiempo (*timestemp authority*); las firmas digitales avanzadas que aseguren que ninguna modificación posterior a ella pase inadvertida.[107]

Sin lineamientos precisos sobre cómo verificar que una evidencia digital no ha sido manipulada o alterada, su validez puede verse comprometida, lo que genera incertidumbre tanto para los operadores de justicia como para las partes involucradas en un litigio.

Por otro lado, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos,[108] aunque establece ciertos parámetros relacionados con los documentos electrónicos, también presenta limitaciones importantes. Esta ley no ofrece un marco robusto que garantice la utilización efectiva de las evidencias digitales como medios probatorios, particularmente en el ámbito penal, donde las exigencias de rigurosidad y certeza probatoria son mayores. A pesar de que reconoce la validez de los documentos electrónicos y regula aspectos básicos de su utilización, la falta de una normativa más específica y adaptada a las complejidades del entorno digital ha generado confusión en su aplicación.

Este vacío normativo afecta no solo a los profesionales del derecho, quienes enfrentan desafíos al momento de presentar y sustentar pruebas digitales, sino también a

---

[106] Vega, *La prueba electrónica*.

[107] Leandro Guillermo Barrios Baudor, *"*La integridad y/o autenticidad de los medios de prueba digital en el proceso laboral: una aproximación al tema a propósito de los correos electrónicos*." Revista de Trabajo y Seguridad Social.* CEF (2017): 23–52. doi:10.51302/rtss.2017.1780.

[108] Ecuador, *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*, Registro Oficial 557, Suplemento, 17 de abril de 2002

los ciudadanos que, en muchas ocasiones, no tienen claridad sobre cómo proceder con evidencias obtenidas de plataformas como redes sociales, servicios de mensajería instantánea o correos electrónicos. Sin un protocolo que estandarice el manejo y la presentación de estas pruebas, su aceptación en los tribunales queda sujeta a criterios subjetivos, lo que puede derivar en decisiones inconsistentes o injustas.

La rápida evolución tecnológica y el aumento sostenido de delitos informáticos han puesto en evidencia la necesidad de actualizar las normativas existentes para que se adecuen a las nuevas realidades. En este contexto, el COIP también enfrenta serias limitaciones. Este cuerpo normativo, diseñado principalmente para regular delitos tradicionales y pruebas físicas, no contempla de manera adecuada las particularidades inherentes a las pruebas digitales. La falta de disposiciones específicas sobre cómo recolectar, preservar y presentar estas evidencias limita la capacidad del sistema judicial para abordar casos que involucran delitos cibernéticos. La situación es especialmente preocupante dado que los delitos informáticos, como el fraude electrónico, el acceso ilícito a sistemas informáticos, la suplantación de identidad y otros similares, están en aumento, lo que exige un marco normativo que permita enfrentarlos de manera efectiva.[109]

La ausencia de una regulación específica para las pruebas digitales no solo dificulta su utilización, sino que también compromete la seguridad jurídica y la confianza en el sistema de justicia. Sin normas claras, las partes en un proceso judicial pueden enfrentar obstáculos significativos para probar sus alegaciones o defenderse de acusaciones. Además, la falta de un enfoque normativo integral limita la capacidad de los jueces para valorar adecuadamente estas pruebas, lo que puede conducir a decisiones judiciales que no reflejan plenamente los hechos del caso. Por lo tanto, es fundamental que las normativas procesales y penales sean objeto de reformas que incorporen disposiciones claras y detalladas sobre las pruebas digitales. Estas reformas deben contemplar aspectos como la autenticidad, la integridad, la recolección y la conservación de las evidencias digitales, así como modos de presentación homogenizados para su presentación en los tribunales.[110]

La actualización del marco normativo no solo incrementaría la eficiencia del sistema judicial para enfrentar los retos derivados del entorno digital, sino que también favorecería la salvaguarda de los derechos de las partes involucradas en un proceso judicial,

---

[109] Evelyn Barahona, "La prueba electrónica en el proceso penal", *Revista Ciencia Multidisciplinaria CUNORI* 6, n.º 2 (2022): 55–64. https://dialnet.unirioja.es/servlet/articulo?codigo=8873602&orden=0&info=link

[110] Celia Ben, "La prueba digital. aspectos procesales", *Revista Derecho y Proceso*, n.º 3 (2023): 29-45, doi: 10.69592/2951-844X-N3-JUNIO-2023-ART2

promoviendo así un acceso más justo a la justicia. En un contexto global cada vez más digitalizado, en el que la tecnología desempeña un papel fundamental en casi todos los ámbitos de la vida, la falta de una regulación adecuada para las pruebas digitales representa un riesgo significativo para la eficacia y la legitimidad del sistema de justicia. Por ello, resulta imperativo que se promuevan y adopten reformas legales que permitan al derecho evolucionar al ritmo de las transformaciones tecnológicas, asegurándose así una administración de justicia acorde con las necesidades de la sociedad contemporánea.

3.4.Capacitación y formación de operadores de justicia

La capacitación y formación de operadores de justicia en el manejo de la prueba digital en Ecuador se ha convertido en un elemento crucial para avanzar en la modernización del sistema judicial del país. Con la creciente relevancia de las evidencias digitales en los procesos judiciales, es indispensable que jueces, fiscales y defensores públicos cuenten con las herramientas necesarias para aplicarlas correctamente en sus funciones. Este esfuerzo no solo busca garantizar una administración de justicia eficiente y acorde con los principios legales, sino que también responde a los desafíos que plantea la evolución tecnológica en el ámbito jurídico.[111]

La digitalización ha transformado profundamente la forma en que se gestionan los procesos judiciales, estableciéndose nuevos estándares sobre cómo se recopilan, presentan y valoran las pruebas. Sin embargo, aspectos como la autenticidad, la integridad y la preservación de la cadena de custodia de los datos digitales requieren una comprensión técnica y jurídica que no siempre forma parte de la formación tradicional de los operadores de justicia. En este contexto, la capacitación se vuelve imprescindible para garantizar que las decisiones judiciales basadas en pruebas digitales sean rigurosas, confiables y justas.[112]

En respuesta a esta necesidad, se han desarrollado diversos programas diseñados para capacitar a los operadores de justicia en el manejo adecuado de las pruebas digitales. Estas iniciativas abordan tanto el marco normativo como los aspectos técnicos asociados al uso de estas evidencias. Los cursos, tanto presenciales como virtuales, han sido diseñados para adaptarse a las demandas de un sistema judicial que busca mantenerse a la vanguardia. Además de proporcionar formación teórica sobre las normas aplicables, estos programas

[111] Barahona, "La prueba electrónica en el proceso penal".

[112] Irma Ramos, José Herrera y Adanhari Fajardo, "Justicia Digital: Un estándar de derechos humanos para la administración de justicia expedita por tribunales online, de forma pronta, completa e imparcial", *Revista Jurídica Jalisciense* 3, n.º 5 (2022) 263-300: https://doi.org/10.32870/rjj.v3i5.157

incluyen actividades prácticas que permiten a los participantes enfrentar situaciones reales en las que deben analizar, presentar y defender evidencias digitales en el contexto de una audiencia judicial.

La formación en el manejo de pruebas digitales no solo se limita a los aspectos técnicos y legales, sino que también aborda las implicancias éticas y contextuales de su uso. En casos de especial sensibilidad, como aquellos relacionados con violencia de género o derechos fundamentales, se han incluido módulos que destacan la importancia de utilizar esta evidencia de manera responsable y en estricto cumplimiento de los principios de equidad y justicia.

En suma, el fortalecimiento de las capacidades de los operadores de justicia en el manejo de pruebas digitales refleja un compromiso con la modernización del sistema judicial ecuatoriano. Este proceso no solo permite alinear la administración de justicia con las demandas de la sociedad contemporánea, sino que también asegura que las decisiones judiciales se fundamenten en estándares elevados de rigor y profesionalismo. La capacitación continua en este ámbito no es únicamente una respuesta a los desafíos tecnológicos actuales, sino también una inversión estratégica en la construcción de un sistema judicial más eficiente, transparente y accesible para todos.

3.5.Impacto de las deficiencias en el proceso penal

Las deficiencias en el proceso penal, particularmente en lo que respecta a la prueba digital, pueden generar un impacto significativo tanto en la administración de justicia como en los derechos de los individuos involucrados. Estas deficiencias evidencian problemas estructurales que afectan la eficacia y la equidad del sistema judicial. En el contexto ecuatoriano, donde el avance tecnológico plantea desafíos específicos, estas falencias adquieren especial relevancia.[113]

Uno de los aspectos críticos es la ineficacia de la defensa técnica. En el proceso penal, la incapacidad de los defensores para manejar adecuadamente las pruebas digitales puede tener graves consecuencias para los acusados y para la integridad del sistema judicial. Esto vulnera el derecho fundamental a un juicio justo, ya que la falta de competencia técnica para interpretar o cuestionar pruebas digitales —como registros de cámaras de seguridad, mensajes electrónicos o datos obtenidos de dispositivos móviles— puede llevar a

[113] José Bermejo y Enrique Pozo, "La ineficacia de la defensa técnica como causa de nulidad en el proceso penal: análisis jurídico", *Visionario Digital* 8, n. 2 (2024): 150-67, doi: 10.33262/visionariodigital.v8i2.3033.

decisiones judiciales arbitrarias o injustas. Además, errores estratégicos, como la omisión de solicitar peritajes adecuados o de cuestionar la validez de las pruebas digitales, pueden derivar en la nulidad del proceso penal, lo cual genera costos adicionales y retrasos en la administración de justicia. Estas ineficiencias reflejan problemas más amplios relacionados con la formación y la capacitación especializada de los defensores técnicos, quienes frecuentemente carecen de recursos o conocimientos suficientes para abordar la complejidad de las pruebas tecnológicas.

