

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

Autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano

Trabajo de titulación previo a la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador

AUTOR:
Cañizares Jácome, Brayan Alexander

TUTORA:
Dra. Rosita Elena Campuzano Llaguno

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, Brayan Alexander Cañizares Jácome, con cédula de ciudadanía 055070888-7, autor del trabajo de investigación titulado: "Autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano", certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mi exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 25 de junio de 2026.



Brayan Alexander Cañizares Jácome
C.I: 0550708887

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Dra. Rosita Elena Campuzano Llaguno catedrática adscrita a la Facultad de Ciencias Políticas y Administrativas, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación "Autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano", bajo la autoría de Brayan Alexander Cañizares Jácome, por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad, en Riobamba, a los 25 días del mes de junio del 2026.



Dra. Rosita Elena Campuzano Llaguno

C.I. 0602523805

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación "Autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano", por Brayan Alexander Cañizares Jácome, con cédula de identidad número 055070888-7, bajo la tutoría de Dra. Rosita Elena Campuzano Llaguno; certificamos que recomendamos la aprobación de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 02 de julio de 2026.

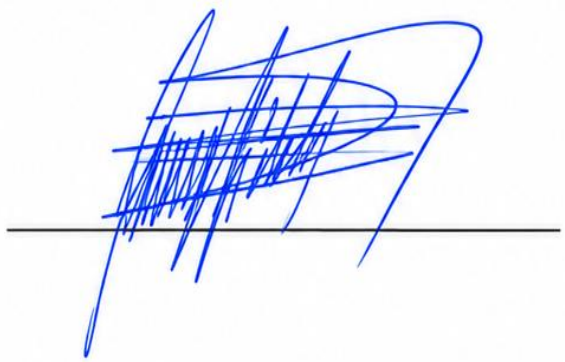
Dr. Segundo Walter Parra Molina
PRESIDENTE DEL TRIBUNAL DE GRADO



Dr. Nelson Francisco Freire Sánchez
MIEMBRO DEL TRIBUNAL DE GRADO



Dr. Fredy Roberto Hidalgo Cajo
MIEMBRO DEL TRIBUNAL DE GRADO



CERTIFICACIÓN

Que, **BRAYAN ALEXANDER CAÑIZARES JÁCOME** con CC: 055070888-7, estudiante de la Carrera **DERECHO**, Facultad de **CIENCIAS POLÍTICAS Y ADMINISTRATIVAS**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"Autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano"**, cumple con el **10% de similitudes y 3% de detección de IA**, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente, autorizo continuar con el proceso.

Riobamba, 08 de junio de 2026

Dra. Rosita Elena Campuzano Llaguno
TUTOR(A)

DEDICATORIA

A Dios, por ser el sustento espiritual que ha guiado cada uno de mis pasos, por otorgarme la fortaleza, la sabiduría y la perseverancia necesaria para culminar esta importante etapa de mi formación académica.

A mis padres, Miriam Jácome y Eduardo Cañizares, a quienes expreso mi más profundo agradecimiento por su amor incondicional, sacrificio y apoyo constante. Su ejemplo de esfuerzo y dedicación ha sido un pilar fundamental en la consecución de este logro.

A mi abuelo, Segundo Cañizares, por sus valiosos consejos y enseñanzas, los cuales han contribuido significativamente en mi desarrollo personal y profesional. De manera muy especial, a la memoria de mis abuelitas, Dorilla Villegas y Carmelina Villegas, quienes, aunque físicamente ausentes, permanecen constantemente en mi vida como fuente de inspiración; a ellas dedico este logro con profundo respeto y gratitud eterna.

A mis hermanos, Eduardo Israel, Richard David y Johanna Elizabeth Cañizares, por su constante apoyo y por acompañarme a lo largo de este proceso, constituyéndose en un valioso soporte en el cumplimiento de esta meta.

A mi tío Miguel Cañizares, y tía Mónica Floridalva a quienes expreso un reconocimiento especial por su respaldo, orientación y confianza brindada en momentos clave de mi formación tanto académica, profesional y personal.

A mis tíos Xavier Cañizares y Soledad Vasco, por su acompañamiento y buenos deseos durante este trayecto académico.