Por otro lado, las deficiencias en el proceso penal afectan de manera desproporcionada a los grupos vulnerables. En el caso de los adolescentes en conflicto con la ley, su limitada comprensión de la tecnología y su mayor exposición al uso de dispositivos electrónicos los sitúan en una posición desfavorable, especialmente cuando las pruebas digitales se utilizan de manera selectiva o como agravantes en su situación procesal.[114] De igual manera, las mujeres víctimas de violencia sexual enfrentan obstáculos adicionales cuando las pruebas digitales son necesarias para sustentar denuncias, como mensajes de acoso o evidencia de vigilancia digital. El carácter patriarcal del sistema penal ecuatoriano puede llevar a la revictimización o a la impunidad, lo que impulsa a muchas víctimas a buscar alternativas extrajudiciales de denuncia, debilitándose aún más la confianza en el sistema judicial.[115]

Adicionalmente, dentro del marco de la cooperación internacional y la armonización de normativas, las deficiencias en el manejo de pruebas digitales también plantean serios desafíos. En casos transnacionales, la ausencia de mecanismos efectivos de extradición y la falta de colaboración entre autoridades judiciales de diferentes países dificultan la obtención y validación de pruebas digitales recolectadas fuera del territorio ecuatoriano. Asimismo, la falta de armonización normativa entre Ecuador y otras jurisdicciones puede complicar la admisión de dichas pruebas en procesos penales, afectándose la persecución de delitos complejos como el lavado de activos, la trata de personas o los cibercrímenes.[116]

---

[114] Violeta González, "Adolescencia "desesperada" y criminalidad juvenil de "subsistencia". Factores situacionales de vulnerabilidad social en la selectividad penal", *Anuario de justicia de menores (18)* (2018): 241-88, https://dialnet.unirioja.es/servlet/articulo?codigo=7144472.

[115] María Castellanos, "Motivaciones y consecuencias de usar el escrache feminista como mecanismo de denuncia pública por parte de víctimas de violencia sexual en Colombia, un análisis crítico del sistema penal patriarcal", *Nuevo Foro Penal* 18, n.° 98 (2022: 115-67), doi:10.17230/nfp18.98.4.

[116] Miguel Calle y Noel Batista, "La cooperación internacional en el proceso penal, extradición, asistencia judicial y armonización de normativas", *Revista Científica de Educación Superior y Gobernanza Interuniversitaria Aula* 24 6, n.° 9 (2024): 55-69, doi:10.56124/aula24.v6i9.005.

3.6.Casos de inadmisibilidad o nulidad de prueba digital

La inadmisibilidad o nulidad de la prueba digital se refiere a aquellas situaciones en las que las evidencias electrónicas presentadas en un proceso judicial no son aceptadas debido a diversas razones legales o procesales. Este tema adquiere especial relevancia en la actualidad, dado el incremento del uso de tecnologías en actividades personales y laborales. Las razones principales que conducen a la nulidad de pruebas digitales están relacionadas con la protección de derechos fundamentales, el cumplimiento de normativas procesales y la autenticidad de las pruebas, entre otros factores.[117]

Ciertamente, la vulneración de derechos fundamentales constituye una de las principales causas de nulidad de pruebas digitales. Cuando la obtención de una evidencia electrónica infringe derechos como la privacidad o la protección de datos personales, esta puede ser declarada inadmisible. Por ejemplo, si un empleador monitoriza las actividades de un trabajador a través de herramientas tecnológicas sin su consentimiento, cualquier prueba obtenida de esta manera podría considerarse nula. Este principio busca garantizar que las pruebas no sean obtenidas mediante métodos que atenten contra los derechos básicos de las personas involucradas.[118]

Otro aspecto esencial es la falta de autenticidad. Las pruebas digitales deben cumplir con criterios estrictos de autenticación para asegurar su validez en un proceso judicial. Si no se puede demostrar de manera confiable que un documento digital es genuino y no ha sido alterado, el tribunal puede rechazarlo. Este requisito es especialmente importante en el contexto de las tecnologías, donde las evidencias pueden ser susceptibles a modificaciones o manipulaciones que comprometan su integridad.[119]

Además, el incumplimiento de normativas procesales también puede llevar a la nulidad de pruebas digitales. La presentación de estas evidencias requiere seguir procedimientos legales específicos, como garantizar una cadena de custodia adecuada y cumplir con los formatos exigidos por la legislación. La omisión de cualquiera de estos pasos puede invalidar las pruebas, independientemente de su relevancia para el caso.

---

[117] Laura Nievas, "La prueba ilícita en la era digital. Aspectos procesales de un problema tradicional con contenido nuevo en el marco del proceso laboral de Córdoba", *Revista de Estudio de Derecho Laboral y Derecho Procesal Laboral* 1 (2019): 71-85. doi:/10.37767/2683-8761(2019)006

[118] Cristóbal Molina, "Control tecnológico del empleador y derecho probatorio: Efectos de la prueba digital lesiva de derechos fundamentales", *Temas laborales: Revista andaluza de trabajo y bienestar social*, n.º 150 (2019): 331-54.

[119] Jackson y Alvarado, "La incorporación de la prueba digital".

En algunas jurisdicciones, la inexistencia de un marco legal claro sobre el uso y admisibilidad de pruebas digitales puede representar un desafío adicional. En estas situaciones, las normas diseñadas para pruebas físicas no siempre son directamente aplicables a las evidencias electrónicas, lo que genera incertidumbre y puede derivar en su inadmisibilidad.[120]

Desde el punto de vista jurisprudencial, la nulidad de pruebas digitales ha sido objeto de análisis en múltiples casos, especialmente en el ámbito laboral. Por ejemplo, en situaciones donde un despido se fundamenta en correos electrónicos obtenidos sin autorización, los tribunales han debatido si la nulidad de la prueba conlleva automáticamente la nulidad del despido o si este puede ser considerado improcedente basándose en otras evidencias válidas. En este contexto, la Sentencia del Tribunal Constitucional Español 61/2021[121] adquiere particular relevancia. En ella se establece que las pruebas obtenidas mediante la vulneración de derechos fundamentales no solo deben ser consideradas nulas, sino que, además, podría ser pertinente otorgar una indemnización a la persona afectada. Este criterio subraya la necesidad de garantizar la protección de los derechos de las partes involucradas en cualquier procedimiento judicial que implique el uso de evidencias digitales.

3.7. Consecuencias en la protección de derechos y garantías de los procesados

En relación con el derecho a la protección de datos personales, la prueba digital está sujeta a una estricta regulación con el fin de proteger la privacidad y los datos personales de las partes. El incumplimiento de estas normas puede dar lugar a que la prueba sea declarada nula, al afectar la validez y continuidad del proceso judicial. Además, la jurisprudencia muestra diferentes concepciones respecto de cómo estas nulidades afectan decisiones judiciales tan importantes como la calificación de sobreseimientos u otras resoluciones. Tal diversidad de criterios crea inseguridad jurídica y subraya la necesidad de una regulación más uniforme y precisa al respecto. Por otro lado, la digitalización ha transformado significativamente el acceso a la justicia, especialmente a través de la implementación de audiencias virtuales y la simplificación de la presentación de pruebas.[122]

---

[120] Marlon Alexander Quchimbo Roman, Leidy Stefania Mereci Balcazar, y Mónica Eloiza Ramón Merchán. "La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos". *Dominio De Las Ciencias 10, N0 3*, (2024):1126–1142. doi.org/10.23857/dc.v10i3.3972

[121] Tribunal Constitucional Español, Sala Primera. Sentencia 61/2021, de 15 de marzo de 2021. Recurso de amparo 6838-2019. 6838-2019 (Tribunal Constitucional Español, 15 de marzo de 2021).

[122] Laura Nievas, "La prueba ilícita en la era digital".

Estas herramientas han facilitado una mayor participación en los procesos judiciales, lo que permite superar barreras geográficas y logísticas. Por otro lado, surgen una serie de nuevos desafíos respecto de la espontaneidad y veracidad de los testimonios rendidos en entornos virtuales. Por ejemplo, se ha mencionado por la Corte Constitucional de Colombia que se deben hacer modificaciones en las normas procesales para garantizar la preservación de los derechos de las partes y los testigos incluso en contextos digitales. También existe un retroceso en el manejo de ciertas inhabilidades que pueden afectar la integridad del proceso. La prueba digital ha generado un amplio debate en los tribunales respecto a su validez y fiabilidad. El avance de las tecnologías de la información y la comunicación ha transformado los procesos de recolección y presentación de evidencias, lo que ha dado lugar a interrogantes sobre su legitimidad debido a posibles vulneraciones de los derechos fundamentales.[123]

Este contexto ha favorecido una revisión crítica del marco normativo actual, dado que las prácticas inadecuadas pueden comprometer el derecho a un juicio justo y el derecho a la defensa. En consecuencia, los tribunales han comenzado a focalizar su atención en estos aspectos, destacando la necesidad de equilibrar los avances tecnológicos con la salvaguarda de las garantías procesales fundamentales. La prueba digital en el ámbito del proceso penal tiene la capacidad de evidenciar la comisión de delitos, pero exige un manejo sumamente cauteloso en su obtención para evitar vulneraciones a los derechos humanos.

La falta de regulación de manera uniforme y clara sobre cómo se maneja este tipo de pruebas las hace inadmisibles, pues si eso sucede, los resultados de los procesos penales pueden ser totalmente diferentes a los que hubieran sido. Por esta razón, se deben realizar lineamientos más específicos para asegurar que la recolección, presentación y análisis de evidencia digital sean apropiados, utilizados de manera ética y con respeto a los derechos de los acusados.[124]

3.8. Desafíos para la correcta aplicación de la prueba digital en Ecuador

El principal problema que enfrenta la aplicación de la prueba digital en Ecuador es la brecha digital, una desigualdad estructural en el acceso a las tecnologías de la información y la comunicación (TIC). Esta problemática se acentúa en las zonas rurales del país, donde el acceso a Internet es limitado y la disponibilidad de dispositivos

[123] Marcela Yepes, Jesús Pérez y Mario Peinado, "Aplicación de la prueba electrónica en el marco normativo colombiano", *Novum Jus* 16, n.º 1 (2022): 253-77 doi: 10.14718/NovumJus.2022.16.1.11

[124] Henry Saca, Anthony Marquez y César Arciniegas, "La inviabilidad de la prueba digital".

tecnológicos adecuados es escasa. En un contexto donde la digitalización juega un papel fundamental en los procesos judiciales, esta brecha representa un obstáculo significativo para garantizar una justicia accesible y equitativa.