A mis amigos Jairo Mera y Fabricio Cabai, por su apoyo incondicional y estar presentes durante esta etapa de mi vida; y a mi primo Fulthon Cajas, por su cariño, compañía y motivación a lo largo de este proceso.

Finalmente, a todas aquellas personas que, de manera directa e indirecta, contribuyeron en la realización de este trabajo, expreso mi sincero agradecimiento.
Con respeto y gratitud.

Bryan Alexander Cañizares Jácome

AGRADECIMIENTO

Agradezco a la Universidad Nacional de Chimborazo, por haberme brindado la oportunidad de formarme académica y profesionalmente, proporcionándome los conocimientos y herramientas necesarias para el desarrollo del presente trabajo.

De manera especial, expreso mi más sincero agradecimiento a mi tutora, Dra. Rosita Campuzano, por su valiosa guía, dedicación y apoyo constante durante el desarrollo de esta investigación, siendo fundamental para la culminación de la misma.

Bryan Alexander Cañizares Jácome

ÍNDICE GENERAL

DECLARATORIA DE AUTORÍA
DICTAMEN FAVORABLE DEL PROFESOR TUTOR
CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL
CERTIFICADO ANTIPLAGIO
DEDICATORIA
AGRADECIMIENTO
ÍNDICE GENERAL
ÍNDICE DE TABLAS
ÍNDICE DE FIGURAS
RESUMEN
ABSTRACT
CAPÍTULO I. 14
1. INTRODUCCIÓN 14
1.1 Planteamiento del problema 15
1.2 Justificación 16
1.3 Objetivos 17
1.3.1 Objetivo general 17
1.3.2 Específicos 17
CAPÍTULO II. MARCO TEÓRICO 19
2.1 Estado del arte 19
2.2 Marco teórico 22
UNIDAD I: Fundamentos jurídicos y normativos de la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano 22
UNIDAD II: Factores técnicos, jurídicos y procedimentales que afectan la autenticidad y fiabilidad de la evidencia digital 34
UNIDAD III: Evaluación del cumplimiento normativo y propuestas de mejora para fortalecer la autenticidad y fiabilidad de la evidencia digital 44
CAPÍTULO III. METODOLOGÍA 51
3.1 Tipo de diseño de la investigación 51
3.2 Enfoques de investigación 51
3.3 Técnicas de recolección de datos 52
3.4 Población de estudio y tamaño de la muestra 52
3.5 Métodos de análisis 52
3.5.1 Método deductivo 53
3.5.2 Método inductivo 53
3.5.3 Método jurídico-analítico 53
3.5.4 Método dogmático 53
3.6 Procesamiento de datos 54

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 55
4.1 Resultados de la encuesta a los cinco jueces y cinco abogados 55
4.2 Discusión de resultados 65
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 67
5.1 Conclusiones 67
5.2 Recomendaciones 68
BIBLIOGRAFÍA 69
ANEXOS 74
Anexo 1. Formato de la encuesta a operadores de justicia 74
Anexo 2. Consentimiento Informado 76

ÍNDICE DE TABLAS.

Tabla 1. Clasificación por tipo y contenido de dispositivo electrónico.....31
Tabla 2. Pregunta 1.....55
Tabla 3. Pregunta 2.....56
Tabla 4. Pregunta 3.....57
Tabla 5. Pregunta 4.....58
Tabla 6. Pregunta 5.....59
Tabla 7. Pregunta 6.....60
Tabla 8. Pregunta 7.....61
Tabla 9. Pregunta 8.....62
Tabla 10. Pregunta 9.....63
Tabla 11. Pregunta 10.....64

ÍNDICE DE FIGURAS

Figura 1. Sistema ABIS 49
Figura 2. Pregunta 1 55
Figura 3. Pregunta 2 56
Figura 4. Pregunta 3 57
Figura 5. Pregunta 4 58
Figura 6. Pregunta 6 59
Figura 7. Pregunta 6 60
Figura 8. Pregunta 7 61
Figura 9. Pregunta 8 62
Figura 10. Pregunta 9 63
Figura 11. Pregunta 10 64