La falta de conectividad impide que muchas personas puedan acceder a información legal, realizar trámites en línea o presentar pruebas digitales de manera eficiente. Además, la ausencia de infraestructura tecnológica adecuada limita la posibilidad de implementar procedimientos judiciales modernos que dependan de herramientas digitales para su correcta ejecución.[125]

Otro desafío crucial es la formación de los operadores de justicia. La correcta gestión de la prueba digital requiere conocimientos especializados en herramientas tecnológicas, normativas sobre ciberseguridad y metodologías de análisis forense digital. Sin embargo, muchos jueces, fiscales y defensores públicos en Ecuador no cuentan con la capacitación necesaria para manejar pruebas digitales de manera adecuada. Un reciente análisis sobre la competencia digital en el sector educativo ha revelado que las habilidades menos desarrolladas incluyen la resolución de problemas tecnológicos y la seguridad digital.

Este déficit de conocimientos técnicos en el ámbito judicial genera riesgos procesales, como la admisión de pruebas obtenidas sin cumplir con estándares de autenticidad e integridad, lo que puede derivar en nulidades o en la vulneración de derechos fundamentales. Para enfrentar esta problemática, es imprescindible la implementación de programas de formación continua que permitan a los operadores de justicia adquirir y actualizar sus competencias digitales, garantizando así un uso adecuado y seguro de las tecnologías en el ámbito procesal.

La infraestructura tecnológica también constituye una barrera significativa para la aplicación efectiva de la prueba digital en Ecuador. No todas las instituciones judiciales cuentan con el equipamiento necesario para gestionar este tipo de pruebas de manera eficiente. Más allá de la necesidad de disponer de hardware adecuado, como computadoras de alto rendimiento, servidores seguros y dispositivos de almacenamiento especializados, se requiere la implementación de software forense avanzado que permita la recuperación, análisis y validación de pruebas digitales.[126]

Sin embargo, incluso en aquellas instituciones que han logrado invertir en tecnología, persisten problemas de mantenimiento y actualización de equipos. La falta de

[125] Ricardo Becerra, “El reconocimiento de la brecha digital”
[126] Irma Ramos, José Herrera y Adanhari Fajardo, “Justicia digital”.

renovación de hardware y software puede comprometer la integridad de la prueba digital y dificultar su adecuada presentación en los procesos judiciales. Asimismo, la falta de procedimientos definidos para el almacenamiento y resguardo de la evidencia digital incrementa el riesgo de pérdida, alteración o manipulación de la información, debilitando la confiabilidad del sistema de justicia.

Los factores socioeconómicos también desempeñan un papel determinante en la implementación de la prueba digital en Ecuador. La crisis económica y las restricciones presupuestarias limitan la capacidad del Estado para invertir en tecnología y formación especializada. Esto afecta tanto a las instituciones públicas como a los ciudadanos, quienes a menudo carecen de los recursos necesarios para acceder a dispositivos tecnológicos o a una conexión estable a internet.

En el ámbito judicial, esta desigualdad tecnológica puede traducirse en una brecha en el acceso a la justicia, afectando especialmente a los sectores más vulnerables de la sociedad. La falta de acceso a medios digitales dificulta la presentación de pruebas electrónicas, la participación en audiencias virtuales y el ejercicio de una defensa efectiva en procesos judiciales. Además, la reducción de la inversión pública en modernización tecnológica impide la adopción de soluciones innovadoras que podrían agilizar la administración de justicia y mejorar la transparencia en los procedimientos legales.

Otro factor que obstaculiza la implementación de la prueba digital en Ecuador es la resistencia cultural a la adopción de nuevas tecnologías en los procesos judiciales. A pesar de los avances tecnológicos, aún persisten reticencias dentro del sistema de justicia para incorporar herramientas digitales de manera generalizada. Esta resistencia puede deberse al desconocimiento, al temor al cambio o a la falta de confianza en la seguridad y fiabilidad de las pruebas digitales. Muchos operadores de justicia continúan prefiriendo los métodos tradicionales de recolección y presentación de pruebas, lo que dificulta la modernización del sistema judicial.

Esta falta de aceptación tecnológica no solo retrasa la digitalización del sistema de justicia, sino que también limita el acceso de los ciudadanos a procesos judiciales más ágiles y eficientes. Para superar esta barrera, es fundamental promover una cultura de innovación y adaptación tecnológica dentro del sector judicial, acompañada de estrategias de capacitación y sensibilización dirigidas a jueces, fiscales, abogados y demás actores del sistema de justicia.[127]

[127] Endara Chamorro, Ronald Estiven Juan Sebastián Espinoza Jiménez, Eder Ronaldo López Fuel y Jessica Johanna Santander Moreno, “Análisis jurídico del deepfake”

En virtud de ello, la superación de estos obstáculos requiere un enfoque integral que combine inversiones en tecnología, programas de formación especializada y el desarrollo de normativas claras que regulen el uso de la prueba digital en el ámbito judicial. Solo a través de estas medidas será posible garantizar que la transformación digital de la justicia ecuatoriana se lleve a cabo de manera efectiva, promoviendo así un acceso equitativo a la justicia en la era digital.

3.9. Lineamientos para diseñar un protocolo nacional sobre la gestión de prueba digital

La instauración de un protocolo nacional para la gestión de la prueba digital resulta indispensable, ya que contribuye a optimizar la eficacia y legitimidad del proceso judicial mediante directrices metodológicas claras. En primer lugar, la implementación de un marco normativo estandarizado permite que los operadores de justicia actúen de manera homogénea en la recolección, tratamiento y presentación de evidencia digital. Esta uniformidad es crucial para preservar la integridad y autenticidad de las pruebas, garantizando que los procedimientos se ajusten a los principios de justicia y fiabilidad.

Uno de los aspectos esenciales en este contexto es la preservación de la cadena de custodia, dado que un protocolo bien estructurado establece procedimientos detallados que previenen cualquier alteración o manipulación de la evidencia digital desde su obtención hasta su presentación en juicio. Este control riguroso fortalece la validez probatoria de los elementos digitales, asegurando su admisibilidad en los procesos judiciales y reforzando su valor como medio de prueba.[128]

Asimismo, la implementación de este tipo de protocolos fomenta la transparencia y la rastreabilidad de los procedimientos. La documentación cuidadosa de cada paso en la gestión de las pruebas digitales permite verificar que los métodos aplicados sean defendibles y reproducibles. Esto fortalece la confianza en los procesos judiciales, pues garantiza que los datos recolectados sean legítimos y que las metodologías empleadas sean claras y accesibles para todas las partes involucradas.

Además, la existencia de un protocolo contribuye directamente a establecer criterios precisos sobre la admisibilidad y autenticidad de la prueba digital. Esto asegura que se cumplan los requisitos legales y normativos necesarios, lo cual evita discrepancias en la

[128] Cléver Tene Lema, y Diego Armando xPilco Pucha, “El manejo de la cadena de custodia”

interpretación de la normativa entre distintos juzgados y al garantizar la uniformidad en la aplicación de la ley.

En ese contexto, la actualización constante en las mejores prácticas para el manejo de pruebas digitales resulta indispensable para que los profesionales del derecho puedan actuar con conocimiento y confianza en un ámbito donde la tecnología avanza rápidamente. Este enfoque no solo fortalece el sistema judicial, sino que también incrementa la credibilidad y la confianza pública en la validez de las pruebas presentadas en los procesos legales.

1.1. Introducción

La digitalización ha cambiado la gestión de todos los procesos judiciales. Resulta de vital importancia, por tanto, la creación de un protocolo nacional que regule la recolección, manejo y presentación de la evidencia digital. Esto es necesario para cubrir la autenticidad, integridad y cadena de custodia respecto de los datos que se manejan. Simultáneamente, se debe establecer un marco normativo efectivo que regule el uso de la evidencia digital en el Poder Judicial ecuatoriano.

1.2. Justificación

La implementación de un Protocolo Nacional para la Gestión de la Evidencia Digital es fundamental para cristalizar los procesos de confianza en la Función Judicial en el Ecuador, al incluir la garantía de que las decisiones que involucren evidencia digital sean rigurosas, confiables y justas. Esto significará, además de resolver los desafíos actuales, preparar al sistema de justicia para los próximos pasos a seguir en la tecnología aplicada a dicho campo.

1.3. Objetivos del protocolo

La implementación de estándares claros para la recolección, manejo y presentación de pruebas digitales es fundamental para garantizar la integridad y validez de los procesos judiciales en la era tecnológica.

De igual forma, la capacitación continua de los operadores de justicia —jueces, fiscales, peritos y defensores— resulta indispensable para cerrar la brecha entre el derecho y la tecnología. Programas de formación especializada en informática forense, análisis de metadatos y gestión de plataformas digitales permitirían a los profesionales interpretar y evaluar críticamente las pruebas electrónicas, evitando errores que podrían derivar en

injusticias. Esta preparación debe complementarse con simulacros de casos reales y colaboraciones interdisciplinarias con expertos en ciberseguridad, reforzando las competencias prácticas del sistema.

La estandarización de procedimientos no solo optimiza la eficiencia judicial, sino que también fortalece la transparencia y la confianza ciudadana. Al unificar criterios y hacer públicos los protocolos aplicados, se genera un marco previsible que reduce discrepancias y arbitrariedades, permitiendo que todas las partes involucradas comprendan las reglas del juego. Esta claridad, sumada a auditorías externas y mecanismos de rendición de cuentas, contribuye a legitimar las decisiones judiciales en un contexto donde la desinformación y el escepticismo hacia las instituciones suelen proliferar.

Asimismo, la adopción de estas medidas facilita la adaptación del sistema judicial a los desafíos tecnológicos contemporáneos, desde el auge de los ciberdelitos hasta la complejidad de las pruebas en entornos *cloud* o *blockchain*. Una justicia ágil y técnicamente competente no solo resguarda los derechos de las víctimas y acusados, sino que también envía un mensaje de modernización y resiliencia frente a un panorama digital en constante evolución, consolidando así su rol como pilar esencial del Estado de derecho en el siglo XXI.

1.4. Elementos para considerar en la estructura del protocolo

La correcta gestión de la prueba digital dentro de los procesos judiciales requiere un protocolo sólido que asegure su integridad, validez y admisibilidad. Este apartado detalla los componentes fundamentales de dicho protocolo, lo que proporciona un marco sistemático que guía su aplicación. En primer lugar, se definen los conceptos clave y el alcance del protocolo, estableciendo los lineamientos generales que lo rigen. A continuación, se aborda el proceso de recolección de prueba digital, destacando las mejores prácticas y medidas necesarias para preservar su autenticidad.

Se analizan también los procedimientos para el manejo y almacenamiento seguro de la evidencia, considerando los estándares técnicos y jurídicos que garantizan su custodia adecuada. También se expone el proceso de presentación de la prueba digital en juicio, al enfatizar los requisitos técnicos y argumentativos necesarios para su aceptación. Como corolario, se resalta la importancia de la capacitación continua de los actores involucrados, así como la necesidad de implementar mecanismos de seguimiento y evaluación que permitan la mejora constante del protocolo en función de los desafíos emergentes.

Figura 2. Elementos para considerar en la estructura del protocolo. Elaboración propia

Sección I: Definiciones y alcance

Definición de prueba digital y su relevancia en el proceso penal: La prueba digital se refiere a cualquier información de naturaleza electrónica que puede ser utilizada como evidencia en un proceso penal. Esto incluye datos almacenados, transmitidos o generados por dispositivos electrónicos como computadoras, teléfonos inteligentes, redes sociales, sistemas de videovigilancia, entre otros. Su relevancia radica en que en un mundo cada vez más digitalizado, muchos delitos dejan rastros en formato electrónico, convirtiéndola en un recurso clave para la investigación y resolución de casos penales.

Estrategia: Realizar un estudio comparativo con otros sistemas judiciales internacionales para consensuar una definición operativa y técnica de "prueba digital".

Indicadores:

- Número de reuniones de expertos realizadas.
- Porcentaje de consenso alcanzado en la definición.

Alcance del protocolo en relación con los diferentes tipos de prueba digital: El alcance del protocolo cubre diferentes tipos de prueba digital, como archivos digitales (documentos, imágenes, videos, registros de llamadas), metadatos asociados a archivos y comunicaciones, registros de sistemas informáticos y bases de datos, actividades en redes sociales y plataformas digitales, datos extraídos de dispositivos IoT (Internet de las cosas) y comunicaciones electrónicas como correos electrónicos y mensajes instantáneos.

Estrategia: Delimitar las áreas y tipos de casos en los que se aplicará el protocolo mediante consultas con representantes de cada instancia judicial.

Indicadores:

- Cobertura porcentual de procesos judiciales abarcados.
- Satisfacción de los operadores de justicia en la delimitación de alcances (medido mediante encuestas).

Sección II: Recolección de prueba digital

Establecimiento de procedimientos estandarizados para la recolección de datos digitales: Para garantizar una recolección adecuada, se deben establecer procedimientos estandarizados que incluyan identificar y documentar la fuente de la prueba digital, evitar la manipulación directa del dispositivo antes de iniciar el proceso y seguir guías claras según el escenario, ya sea que los dispositivos estén encendidos o apagados.

Estrategia: Desarrollar manuales operativos y guías técnicas que describan detalladamente cada paso en la recolección de datos digitales.

Indicadores:

- Número de manuales desarrollados y distribuidos.
- Tasa de cumplimiento de los procedimientos en auditorías internas.

Instrucciones sobre el uso de herramientas forenses para asegurar la integridad de la prueba: El uso de herramientas forenses certificadas es esencial para asegurar la integridad de la prueba. Entre los mecanismos más relevantes se encuentran las funciones *hash*, sellos de tiempo, firmas digitales avanzadas y los procedimientos de cadena de custodia digital Estas herramientas deben generar registros de auditoría automáticos y permitir la realización de copias exactas o "imágenes forenses" de los dispositivos originales sin alterarlos.

Estrategia: Seleccionar, adquirir y capacitar en el uso de herramientas forenses digitales, realizando pruebas piloto que validen su eficacia.

Indicadores:

- Número de herramientas evaluadas y aprobadas.
- Resultados de las pruebas piloto en términos de eficiencia y confiabilidad.

Protocolos para preservar la cadena de custodia desde el momento de la recolección: Esto incluye documentar cada etapa del manejo de la prueba, etiquetar y

sellar los dispositivos recolectados, y registrar cada traslado con firmas de las partes responsables. El acceso debe estar limitado a personal autorizado.

Estrategia: Implantar sistemas de registro digital que permitan el seguimiento en tiempo real de la evidencia desde su recolección hasta su presentación en juicio.

Indicadores:

- Porcentaje de evidencias con cadena de custodia registrada digitalmente.
- Tiempo promedio de actualización de registros en la cadena de custodia.

Sección III: Manejo y almacenamiento

Lineamientos sobre el almacenamiento seguro de la prueba digital: El almacenamiento seguro de la prueba digital es crucial. Se deben utilizar sistemas que cuenten con medidas de seguridad avanzadas, como encriptación y acceso restringido y mantener un registro detallado de quién y cuándo accedió a la prueba.

Estrategia: Implementar protocolos de encriptación, backup y control de acceso, junto con auditorías periódicas para verificar la integridad del almacenamiento.

Indicadores:

- Frecuencia de las auditorías realizadas.
- Incidentes de pérdida o alteración de datos reportados.

Procedimientos para el control de acceso a la prueba digital, que incluyen políticas que especifican quién puede manipular la prueba digital: Para el control de acceso, es necesario establecer políticas claras que definan los roles y responsabilidades de quienes pueden manipular la prueba. Las auditorías periódicas verificarán el cumplimiento de estas políticas, y se recomienda implementar sistemas de autenticación multifactorial para proteger el acceso.

Estrategia: Establecer un sistema jerárquico de permisos y autenticación robusta, que limite el acceso a la evidencia digital a personal autorizado y capacitado.

Indicadores:

- Número de accesos no autorizados detectados.
- Porcentaje de personal con certificación en manejo seguro de la evidencia.

Sección IV: Recomendaciones sobre reglas de presentación de la prueba digital en juicio

Reglas para la presentación de la prueba digital ante el tribunal, como requisitos sobre los informes periciales: La presentación de la prueba digital ante el

tribunal requiere informes periciales claros que expliquen su relevancia, autenticidad y procedencia. Estos informes deben incluir evidencias de las metodologías utilizadas durante la recolección y el análisis.

Estrategia: Definir estándares técnicos y formales para la presentación de evidencia digital, incluyendo la elaboración de informes periciales certificados y validados por expertos.

Indicadores:

- Porcentaje de pruebas presentadas con informes periciales.
- Evaluación de la calidad de los informes en revisión judicial.

Formular criterios sobre admisibilidad de la prueba digital: La prueba digital debe auténtica, relevante y no manipulada. La recolección y el manejo deben cumplir con las leyes y regulaciones aplicables.

Estrategia: Establecer criterios técnicos y legales claros que sirvan como referencia para evaluar la autenticidad y relevancia de la prueba digital en cada caso.

Indicadores:

- Número de casos en los que la evidencia digital fue admitida sin objeciones técnicas.
- Tasa de revisión de criterios de admisibilidad y actualizaciones realizadas.

Sección V: Contenido de la capacitación y educación

Formular un programa de capacitación continua para jueces, fiscales y abogados sobre el manejo de la prueba digital: Cursos teóricos y prácticos sobre aspectos técnicos y legales de la prueba digital y actualizarse regularmente para reflejar los avances tecnológicos y normativos.

Estrategia: Diseñar e implementar un programa de capacitación integral para jueces, fiscales, abogados y técnicos, que combine teoría y práctica, con simulaciones y ejercicios en entornos controlados.

Indicadores:

- Número de cursos y talleres realizados anualmente.
- Nivel de mejora en las competencias técnicas de los operadores, medido a través de evaluaciones pre y post capacitación.

Diseñar un modelo de formación especializada de peritos: A instancias del Consejo de la Judicatura, en su rol rector sobre el sistema de peritos, determinar las necesidades de capacitación y diseñar un sistema de entrenamientos.

Estrategia: Determinar las demandas actuales y futuras en la actividad pericial en materia de forensia digital y realizar entrenamientos en:

- RAM, data recovery, blockchain, hard drive y big data forensics
- Estegoanálisis
- Aplicación de normas ISO 27041:2015, 27043:2015 y 27037:2012
- Verificación de integridad (MD5, SHA1, SHA256)
- Metodología para el peritaje digital

Indicadores:

- Cantidad de peritos entrenados
- Niveles de esclarecimiento de delitos digitales.
- Cantidad de peritos informáticos capacitados por cada cantón.

Incluir módulos prácticos que simularían situaciones reales en el manejo de la prueba digital: Los módulos prácticos deben simular situaciones reales, al organizar talleres que reproduzcan escenarios de recolección, manejo y presentación de pruebas digitales. También se pueden realizar simulacros de audiencias judiciales para mejorar las habilidades de los participantes.

Estrategia: Incorporar módulos prácticos en el programa de formación que simulen situaciones reales de manejo de prueba digital, evaluando la respuesta y desempeño del personal.

Indicadores:

- Resultados de las simulaciones (porcentaje de aprobación).
- Retroalimentación de los participantes sobre la aplicabilidad de los ejercicios.

Sección VI: Seguimiento y evaluación

Establecer un comité de supervisión para evaluar la implementación del protocolo y hacer ajustes cuando sea necesario: Establecer un comité de supervisión compuesto por un grupo multidisciplinario. Este comité realizará evaluaciones periódicas y emitirá informes con recomendaciones para la mejora continua.

Estrategia: Crear un comité interdisciplinario que supervise la implementación del protocolo, evalúe su eficacia y proponga ajustes periódicos basados en los avances tecnológicos y necesidades del sistema judicial.

Indicadores:

- Frecuencia de reuniones del comité.
- Número de ajustes y actualizaciones implementadas en el protocolo.

Establecer mecanismos de retroalimentación para la mejora continua del protocolo: Encuestas y reuniones con los actores involucrados. El análisis de casos concretos permitirá identificar áreas de mejora y actualizar el protocolo según sea necesario.

Estrategia: Establecer canales formales para recibir sugerencias, denuncias y evaluaciones de los operadores de justicia y usuarios del sistema, integrando estos aportes en revisiones regulares del protocolo.

Indicadores:

- Número de sugerencias y observaciones recibidas.
- Tiempo de respuesta y efectividad en la implementación de mejoras derivadas de la retroalimentación.