RESUMEN

Actualmente, la utilización de la tecnología es cada vez más indispensable en todos los ámbitos de la vida, incluido en los medios de prueba, porque hoy es posible incluir dentro del proceso legal penal información que se origina de dispositivos electrónicos, así como de sistema informáticos y redes sociales que ya constituyen elementos probatorios actualmente. La presente investigación analiza de manera directa y sustancial la autenticidad y fiabilidad de la evidencia digital dentro de los procesos penales en el Ecuador, para que de esta manera se pueda determinar cuáles son las deficiencias normativas y técnicas que afectan directa e indirectamente la valoración probatoria de la evidencia digital. De tal manera que, se pueda obtener resultados coherentes y precisos encaminados a orientar el tratamiento, mejorar y fortalecer la administración de justicia. El objetivo general se enfoca netamente la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano para determinar las falencias normativas y técnicas que afectan su valoración probatoria, con el fin de establecer lineamientos orientados a mejorar su tratamiento y fortalecer la administración de justicia. Se utilizó una metodología con enfoque jurídico-analítico con uso de la revisión bibliográfica de doctrina y jurisprudencia además de un análisis sobre la práctica de la evidencia digital en Ecuador. Los resultados arrojaron que la evidencia digital dispone de alto impacto actualmente como parte de la toma de decisiones de jueces, peritos, fiscales y otros actores dentro del proceso, sin embargo, se observó limitantes asociadas con la falta de capacitación de los operadores de justicia de forma técnica y legal para tratar este tipo de evidencia, además los vacíos jurídicos en cuanto a la interpretación de la norma. Finalmente, se observó que la evidencia digital actualmente constituye un elemento clave dentro del sistema judicial. Por cuanto, radica en la necesidad objetiva de garantizar que la evidencia digital sea obtenida, preservada y valorada eficazmente dentro del proceso judicial, permitiendo identificar vacíos normativos y deficiencias técnicas que pueden afectar su credibilidad probatoria, para ello se necesita fortalecer la seguridad jurídica y la correcta administración de justicia.

Palabras clave: autenticidad, fiabilidad, evidencia digital, valoración probatoria, operadores de justicia, técnica, legal, sistema judicial.

ABSTRACT

The rapid advancement of technology has rendered its use indispensable across all spheres of contemporary life, including the legal domain. In criminal proceedings, information derived from electronic devices, computer systems, and social networks is increasingly incorporated as probative material, giving rise to what is now recognized as digital evidence. This research analyses the authenticity and reliability of digital evidence within criminal proceedings in Ecuador, with the aim of identifying normative and technical deficiencies that affect its evidentiary assessment. The findings are intended to guide the proper treatment of such evidence, ultimately improving and strengthening the administration of justice. To this end, the study adopts a legal-analytical methodology grounded in a systematic review of legal doctrine and jurisprudence, complemented by an examination of the practical application of digital evidence in the Ecuadorian criminal justice system. The results show that digital evidence exerts a significant influence on judicial decision-making, playing a central role for judges, forensic experts, prosecutors, and other procedural actors. Nevertheless, critical limitations were identified, particularly the lack of adequate technical and legal training among justice operators, alongside notable legal gaps in the interpretation of applicable norms. These findings underscore that digital evidence has become a key element within the Ecuadorian judicial system. Consequently, ensuring its proper collection, preservation, and evidentiary assessment is not merely advisable but objectively necessary. Addressing the identified normative gaps and technical deficiencies is therefore essential to safeguarding evidentiary credibility, reinforcing legal certainty, and guaranteeing the sound administration of justice.

Keywords: digital evidence, justice system personnel, technical, legal, judicial system.

Reviewed and improved by Jacqueline Armijos



Firmado electrónicamente por:
JACQUELINE ALEXANDRA ARMIJOS MORA
Validar únicamente con FirmaEC

CAPÍTULO I.

1. INTRODUCCIÓN

En el mundo globalizado de hoy, las tecnologías de la información y comunicación han transformado los procesos de dinamización de la información en todos los contextos incluyendo el jurídico, en el cual se amplía su uso debido a que en la administración de justicia se requieren mecanismos que permitan este fin y sea posible mejorar la transparencia en los datos e información que se procesa. En base a lo dicho, Navas y Vásquez (2025) refieren la necesidad de mirar a la evidencia digital como un elemento probatorio que se ha usado para diversos casos incluyendo los delitos del ciberespacio con utilización de recursos digitales como correo, mensajería, así como redes sociales, archivos de audio y video, del mismo modo el uso de blockchain o grandes bloques de información que permiten la reconstrucción de los hechos.