3.10. Viabilidad de la propuesta

La estandarización de procedimientos (como la recolección con herramientas forenses certificadas y la cadena de custodia digital) se sustenta en prácticas ya validadas en sistemas judiciales avanzados, lo que reduce la incertidumbre en su implementación. Además, la inclusión de indicadores medibles —como tasas de cumplimiento en auditorías o número de cursos impartidos— facilita la evaluación objetiva de cada fase. Sin embargo, una limitación crítica radica en la dependencia de recursos tecnológicos y humanos especializados: la adquisición de software forense, la capacitación constante y la infraestructura de almacenamiento seguro requieren inversiones sostenidas, que pueden ser inaccesibles para jurisdicciones con presupuestos limitados o sistemas judiciales fragmentados.

En cuanto a la adaptabilidad del protocolo, su diseño modular y la creación de un comité de supervisión interdisciplinario permiten actualizaciones periódicas ante innovaciones tecnológicas, como el uso de inteligencia artificial en el análisis de datos o la aparición de dispositivos IoT más complejos. No obstante, existe una limitación inherente

a la velocidad de los cambios legales y técnicos: mientras los protocolos se revisan, las prácticas delictivas evolucionan, generando brechas temporales que podrían explotarse. Concretamente, la criptografía cuántica o los metaversos podrían desafiar los criterios de admisibilidad actuales, obligando a ajustes reactivos en lugar de preventivos. Esta tensión entre lo estático (protocolos) y lo dinámico (tecnología) exige agilidad institucional, algo difícil de garantizar en sistemas judiciales tradicionalmente burocráticos.

En ese orden de ideas, la capacitación continua es un aspecto viable para cerrar la brecha de conocimiento entre operadores jurídicos y expertos técnicos. La combinación de módulos teóricos y simulaciones prácticas —como audiencias con pruebas digitales ficticias— asegura un aprendizaje aplicable. Los indicadores de mejora en competencias, medidos mediante evaluaciones pre y post formación, refuerzan su efectividad. Sin embargo, una limitación significativa es la resistencia cultural al cambio: jueces o fiscales con arraigo en métodos tradicionales podrían subestimar la relevancia de la prueba digital o desconfiar de procesos automatizados. Además, la rotación de personal o la falta de incentivos para la certificación continua pueden diluir el impacto de los programas de capacitación, especialmente en regiones con alta carga laboral y escaso tiempo para formación.

Es necesario destacar el rol del Consejo de la Judicatura, cuya existencia está refrendada en la sección quinta del Capítulo Cuarto, correspondiente al Título IV de la Constitución de la República de Ecuador. Está integrado a la función judicial y se encarga de administrar, vigilar y garantizar la disciplina de los demás órganos que integran esa función.[129] El artículo 186 de la Ley Suprema designa al CJ para determinar la cantidad de jueces, peritos, fiscales y notarios de cada cantón. También se le atribuye la facultad de definir la cantidad de tribunales y juzgados en cada región del país en correspondencia con la densidad de población, lo cual, por supuesto, incluye a los funcionarios del sistema de justicia penal.

Es necesario tener en consideración que la formación especializada de peritos informáticos representa un costo de cierta consideración, ya que actualmente este proceso se cotiza en 200 dólares para la habilitación o más 1200 para la formación de nivel superior[130], lo que se acompaña de la emisión de licencias y certificaciones. En adición,

[129] Ecuador, Constitución de la República, art. 178 y 181.

[130] En estos momentos se ofrecen cursos especializados en UNIR, los cuales se imparten en colaboración con la Asociación Profesional de Peritos Informáticos (ASPEI), ILM Forensics y Evidentia. Consultar ofertas en https://ecuador.unir.net/ingenieria/curso-perito-judicial-informatico/ y https://educacioncontinua.uhemisferios.edu.ec/programa/certificacion-para-peritaje-informatico/.

la realización de peritajes extraordinarios, está específicamente regulada en el Reglamento del sistema pericial integral de la función judicial, donde se prevé el pago de horarios diferenciados por pericias "de alta complejidad técnica, así como los peritajes que no se encuentran en el catálogo de especialidades periciales o a su vez no cuenta con perito calificados en determinada especialidad".[131]

Por último, los mecanismos de seguimiento y retroalimentación son viables para mantener la integridad del protocolo a largo plazo. La revisión periódica por un comité multidisciplinario y la incorporación de sugerencias de usuarios aseguran que el protocolo no se vuelva obsoleto. No obstante, su éxito depende críticamente de la transparencia y voluntad política: si los informes de auditorías se ocultan o las recomendaciones del comité se ignoran por intereses institucionales, el protocolo perderá credibilidad. Asimismo, la estandarización internacional propuesta en la Sección I —mediante estudios comparativos— podría chocar con diferencias jurisdiccionales en marcos legales, lo que limitaría su armonización global y generaría inconsistencias en casos transfronterizos. En síntesis, aunque el protocolo es sólido en diseño, su eficacia real estará sujeta a la capacidad de superar estas barreras estructurales y culturales.

Como colofón de este proceso, es necesario incrementar la producción jurisprudencial por parte de los órganos facultados para ello en el sistema de justicia ecuatoriano. Se requiere el establecimiento de pronunciamientos vinculantes sobre los modos de proceder en casos donde la evidencia digital, aun cuando no está tasada, sea trascendental en la determinación del contenido de la sentencia judicial. Se debe prever que las actuales tendencias de desarrollo tecnológico introduzcan en el futuro cercano nuevos conceptos que conduzcan a modificar paradigmas y tradiciones judiciales. Para evitar la inseguridad jurídica que pudiera generar la inexistencia de vacíos legales específicos, corresponde fundamentalmente a la Corte Constitucional y la Corte Nacional de Justicia, mantener una claridad doctrinal en los enfoques a emplear en el sistema de impartición de justicia.

[131] Ecuador. Consejo de la Judicatura, *Reglamento del sistema pericial integral de la función judicial,* Resolución 216-2024, (2024) 4, https://www.funcionjudicial.gob.ec/resources/pdf/resoluciones/2024/ 216-2024.pdf

Conclusiones y recomendaciones

Conclusiones

La evidencia digital se ha consolidado como un elemento esencial en la administración de justicia en el siglo XXI, adquiriendo una relevancia particular en el contexto ecuatoriano. Su desarrollo es reflejo del impacto de la transformación digital en los sistemas judiciales, lo que pone de manifiesto la imperiosa necesidad de reformar y actualizar las normativas vigentes para responder de manera efectiva a las especificidades y desafíos que el derecho penal enfrenta en un entorno progresivamente digitalizado.

No obstante, la incorporación de pruebas digitales en los procesos penales conlleva desafíos significativos en lo que respecta a su autenticidad, integridad y la adecuada preservación de la cadena de custodia, elementos determinantes para su admisibilidad y valor probatorio. La correcta gestión de estas evidencias no solo garantiza el cumplimiento del debido proceso, sino que también incide directamente en la toma de decisiones judiciales, asegurando la equidad y justicia en la resolución de los casos.

Además, la creciente relevancia de las pruebas digitales exige una formación adecuada para los operadores de justicia en Ecuador. Desde jueces hasta fiscales y defensores públicos, todos deben estar equipados con las herramientas y conocimientos necesarios para manejar adecuadamente las evidencias digitales. Esto es crucial para garantizar un proceso judicial que refleje los estándares modernos de legalidad y eficiencia.

Por otro lado, aunque el marco legal ecuatoriano, como el Código Orgánico General de Procesos (COGEP), está orientado principalmente hacia los procedimientos civiles, su capacidad de incluir pautas sobre pruebas digitales muestra una apertura a la adaptación normativa necesaria. Esta flexibilidad resulta esencial para abordar las necesidades del derecho penal en el país, especialmente en el contexto de delitos informáticos y otros crímenes que requieren un análisis detallado de las evidencias digitales. En este aspecto, corresponde un rol fundamental al Consejo de la Judicatura, órgano integrante del poder judicial que, por mandato constitucional ejerce la rectoría de los procesos técnico jurídicos y de capacitación.

Adicionalmente, a medida que los tribunales reconocen la importancia de las pruebas digitales, es crucial encontrar un equilibrio entre la innovación tecnológica y la

protección de las garantías procesales. Un manejo cauteloso de las evidencias digitales permitirá evitar vulneraciones a los derechos humanos en el proceso penal, asegurando que el desarrollo de la justicia no comprometa principios fundamentales.

Como parte de las conclusiones es menester señalar entre los hallazgos de este estudio, que se determinó la inexistencia de recursos metodológicos como protocolos o guías que sirvan de orientación a los operadores del sistema de justicia, particularmente a los jueces, fiscales, abogados y peritos. La literatura especializada informa sobre un sólido desarrollo doctrinal que actualiza las concepciones tradicionales de prueba, medio de prueba y fuente de prueba a los escenarios digitales.

En tal sentido sebe decirse que, a pesar de los incuestionables avances en materia legislativa, el sistema de justicia ecuatoriano está requerido de alinearse con los estándares internacionales que han sido presentados por organismos internacionales como la ISO, la INTERPOL y naciones de alto desarrollo tecnológico. Se necesita también explorar las posibilidades de adhesión al convenio de Budapest como instrumento marco para propiciar una sólida colaboración con agencias extranjeras y para el establecimiento de vínculos bilaterales y multilaterales.

El estudio de casos realizado revela que, en causas penales de elevada significación política, las evidencias digitales, aun sin constituir pruebas tasadas, tienen un peso significativo en el esclarecimiento de los delitos y en la demostración pública de la responsabilidad de los autores. En la era digital, las tecnologías de la información y las comunicaciones transversalizan todas las esferas de la vida social, lo que se refleja en el incremento en cantidad y diversidad de los delitos informáticos y, consecuentemente impacta en la práctica judicial.

Una de las principales contribuciones, que a su vez resalta como novedad del estudio, reside en definir los lineamientos para diseñar un protocolo nacional sobre el manejo de la prueba digital. Su construcción debe partir del análisis de las limitaciones y oportunidades de tipo tecnológico y las actuales carencias normativas. Los estándares que se modelen deberán abarcar la recolección, integración, manejo y almacenamiento, así como la presentación de las pruebas digitales. En todos los casos, las acciones deberán observar rigurosamente el respeto a los derechos fundamentales de las personas.

De cara al futuro, será conveniente conformar equipos multidisciplinarios que asuman la tarea de diseñar, pilotar, implementar y monitorear la funcionalidad del protocolo de manejo de la evidencia digital. Para ello será propicio atraer al sistema de justicia ecuatoriano, las mejores experiencias en temas de empleo de la evidencia digital y, con base

en la visión prospectiva del desarrollo tecnológico, prever los posibles escenarios y las medidas a adoptar para adecuar el proceso penal a las tendencias más probables.

A modo de resumen cabría decirse que el mejoramiento de los actuales procedimientos para el manejo y gestión de las evidencia digitales, se asiente sobre pilares, a saber, el desarrollo y ampliación de la infraestructura tecnológica, la incorporación de las mejores experiencias de los países y organismos supranacionales que ejercen el liderazgo en este frente, la adecuación del sistema normativo, especialmente en las normas procesales para asimilar de manera flexible los nuevos cambios que se impongan a partir de la evolución tecnológica y, por último, más no menos importante, el reforzamiento de las capacidades humanas, tanto en términos cuantitativos como en la calidad y rigor de la capacitación de especialistas, operadores legales y funcionarios en general.

Recomendaciones

Se recomienda a las autoridades judiciales valorar la conveniencia a crear equipos multidisciplinarios que, sore la base de las propuestas que se presentan, trabajen en el diseño e implementación de un protocolo nacional sobre el manejo de la evidencia digital.

Es fundamental que las autoridades ecuatorianas actualicen y fortalezcan el marco legal existente, como el COGEP, para incluir disposiciones específicas y detalladas sobre la gestión de pruebas digitales. Esto incluye la creación de protocolos para la recolección, preservación y presentación de evidencias digitales, asegurando que se ajusten a los estándares internacionales y a las particularidades del derecho penal en el entorno digital.

Implementar sistemas de certificación y validación de pruebas digitales mediante el uso de tecnologías que garanticen la integridad y trazabilidad de las evidencias. Además, es crucial establecer procedimientos estandarizados para la cadena de custodia, con la participación de peritos especializados en informática forense, para evitar la manipulación o alteración de las pruebas.

El Consejo de la Judicatura y otras instituciones relacionadas con la administración de justicia en Ecuador deberían diseñar e implementar programas de capacitación continua en materia de pruebas digitales. Estos programas deben estar dirigidos a jueces, fiscales, defensores públicos y otros operadores jurídicos, con el fin de que adquieran competencias técnicas y legales para manejar evidencias digitales de manera efectiva y conforme a la ley.

Resulta conveniente establecer alianzas entre las instituciones del Estado implicadas en la gestión de la evidencia digital y las universidades y centros de

investigación, a fin de promover proyectos que permitan ampliar las capacidades tecnológicas del país para obtener y procesar la evidencia digital, así como para desarrollar la formación continua de operadores del derecho en cuanto a las tecnologías involucradas en este proceso.

Promover reformas legales que permitan una mayor especialización en el tratamiento de delitos informáticos y otras infracciones relacionadas con el entorno digital. Esto incluye la creación de juzgados especializados en materia digital y la inclusión de peritos en tecnología dentro de los equipos de investigación, para garantizar un análisis riguroso y técnico de las pruebas digitales.

Establecer un marco de protección de derechos fundamentales en el uso de pruebas digitales, asegurando que su obtención y manejo no violen la privacidad, la intimidad u otros derechos humanos. Para ello, se recomienda la creación de comités de supervisión que evalúen el impacto de las tecnologías en los procesos penales y velen por el respeto de las garantías constitucionales.

Será beneficioso continuar desarrollando estudios sobre el tema donde se profundice en:

La actualización de los tipos penales donde se prevé el uso de las TIC para adecuar los elementos de integración a las necesidades de protección social.

Analizar las particularidades del empleo de la evidencia digital en los procesos abreviados.

El establecimiento de disposiciones administrativas para compeler a las empresas desarrolladoras e importadoras de tecnologías a declarar las características de los nuevos productos y servicios tecnológicos para que sean considerados en el protocolo de manejo de la evidencia digital.

El empleo de sistemas de inteligencia artificial en el proceso de recolección, integración y análisis de la evidencia digital.

Bibliografía

Acevedo Silva, Ana Milena y Deyanira Castillo, "La tecnología y el carácter de la notificación personal frente al principio de publicidad". Tesis de maestría, Universidad La Gran Colombia, Bogotá, 2022. https://repository.ugc.edu.co/server/api/core/bitstreams/ed008317-c952-4e6b-ab05-9ef83dc4cfbd/content

Almeida Idiarte, Rodrigo "La prueba testimonial y los testigos de oídas" (tesis de maestría, Universitát de Gironas, 2022.) 4, Https://dugidoc.udg.edu/bitstream/handle/10256/21614/Almeidaidiarte.TFM.pdf?sequence=1&isAllowed=y.

Arias, Vicente y Luis Cedeño. "Análisis de la confiabilidad en la incorporación de los medios de prueba en materia penal en el Ecuador". *Religación* 9, n.° 41 (2024): e2401306, doi: 10.46652/rgn.v9i41.1306.

Ayala, Rafael. "Credibilidad testimonial en el proceso penal", *Revista Brasileira de Direito Processual Penal* 6, n.° 1 (2020): 453-80, https://www.redalyc.org/articulo.oa?id=673971418015.

Banegas, Danilo y Daniel Andrade. "Análisis Forense en dispositivos móviles Android para casos de ciberextorsión: Revisión sistemática de literatura". *MQRInvestigar* 8, n.° 3 (2022): 4076-97. doi:10.56048/mqr20225.8.3.2024.4076-4097.

Barahona, Evelyn. "La prueba electrónica en el proceso penal". *Revista Ciencia Multidisciplinaria CUNORI* 6, n.º 2 (2022): 55–64. https://dialnet.unirioja.es/servlet/ articulo?codigo=8873602&orden=0&info=link

Barrios Baudor, Leandro Guillermo. *"*La integridad y/o autenticidad de los medios de prueba digital en el proceso laboral: una aproximación al tema a propósito de los correos electrónicos*." Revista de Trabajo y Seguridad Social.* CEF (2017): 23–52. doi:10.51302/rtss.2017.1780

Basantes, Klever y Danny Sánchez. "La exclusión de la prueba en materia penal frente al debido proceso", *Polo del Conocimiento* 9, n.° 3 (2024): 2873-94, doi: 10.23857/pc.v9i3.6822.

Becerra, Ricardo "El reconocimiento de la brecha digital para garantizar el acceso efectivo a la administración de justicia civil", Precedente. Revista Jurídica 23 (2023): 11-35. https://doi.org/10.18046/prec.v23.5875

Ben, Celia. "La prueba digital. aspectos procesales". *Revista Derecho y Proceso*, n.º 3 (2023): 29-45, doi: 10.69592/2951-844X-N3-JUNIO-2023-ART2

Benavides, Merck, y Edward Benavides. *Derechos, garantías y principios constitucionales y su aplicación en el proceso penal*. Quito: Cevallos Editora Jurídica, 2019.

Bermejo, José y Enrique Pozo "La ineficacia de la defensa técnica como causa de nulidad en el proceso penal: análisis jurídico". *Visionario Digital* 8, n. 2 (2024): 150-67. doi: 10.33262/visionariodigital. v8i2.3033.

Briceño Ruiz, Anahí Verónica y Diego Adrián Ormaza Ávila. "Régimen Normativo del Sistema Nacional de Protección y Asistencia a Víctimas, Testigos y Otros Participantes en el Proceso Penal en el Ecuador", *Revista Multidisciplinaria Arbitrada de Ciencias Sociales,* 8, no. 3 (2024) 4675–4705: doi:10.56048/MQR20225.8.3.2024.4675-4705

Caballero Laura, Raúl. "El método de la prueba indiciaria, aplicable para la valoración de indicios y la prueba directa en las sentencias sobre delitos de concusión (colusión), peculado y corrupción de funcionarios (cohecho)", *Revista Oficial del Poder Judicial,* 11, n.° 13, (2020): 363-388, doi.org/10.35292/ropj.v11i13.49

Calle, Miguel y Noel Batista. "La cooperación internacional en el proceso penal, extradición, asistencia judicial y armonización de normativas". *Revista Científica de Educación Superior y Gobernanza Interuniversitaria Aula* 24 6, n.° 9 (2024): 55-69, doi:10.56124/aula24.v6i9.005.

Castellanos, María "Motivaciones y consecuencias de usar el escrache feminista como mecanismo de denuncia pública por parte de víctimas de violencia sexual en Colombia, un análisis crítico del sistema penal patriarcal". *Nuevo Foro Penal* 18, n.° 98 (2022: 115-67). doi:10.17230/nfp18.98.4.

Coloma, Rodrigo. "La prueba y sus significados". *Revista chilena de derecho* 46, n.° 2 (2019): 427-49. doi:10.4067/S0718-34372019000200427.

Consejo de Europa. *Convenio de Budapest sobre la Ciberdelincuencia*. Serie de Tratados No. 185 (2001), https://rm.coe.int/1680081561

Consejo de Europa. *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas*. Diario Oficial de la Unión Europea L 63/28 (2023), https://rm.coe.int/1680a83724&ved=2ahUKEwivgsPul8yNAxXVSTABHUz-AM0QFnoECAkQAQ&usg=AOvVaw0hIEEFou2J0gg7J_iZj83v

Dalal, Mukesh y Juneja, Mamta. “Steganography and Steganalysis (in digital forensics): a Cybersecurity guide”, Multimedia tools and aplications 80, no. 4, (2021), 5723-5771. doi:https://doi.org/10.1007/s11042-020-09929-9

Daniela Alejandra León Ordoñez, Rayza Belén León Ortiz y Armando Rogelio Durán Ocampo, “La prueba en el código orgánico general de procesos”, Universidad y Sociedad 11, n. 1 (2019): 359-368, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000100359&lng=es&nrm=iso

Dellepiane, A. *Nueva Teoría General de la Prueba.* Bogotá: Ed. Temis, 2016.