Es así que, la asociación de la evidencia digital en el entorno penal del Ecuador involucra aquella necesidad de utilizar aspectos jurídicos y técnicos asociados con la fiabilidad de la información, buscando mejorar aspectos como la seguridad informativa. En el caso de las pruebas comunes puede haber mayor facilidad de duplicación o manipulación de las mismas, es por esto que cada vez los procesos de valoración de la prueba se van tecnificando, de tal forma que se garantice la integridad informativa (De la Torre et al., 2024), por consiguiente, se evidencia la necesidad del uso de protocolos para fortalecer el debido proceso y la seguridad jurídica, en casos donde la toma de decisiones y las pruebas conjuntamente con su tratamiento y manipulación son de carácter sustancial en un proceso judicial.

Por otra parte, en el Ecuador, a partir de la Constitución de la República (2008) determina que el Estado es un país soberano y democrático estipulado así desde el art. 1, además de ello, es preciso señalar que el debido proceso positivado en el art. 76 de la CRE, es denominado como un derecho fundamental complejo y de carácter instrumental en la administración de justicia, debido a que incluye elementos homogéneos e intrínsecos que complementan a los procesos judiciales integralmente, así como, aquel marco de obtención probatoria, mismo que no debe ser vulnerado ni obtenido con violación a la norma. Sin embargo, esta normativa y muchos otros cuerpos legales no afirman de manera expresa cómo tratar la evidencia digital, por consiguiente, aún persisten vacíos jurídicos referentes a al derecho probatorio.

El Código Orgánico Integral Penal (2014), en su artículo 500 identifica a la prueba digital como aquel mecanismo que puede tener susceptibilidad de ser analizado, pero tampoco se definen aspectos técnicos que formen parte de la cadena de custodia digital, ni el labor específico de los médicos forenses cuando disponen de este tipo de pruebas. Entonces se ha evidenciado la ausencia de protocolos o marcos concretos legales que respondan a esta necesidad, además de resoluciones judiciales “erga omnes” que sean determinantes para mitigar este conflicto legal y que no pongan en riesgo el debido proceso y demás principios adecuados para garantizar justicia, al no haber procesos estandarizados para la valoración de la prueba

digital, lo que puede reducir su eficiencia probatoria y podrían darse casos de nulidad o impunidad. Según Molina (2021) afirma que, tampoco existe capacitación sobre el uso de medios digitales probatorios para los jueces, fiscales y otros actores de justicia, lo que también limita una valoración accesible y pertinente de este tipo de evidencia digital.

En vista de ello, se analizó la normativa internacional, tal es el caso de, La Norma ISO/IEC 27037:2012 donde se detalla la posibilidad de recopilación, preservación y otros procesos de la evidencia probatoria digital, de tal manera que sea posible comparar con el marco normativo del Ecuador y a ello se debe incorporar el análisis de los principios de autenticidad, integridad de la prueba y confiabilidad de la misma, de tal forma que garantice un adecuado proceso evitando impunidad objetiva.

La presente investigación supone la necesidad sustancial de analizar la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano para determinar las falencias normativas y técnicas que afectan su valoración probatoria, con el fin de establecer lineamientos orientados a mejorar su tratamiento y fortalecer la administración de justicia. Además, es preciso señalar que existe una falta de reglas técnicas y legales claras con relación a este problema jurídico, por cuanto, de ello se desprende, ¿por qué, y en qué medida la ausencia de disposiciones tanto técnicas como jurídicas concretas afectan la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano, y qué normas procedimentales son necesarias para que las pruebas sean valoradas con sujeción al debido proceso?

Es así que, la evidencia digital debe ser manejada como un mecanismo probatorio en el proceso penal del Ecuador, y también es necesario verificar los vacíos jurídicos y técnicos al respecto que pueden debilitar su valoración probatoria, de esta forma también se puede fortalecer la administración de justicia, a partir de un enfoque cualitativo descriptivo y analítico-sintético donde se analizó la doctrina y jurisprudencia existente sobre el tema propuesto.