Echandia, Hernando Devis. *Compendio de la Prueba Judicial* (Buenos Aires: Rubinzal-Culzoni Editores, 1984), https://www.salapenaltribunalmedellin.com/images/doctrina/libros01/ compendio_de_la_prueba_judicial_i.pdf.

Ecuador Corte Nacional de Justicia. “Oficio: 171-2020-P-CPJP-YG”. 3 de febrero de 2020. https://www.cortenacional.gob.ec/cnj/images/pdf/consultas_absueltas/No_Penales/Civil/127.pdf.

Ecuador. Corte Provincial de Justicia Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito. “Resolución Nro. 1972-2018”. *Juicio n.° 03282-2017-00133*, 13 de noviembre de 2018.

Ecuador. *Código Orgánico General de Procesos (COGEP)*. Registro Oficial 506, Suplemento, 22 de mayo de 2015, https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Orgánico-General-de-Procesos.pdf.

Ecuador. Consejo de la Judicatura, *Reglamento del sistema pericial integral de la función judicial,* Resolución 216-2024, 4, https://www.funcionjudicial.gob.ec/resources/pdf/resoluciones/2024/ 216-2024.pdf

Ecuador. *Constitución Política de la República del Ecuador*, Registro Oficial1, 11 de agosto de 1998, arts. 24 y 76

Ecuador. *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*. Registro Oficial 557, Suplemento, 17 de abril de2002

Ecuador. *Código Orgánico Integral Penal*. Registro Oficial 180, 10 de febrero de 2014.

Ecuador. Corte Constitucional “Sentencia No. 2064-14-EP/21” sobre *juicio No. 2064-14-EP* de 27 de enero de 2021, 20

Ecuador. Corte Nacional de Justicia “Tribunal Penal de la CNJ dictó sentencia en el caso Sobornos 2012 – 2016”, https://www.cortenacional.gob.ec/cnj/index.php/noticias-2020/128-abril-2020/264-tribunal-pernal-de-la-cnj-dicto-sentencia-en-el-caso-sobornos-2012-2016

Ecuador. Corte Nacional de Justicia. "Oficio: 171-2020-P-CPJP-YG". 3 de febrero de 2020, https://www.cortenacional.gob.ec/cnj/images/pdf/consultas_absueltas/No_Penales/Civil/127.pdf.

Ecuador. Corte Provincial de Justicia Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito. "Resolución Nro. 1972-2018". en *Juicio n.° 03282-2017-00133*, 13 de noviembre de 2018

Ecuador. *Ley Orgánica de Garantías Jurisdiccionales.* Suplemento del Registro Oficial No.52, 22 de octubre 2009, art. 89.

Ecuador. Procuraduría General de la República. "Caso Sobornos 2012-2016: Doce funcionarios públicos constan en la acusación particular", Boletín de Prensa, Quito, 20 de noviembre de 2019, http://www.pge.gob.ec/index.php/prensa/boletines-de-prensa/noviembre-2019/caso-sobornos-2012-2016-doce-funcionarios-publicos-constan-en-la-acusacion-particular

El Universo. "Caso Petroecuador: audiencia preparatoria de juicio contra Nilsen Arias y otros 16 acusados por el delito de cohecho sin fecha para reanudarse", 14 de octubre, 2024. https://www.eluniverso.com/noticias/

Endara Chamorro, Ronald Estiven, Juan Sebastián Espinoza Jiménez, Eder Ronaldo López Fuel y Jessica Johanna Santander Moreno. "Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador" *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, IX. n° 1 (2024)240-252: doi:10.35381/racji.v9i1.3530

Escobar, Mirian. "La valoración de la prueba, en la motivación de una sentencia en la legislación ecuatoriana". Tesis de maestría, Universidad Andina Simón Bolívar, Sede Ecuador, 2010. https://repositorio.uasb.edu.ec/bitstream/10644/1135/1/T0836-MDP.

Freire Padilla, Génesis Belén y Estefanía Cristina Mayorga Mayorga. "Los medios probatorios en los actos de proposición en el ordenamiento jurídico ecuatoriano" *Revista Latinoamericana de Ciencias Sociales y humanidades.* Nº.2 (2024), 777: 196: doi: 10.56712/latam.v5i2.1915, p.182

García, Ramiro, Agustín Pérez y Alba Guevara. *El proceso penal: Derechos y garantías en el proceso penal*. t. 1 (Lima: Ara Editores, 2014).

González, José "La prueba digital y la cadena de custodia", *Anales de la Facultad de Derecho*, n.° 38 (2021: 43-79), https://www.ull.es/revistas/index.php/derecho/article/view/2425.

González, José. "La prueba digital y la cadena de custodia." *Anales de la Facultad de Derecho* 38 (2021): 43-79.

González, José. "La prueba digital y la cadena de custodia", *Anales de la Facultad de Derecho,* n.° 38 (2021): 43-79, https://www.ull.es/revistas/index.php/derecho/article/view/2425.

González, Violeta. "Adolescencia "desesperada" y criminalidad juvenil de "subsistencia". Factores situacionales de vulnerabilidad social en la selectividad penal". *Anuario de justicia de menores 18,* (2018): 241-88, https://dialnet.unirioja.es/servlet/articulo?codigo=7144472.

González, Violeta. "Adolescencia 'desesperada' y criminalidad juvenil de 'subsistencia': Factores situacionales de vulnerabilidad social en la selectividad penal". *Anuario de justicia de menores*, n.° 18 (2018): 241-88. https://dialnet.unirioja.es/servlet/articulo?codigo=7144472.

Guerra Soto, Mario. *Análisis Forense Informático*. (Ediciones Ra-Ma.:2021), 60-1, https://www.ra-ma.es/media/rama/files/book-attachment-6367.pdf

Guerra Soto, Mario. *Análisis Forense Informático*. Ediciones Ra-Ma.:2021. https://www.ra-ma.es/media/rama/files/book-attachment-6367.pdf

Jackson, Imaicela y Lissette Alvarado. "La incorporación de la prueba digital en el derecho procesal ecuatoriano", *Revista LEX* 7, n.º 27 (2024): 1338-50. https://doi.org/10.33996/revistalex.v7i27.247

Jaya, Víctor. "Testimonio sobre el abuso sexual y su efecto jurídico en las sentencias emitidas por tribunales", *Lex: Revista de Investigación en Ciencias Jurídicas* 4, n.° 11 (2021): 48-59, doi: 10.33996/revistalex.v4i11.70.

Jimbo Granda, Martha Elizabeth. "Principio de igualdad de armas en relación con el testimonio anticipado en víctimas de delitos sexuales en el contexto ecuatoriano y peruano". Tesis de maestría Universidad Técnica Particular de Loja, 2020. https://bibliotecautpl.utpl.edu.ec/cgi-bin/abnetclwo?METS=61044333737

Lema, Cléver Tene y Diego Armando xPilco Pucha. "El manejo de la cadena de custodia como requisito fundamental para la legitimidad probatoria de los procedimientos administrativos disciplinarios de la Policía Nacional". (Tesis de maestría, Universidad de Chimborazo, 2023), http://dspace.unach.edu.ec/handle/51000/11333

León Ordoñez, Daniela Alejandra, Rayza Belén León Ortiz y Armando Rogelio Durán Ocampo. "La prueba en el código orgánico general de procesos". *Universidad y*

Sociedad, 11, n. 1 (2019): 359-368, http://scielo.sld.cu/ scielo.php?script= sci_arttext&pid=S2218-36202019000100359&lng=es&nrm=iso

López, Zander. "Validez jurídica de la prueba digital en Guatemala". *Revista Ciencia Multidisciplinaria CUNORI* 7, n.° 2 (2023): 203-14.

Magro, Vicente. "Casuística práctica de la prueba digital en el proceso civil y penal". *Actualidad Civil,* n.° 1 (2020). https://www.asambleaex.es/vernumero-8637.

Martínez, Gemma. "Problemática jurídica de la prueba digital y sus implicaciones en los principios penales". *Revista Electrónica de Ciencia Penal y Criminología*, n.° 24-23 (2022): 1-38. https://reunir.unir.net/handle/123456789/15287

Medina Medina, Vanessa Estefanía y Yudith López Soria. "Los medios telemáticos en el proceso penal frente al debido proceso", Sociedad & Tecnología, 5, no. S1 (2022): 86–99: doi: 10.51247/st.v5iS1.235

Mendoza Prado, María de Lourdes."Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal". *Código Científico Revista De Investigación* 5, Nº E3 (2024), 480–498. https://doi.org/10.55813/gaea/ccri/v5/nE3/328

Molina, Cristóbal. "Control tecnológico del empleador y derecho probatorio: Efectos de la prueba digital lesiva de derechos fundamentales" *Temas laborales: Revista andaluza de trabajo y bienestar social*, n.º 150 (2019): 331-54

Montenegro Bósquez, Israel Emiliano, Diego Francisco Granja Zurita, Mario Ramiro Aguilar Martínez y Diego Patricio Gordillo Cevallos. "Las aclaraciones a testigos por parte de los jueces penales en las audiencias de juicio, un análisis desde el estándar de prueba". *Revista Universidad y Sociedad* 14, nº.2 (2022): 51-56, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000200051&lng=es&tlng=es.

Nahuatt Javier, Margarita. "Diferencia entre datos de prueba, medios de prueba y prueba: en el nuevo proceso penal acusatorio" *Revista del Instituto de la Judicatura Federal,* (2014): 161-173, https://codigo-juridico-mx.webnode.es/l/dato-de-prueba-medio-de-prueba-y-prueba-los-conceptos-que-los-penalistas-se-niegan-a-entender/

Nievas, Laura. "La prueba ilícita en la era digital. Aspectos procesales de un problema tradicional con contenido nuevo en el marco del proceso laboral de Córdoba". *Revista de Estudio de Derecho Laboral y Derecho Procesal Laboral* 1 (2019): 71-85.

ONU. *Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020. UN,* 6 de abril de 2021, https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101015.pdf

Organización Internacional de Normalización *ISO/IEC 27041:2015 Tecnologías de la información – tecnologías de la seguridad – directrices para asegurar la adecuación de métodos de investigación de incidentes.* (2015). https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027041-2015.pdf.

_____ . *ISO/IEC 27043:2015 Tecnologías de la información – tecnologías de la seguridad – principios de investigación numérica en los procesos.* (2015). https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027043-2015.pdf.