1.1 Planteamiento del problema

En la actualidad, se ha incurrido en un proceso de transformación e innovación global, donde la tecnología es la clave, dentro de procesos legales y penales en las distintas naciones del mundo, considerando además que, el uso masificado de la tecnología ha permitido que muchos delitos se esclarezcan usando sistemas informáticos de gran alcance, como; redes sociales o plataformas digitales, implicando la necesidad de replantear las técnicas con las que se llega a la verdad procesal (Navas y Vásquez, 2025).

Por lo tanto, la investigación forense involucra aspectos de uso de la tecnología de la información, criminología y evaluación de datos, de tal forma que es indispensable comprender y aplicar técnicas innovadoras para lograr la verdad probatoria, tomando en cuenta además que, tales datos requieren un análisis con sentido ético, privado, e imparcial (Universidad Técnica del Norte de Ibarra, 2020). Si bien, la evidencia digital implica todo tipo de dato o información que dispone de valor probatorio y se emite por medio del uso de dispositivos electrónicos como computadoras de escritorio, portátiles, estaciones de trabajo, smarthphones, servidores y más, los cuales se usan dentro de los procesos penales para identificar los hechos imputados en un delito (Avemañay et al., 2025)

En el caso del Ecuador, la Constitución (2008) en su artículo 76 detalla la necesidad de cumplimiento del debido proceso en la administración de justicia, tomando en cuenta que, las pruebas que se obtienen con violación a este principio carecen de eficacia probatoria.

En base a este contexto, el Código Orgánico Integral Penal, no cita de manera expresa parámetros sustanciales para el tratamiento de la evidencia digital. Sin embargo, en el artículo 500 del código antes indicado manifiesta que: El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. (COIP, 2023).

Sin embargo, se determina que todo contenido digital es un elemento que puede ser muy susceptible de valor probatorio, pero tampoco se mencionan los procesos concretos de la cadena de custodia para este tipo de mecanismos, así como no se detallan los aspectos que el forense debe cumplir para lograr la fiabilidad de este tipo de pruebas.

Bajo este análisis, el Código Orgánico Integral Penal brinda diversas reglas para el análisis, valoración, recuperación y presentación del contenido digital que reposa en diversos sistemas informáticos. No obstante, cada una de estas reglas son parámetros generales que no responden a una necesidad específicas. Es decir, no contempla disposiciones específicas que regulen la cadena de custodia digital, ni define procedimientos técnicos que garanticen la recolección, preservación y autenticación de los medios electrónicos.

Lo anterior demuestra que, no existen normas concretas sobre el tema en cuestión, lo cual puede dar paso a malas interpretaciones por los actores de justicia, como jueces, fiscales, peritos y abogados, referente al tratamiento de la evidencia digital, influyendo de manera directa en el debido proceso y la seguridad jurídica que debe ser garantizada en un Estado de Derecho como el Ecuador. La insuficiente capacitación tecnológica de los operadores de justicia, limita su capacidad para valorar correctamente este tipo de evidencia, lo que incrementa el riesgo de alteración, manipulación o pérdida de información relevante, provocando inseguridad jurídica, vulnerando el artículo 76 de la Constitución del Ecuador (2008) que refiere al debido proceso y criterios de valoración desiguales, especialmente en investigaciones relacionadas con delitos informáticos, cuyo esclarecimiento depende de la fiabilidad de los elementos probatorios digitales.

Por consiguiente, el problema que se analiza en el presente documento tiene que ver con la falta de lineamientos en el marco normativo y de protocolos diseñados para la preservación y valoración de la evidencia digital dentro del contexto penal del Ecuador, y a ello se añade la falta de capacitación de los actores de justicia para su tratamiento, lo que puede dejar de lado la posibilidad de fortalecimiento de la administración de justicia y su fiabilidad.

1.2 Justificación

El problema objeto de estudio en el presente trabajo de investigación se relaciona con la insuficiente delimitación de lineamientos dentro del marco normativo vigente, así como la inexistencia o escasa estandarización de protocolos técnicos y jurídicos orientados a la

preservación, tratamiento y valoración de la evidencia digital en el contexto del proceso penal ecuatoriano. A esta problemática se suma la limitada capacitación y especialización de los operadores del sistema de justicia en el manejo adecuado de este tipo de elementos probatorios, situación que puede incidir de manera directa en la eficacia de su incorporación y valoración dentro del proceso. En consecuencia, estas deficiencias pueden obstaculizar el fortalecimiento de la administración de justicia y comprometer los niveles de confiabilidad y seguridad jurídica que deben caracterizar al sistema judicial.