_____Organización Internacional de Normalización. ISO/IEC 27037:2012 Tecnologías de la *información – tecnologías de la seguridad – directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.* (2012). https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf.

Orlando J. Pacheco. "Principio probatorio de mismidad en el Código Orgánico Procesal Penal venezolano. Una hermeneusis del derecho probatorio" *Revista Escandalar Investigativa*. No. 2 (2024): 165-177: http://revistas.unellez.edu.ve/index.php/resi/article/view/2581/2299

Pabón, Pedro. *La prueba pericial, sistema acusatorio: Parte general y especial*. Colombia: Librería Jurídica Sánchez R.. 2006.

Pabón, Pedro. *La prueba pericial, sistema acusatorio: Parte general y especial*. Colombia: Librería Jurídica Sánchez R., 2006.

Pacheco, Orlando J. "Principio probatorio de mismidad en el Código Orgánico Procesal Penal venezolano. Una hermeneusis del derecho probatorio". *Revista Escandalar Investigativa,* No. 2 (2024): 165-177: http://revistas.unellez.edu.ve/ index.php/resi/article/view/2581/2299

Parkinson, Simon y Saad Khan. "The role of Artificial Intelligence in digital forensics: Case studies and future directions" *Assesment and development matter.* Vo. 16, n.

1, 2024: 42-47, https://pure.hud.ac.uk/ws/portalfiles/portal/81261791/ accepted_version.pdf

Parkinson, Simon y Saad Khan. “The role of Artificial Intelligence in digital forensics: Case studies and future directions”, *Assesment and development matters* 16, N. 1, 2024, 42-47, https://pure.hud.ac.uk/ws/portalfiles/portal/81261791/ accepted _version.pdf

Perito IT. "ISO/IEC 27037:2012 Nueva norma para la Recopilación de Evidencias Digitales." Blog. 23 de octubre de 2012. https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/.

Pincay Rodríguez, Yuli Llerena. “Testimonio anticipado en el ámbito de los delitos sexuales en el Ecuador”. *Revista Científica de Educación Superior y Gobernanza Interuniversitaria Aula* 24, n.° 6 (2024): 41-54, doi: 10.56124/aula24.v6i9.004.

Pino Icaza, Edith. “Informática Forense como medio de prueba en el Ecuador”. *Revista Universidad de Guayaquil* 108, Nº. 3, (2020),56-63: https://dialnet.unirioja.es/ servlet/articulo?codigo=8368273&orden=0&info=link

Porras, Pablo. “La incorporación de la prueba digital en el proceso penal colombiano”. Tesis de maestría, Unilibre, 2023. https://repository.unilibre.edu.co/handle/10901/29366?show=full.

Quchimbo Roman, Marlon Alexander, Leidy Estefanía Mereci Balcázar, y Mónica Eloiza Ramón Merchán. “La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos”. *Dominio De Las Ciencias*. 10, N0 3, (2024):1126–1142. doi.org/10.23857/dc.v10i3.3972

Quintero, Mary, “La prueba testimonial de la víctima de delitos de violencia contra la mujer, valorada desde una perspectiva de género: Causa M.M.A.C. Resolución de Corte Provincial No. 5101283 (Trata de personas)”. Tesis de maestría, Universidad Andina Simón Bolívar, Sede Ecuador, 2020. https://repositorio.uasb.edu.ec/ handle/10644/7281.

Ramírez, Carlos. *Apuntes sobre la prueba en el COGEP* (Quito: Corte Nacional de Justicia, 2017), https://www.cortenacional.gob.ec/cnj/images/ Produccion_CNJ/ La%20prueba%20en%20el%20COGEP.pdf.

Ramos, Irma José Herrera y Adanhari Fajardo. “Justicia Digital: Un estándar de derechos humanos para la administración de justicia expedita por tribunales online, de forma pronta, completa e imparcial”. *Revista Jurídica Jalisciense* 3, n.º 5 (2022) 263-300: https://doi.org/10.32870/rjj.v3i5.157

Reedy, Paul. “Interpol review of digital evidence for 2019–2022”. *Forensic Science International Sinergic*. 6:100313 (2023): doi: 10.1016/j.fsisyn.2022.100313

Revelez, Daniel L. “Dato de prueba, medio de prueba y prueba: los conceptos que los penalistas se niegan a entender”. *Revista Código Jurídico Mx,* S/N (2021). https://codigo-juridico-mx.webnode.es/l/dato-de-prueba-medio-de-prueba-y-prueba-los-conceptos-que-los-penalistas-se-niegan-a-entender/

Riofrio García, Iván Alejandro, Wagner Guido Morales Román, Johanna Irene Escobar Jara y Fátima Eugenia Campos Cárdenas. “La prueba electrónica en los procesos penales en Ecuador en concordancia con celeridad y economía procesal.” *Serie Científica de la Universidad de las Ciencias Informáticas* 18, Nº. 2 (2025) 49-71, http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2306-24952025000200049&lng=es&tlng=es.

Roatta, Santiago, Maria Eugenia Casco y Martin Fogliatto, “El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012”, XXI Congreso Argentino de Ciencias de Computación (Junín, 2015), https://sedici.unlp.edu.ar/ handle/ 10915/50586

Román, Luis. “La prueba en el proceso penal”. *Aldaba,* n.° 24 (1995): 47-80, doi: 10.5944/aldaba.24.1995.20334

Saca, Henry Anthony Márquez y César Arciniegas. “La inviabilidad de la prueba digital por falta de regulación en los delitos informáticos”. *593 Digital Publishet CEIT* 8, n.º 4 (2023): 21-34:doi.10.33386/593dp.2023.4.1887

Sentis, S. “Qué es la prueba (Naturaleza de la prueba) 1”. *Revista derecho Procesal Iberoamericana* 2, n.° 3 (2013): 259-60.

Solórzano León, Erika Estefanía “La valoración de las pruebas en las sentencias emitidas por los Jueces de la Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito de la Corte Provincial de Justicia de Pichincha, frente a casos de abuso sexual en el periodo de enero hasta diciembre del año 2019”. Tesis de maestría, Universidad Central de Ecuador, 2023. https://www.dspace.uce.edu.ec/server/api/core/bitstreams/9508a225-607e-46a8-bb10-50c22916c3f0/content

Tene Lema, Cléver y Diego Armando xPilco Pucha, “El manejo de la cadena de custodia como requisito fundamental para la legitimidad probatoria de los procedimientos administrativos disciplinarios de la Policía Nacional”. Tesis de maestría, Universidad de Chimborazo, 2023. http://dspace.unach.edu.ec/handle/51000/11333

Topping, Alexandra "Police and CPS scrap digital data extraction forms for rape cases. Exclusive: case of two complainants funded by Equality and Human Rights Commission forces U-turn" The Guardian, 16. julio, 2020, https://www.theguardian.com/society/2020/jul/16/police-and-cps-scrap-digital-data-extraction-forms-for-cases

Torres Loján, Carlos Geovanny. "WhatsApp como herramienta de prueba en litigios por obligaciones financieras: Una mirada al sistema judicial ecuatoriano". *Revista Lex* 7, n.° 25 (2024): 496-511. doi:10.33996/revistalex.v7i25.196.

Toscano López, Fredy Hernando, Juan Carlos Naizir Sistac, Luis Guillermo Acero Gallego y Ramiro Bejarano Guzmán, *Derecho probatorio: desafíos y perspectivas.* Universidad Externado de Colombia, 2021.

Tribunal Constitucional Español, Sala Primera. Sentencia 61/2021, de 15 de marzo de 2021. Recurso de amparo 6838-2019. 6838-2019 (Tribunal Constitucional Español, 15 de marzo de 2021)

Tulcanaza Ruiz, Edward Andrés, Elias Alberto Herrera Peñafiel, Yudith López Soria y Holger Geovanny García Segarra, "Restricciones procesales para la realización del testimonio anticipado en el proceso penal ecuatoriano", *Revista UGC*, 3 N0. 1 (2025): 147–155. https://universidadugc.edu.mx/ojs/index.php/rugc/ article/view/

Twinning, William. *Repensar el derecho probatorio. Ensayos exploratorios*, Editorial de la Universidad Nacional de Colombia, 2022.

Valderrama, Diego. "Diferencias entre objeto de prueba, fuente de prueba y medio de prueba" Pasión por el Derecho, s/n, 2021, https://lpderecho.pe/diferencias-objeto-prueba-fuente-prueba-medio-prueba

Vega, Sandy. *La prueba electrónica y su aplicación en el Código Orgánico General de Procesos* (Guayaquil: UCSG, 2016). http://repositorio.ucsg.edu.ec/bitstream/3317/7128/1/T-UCSG-PRE-JUR-DER-98.pdf

Vela Andrade, Nelson. "La prueba ilícita en el proceso penal ecuatoriano: Bases doctrinales y jurídicas" *Journal of business and entrepreneurial sutdies* 4 nº. 2 (2020): 295 – 307: doi.10.37956/jbes.v4i2.107

Yanes, Marjorie. "El testimonio anticipado como medio de prueba en delitos de abuso sexual: estudio de casos" (tesis de maestría, Universidad Andina Simón Bolívar, 2021), https://repositorio.uasb.edu.ec/handle/10644/8202

Yepes, Marcela Jesús Pérez y Mario Peinado, “Aplicación de la prueba electrónica en el marco normativo colombiano”, *Novum Jus* 16, n.º 1 (2022): 253-77 doi: 10.14718/NovumJus.2022.16.1.11

Zambrano, Alfonso. “La prueba ilícita en el proceso penal: Estudio doctrinario y jurisprudencial” *Journal of business and entrepeneural studies*, 4, n. 2 (2020): 295 – 307. doi:10.37956/jbes. v4i2.107.

Zapata, Daniela. “La prueba en material penal y el debido proceso”. Tesis de maestría, Uniandes, 2016. https://dspace.uniandes.edu.ec/handle/123456789/5413.

Zeferín, Iván. *La prueba libre y lógica: Sistema penal acusatorio mexicano.* Ciudad de México: Instituto de la Judicatura Federal, 2016. https://archivos.juridicas.unam.mx/www/bjv/libros/11/5263/6.pdf