Por lo tanto, el proyecto tiene fiabilidad teórica porque es posible analizar la normativa legal nacional e internacional sobre la aplicación de las tecnologías de la información y comunicación dentro de los procesos penales como elementos probatorios, además también incluye un aspecto práctico, en virtud a que articula la responsabilidad de los administradores de justicia acerca de la necesidad de estudiar la evidencia digital con prolijidad y capacitación previa, considerando que es indispensable el manejo adecuado de la evidencia digital, para ofertar un sistema jurídico efectivo, evitando la impunidad en delitos comunes y también en los ciberdelitos.

Así también en el ámbito metodológico la investigación es favorable, debido a que, además de identificar doctrina y jurisprudencia sobre el tema de la evidencia digital como medio probatorio también se incluye una indagación de fuentes primarias recopilando datos de los operadores de justicia sobre su percepción acerca de cómo se ejecuta actualmente el tratamiento de la evidencia digital. Adicionalmente, se ha tomado en cuenta elementos prácticos referentes al ejercicio del derecho con relación al tratamiento de la evidencia digital, datos que han sido recopilados por fiscales, peritos y abogados en libre ejercicio.

1.3 Objetivos

1.3.1 Objetivo general

- Analizar la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano para determinar las falencias normativas y técnicas que afectan su valoración probatoria, con el fin de establecer lineamientos orientados a mejorar su tratamiento y fortalecer la administración de justicia.

1.3.2 Específicos

- Examinar el marco normativo ecuatoriano vigente respecto a la obtención, conservación y valoración de la evidencia digital dentro del proceso penal.
- Identificar las principales dificultades técnicas y jurídicas que enfrentan los operadores de justicia en el manejo de evidencia digital, especialmente en casos de delitos comunes y delitos cibernéticos.
- Evaluar lineamientos normativos nacionales e internacionales prácticos que garanticen la autenticidad, fiabilidad y validez de la evidencia digital en el proceso penal

ecuatoriano, contribuyendo a una justicia penal más eficaz y acorde con los desafíos tecnológicos actuales.

CAPÍTULO II. MARCO TEÓRICO

2.1 Estado del arte

Dr. César Eugenio Navas Abad, acompañado del Dr. David Sebastián Vázquez Martínez, dentro de su artículo científico, para la revista científica Polo del Conocimiento en el año 2025, denominado "La importancia de la prueba digital en los procedimientos penales en Ecuador", manifiesta que:

La prueba electrónica se ha consolidado como un mecanismo sustancial del derecho procesal contemporáneo, debido al uso tan progresivo y generalizado de las tecnologías digitales en las relaciones sociales y jurídicas. En un entorno impregnado por la interconexión y la digitalización homogénea entre el ser humano y el mundo tecnológico han hecho que la evidencia que reposa en los distintos medios digitales permita reconstruir de manera objetiva y precisa los hechos relevantes que son materia sustancial para la resolución eficiente de controversias jurídicas. El empleo de mensajes electrónicos, correos digitales, contenidos de redes sociales y registros audiovisuales provenientes de sistemas electrónicos se han vuelto recurrente en los procesos judiciales, hasta tal punto que la doctrina considera que es prácticamente imposible concebir un procedimiento judicial actual sin la intervención directa de algún tipo de prueba digital, lo que conlleva su creciente importancia y los desafíos que plantea para el sistema de justicia. (Navas & Vázquez, 2025, p. 1748)

Dr. Fernando Mauricio De la Torre Muñoz; Dr. Alejandro Xavier Puertas Realpe; Dr. Christian Eduardo Burbano Peña, dentro de su artículo científico, para la revista Innovación & Saber en el año 2024, denominado "Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador", manifiesta que:

Todo elemento físico, biológico o electrónico identificado y descrito en una escena del crimen constituye principalmente un indicio que, tras ser debidamente localizado, fijado, levantado, rotulado y sellado, puede transformarse en evidencia con valor probatorio dentro de un proceso judicial para llegar a esclarecer los hechos objeto de controversia. En Ecuador, la evidencia digital distingue a cualquier objeto o dato extraído de un sistema informático, por lo tanto, se considera a aquellos elementos como la materia prima del proceso investigativo, en el que la tecnología se convierte en el epicentro fundamental tanto para la extracción y preservación de la información digital. Sin embargo, esta clase de evidencia presenta rasgos particulares como su volatilidad, posibilidad de anonimato, facilidad de duplicidad, alteración o deterioro que dificultan en gran medida su tratamiento técnico y jurídico. En este sentido, Ecuador batalla constantemente con el desafío de adoptar estándares y modelos internacionales que garanticen la correcta identificación, recolección y preservación de la evidencia digital, destacando la aplicación de la norma ISO/IEC 27037:2012 como un referente sustancial para asegurar su valor probatorio dentro del proceso penal. (DE la Torre Muñoz, Puertas Realpe, & Burbano Peña, 2024, p. 44-45)

Dr. Mauricio Jovanny Molina Troya, dentro de su trabajo de titulación para la obtención del grado de magister en derecho procesal, para la Universidad Católica de Santiago de Guayaquil, en el año 2021, denominado "Las tecnologías de la información y comunicación y la prueba en el proceso penal del Ecuador", manifiesta que:

De conformidad con el numeral 4 del artículo 76 de la Constitución de la República del Ecuador, se entiende que toda prueba obtenida e incorporada a cualquier proceso judicial con inobservancia de las normas legales carece de total validez jurídica y debe ser excluida. Este principio garantiza que la actividad de los medios probatorios obtenidos de manera ilícita, así como de aquellos procedentes de dichas actuaciones, tal como lo establece la doctrina referente al "fruto del árbol envenenado". En este sentido, el uso de las tecnologías de la información y comunicación en la investigación penal solo adquiere eficacia probatoria cuando su aplicación respeta las directrices del Código Orgánico Integral Penal y asegura la integridad sustancial y la autenticidad de los medios electrónicos de la evidencia digital. (Molina, 2021, p. 48-49-50)

Dr. Segundo Medardo Herrera Zapata, dentro de su trabajo de investigación para la obtención de su maestría en Derecho Penal, con la Universidad Andina Simón Bolívar, en el año 2025, denominada "El papel de la prueba digital en los procedimientos penales en Ecuador", manifiesta que:

El Código Orgánico Integral Penal establece un marco normativo para la aplicación de la cadena de custodia, comprendiendo tanto los elementos materiales como los contenidos digitales incorporados como medios de prueba en el proceso penal. Esta herramienta judicial tiene por concepto de finalidad asegurar la autenticidad e integridad de los elementos probatorios tanto materiales como digitales, mediante la identificación inequívoca de la evidencia y la conservación de sus condiciones originales a lo largo de todas las etapas procesales, que van desde su obtención hasta su análisis y resguardo. El correcto manejo de la cadena de custodia exige un registro riguroso y continuo de cada actuación realizada sobre la evidencia, incluyendo el traslado, la manipulación y cualquier intervención técnica, así como la individualización de los responsables en cada fase, a fin de garantizar su validez probatoria y evitar cuestionamientos en sede judicial. De tal manera, que, si en alguna de estas fases la evidencia digital es manipulada o trasladada de manera incorrecta la cadena de custodia de mencionada prueba digital carecería totalmente de validez jurídica dentro de la sustanciación de un proceso judicial. (Herrera, 2025, p. 43)

Dra. Arleth Fergie Álvarez Chica, dentro de su trabajo de titulación previo a la obtención del grado académico en magister en Derecho Penal, para la Universidad Estatal Península de Santa Elena en el año 2025, denominado "Desafíos de la prueba digital en el proceso penal", manifiesta que:

La incorporación de la evidencia digital en el sistema de justicia penal ha situado a la autenticidad e integridad como ejes problemáticos centrales, dado que, resulta indispensable

demostrar que la información no ha sido vulnerada, alterada o manipulada. Dentro del contexto tecnológico donde archivos digitales como imágenes, audios, videos y documentos pueden modificarse con facilidad, la fiabilidad probatoria depende de la acreditación de su origen, autoría y conservación integra desde su creación, siendo este un aspecto fundamental en toda prueba. Esta controversia se agudiza en Ecuador, debido a la falta de normas técnicas específicas que regulen el manejo y aspectos como la gestión de metadatos, los formatos admisibles, la validez de firmas digitales y los requisitos mínimos que debe cumplir la evidencia digital para ser considerada autentica y jurídicamente valida. (Álvarez, 2025, p. 3)

2.2 Marco teórico

UNIDAD I: Fundamentos jurídicos y normativos de la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano

- **Marco constitucional y legal de la evidencia digital en Ecuador.**

En el Ecuador la existencia de un marco legal referente a la evidencia digital es muy escaso, pese al fomento constante de delitos por medios informáticos, tomando en cuenta que su avance ha sido un tanto lento en cuanto a reconocer y regular estas pruebas, en relación a su admisibilidad, valoración y practicidad. Sin embargo, de aquello resulta esencial abordar con primicia ciertos aspectos conceptuales y doctrinarios esgrimidos del ámbito probatorio.

En este sentido, es preciso examinar, en primera instancia, el significado jurídico de la prueba, la cual es la base primordial de todo proceso judicial, debido al objetivo que persigue el cual es acreditar la existencia o inexistencia de los hechos relevantes dentro del proceso; así como también abordar la tipología y medios probatorios que sirven como armas o herramientas en el ámbito jurídico.

- **La prueba**

Dentro del ámbito probatorio, la prueba es entendido como aquel mecanismo utilizado por las partes intervinientes dentro de un proceso judicial en la que buscan evidenciar o acreditar un hecho persuadiendo al juzgador respecto a las afirmaciones dichas por ellos mismos. A su vez, Echandía, acertadamente ha manifestado que la prueba es de carácter instrumental y el objetivo es eminentemente ineludible, debido a que, busca generar convicción racional en la autoridad jurisdiccional. (Echandia, 2012).

En concordancia a lo anterior Cabanellas, (1993), define de manera textual lo siguiente: *"PRUEBA. Demostración de la verdad de una afirmación, de la existencia de una cosa o de la realidad de un hecho. Cabal refutación de una falsedad. Comprobación. Persuasión o convencimiento que se origina en otro, y especialmente en el juez o en quien haya de resolver sobre lo dudoso o discutido."* (Cabanellas de Torres, 1993).

Por su parte, Luna & Toro, (2022), manifiestan que para Taruffo; *"en términos generales, se puede entender por prueba cualquier instrumento, método, persona, cosa o circunstancia que pueda suministrar información útil para resolver incertidumbres del proceso"*. Por lo tanto, se puede colegir que la prueba constituye un elemento base para la determinación de hechos facticos, siendo el engranaje que sirve para determinar la reconstrucción lógica y cronológica de la verdad. Además, la prueba no solamente debe ser concebida como un mero formalismo procesal, sino como aquel medio direccionado a alcanzar la verdad procesal a través de criterios objetivos y racionales.

- **Medios de Prueba**

Los medios de prueba son todos aquellos componentes que puedan ser utilizados para determinar la veracidad de los hechos concretos, relevantes y objetivos que sustentan la teoría del caso. (Taruffo, 2008).

En concordancia con lo anterior, el (Código Orgánico General de Procesos, 2018), ha establecido los siguientes medios probatorios:

- *Art. 174 y siguientes. – Prueba testimonial. Es la declaración que rinde una de las partes o un tercero.*
- *Art. 193 y siguientes. – Prueba documental. Es todo documento público o privado que recoja, contenga o represente algún hecho o declare, constituya o incorpore un derecho.*
- *Art. 221 y siguientes. – Prueba pericial. Perito. Es la persona natural o jurídica que por razones de sus conocimientos científicos, técnicos, artísticos o profesionales está en condiciones de informar al juzgador sobre algún hecho o circunstancia relacionado con la materia de la controversia.*
- *Art. 228 y siguientes. – Inspección judicial. La o el juzgador cuando lo considere conveniente o necesario para la verificación o esclarecimiento del hecho o materia del proceso, podrá de oficio o a petición de parte, examinar directamente lugares, cosas o documentos.*

Con relación a lo anterior se puede colegir que los medios de prueba son aquellos instrumentos o caminos legales que sirven a las partes para lograr esclarecer sus hechos. Por lo tanto, son fuentes de información que producen convicción en el juzgador, ya sean estos hechos veraces o falsos.

- **Tipos de Prueba**

Los tipos de prueba son mecanismos que constituyen la categorización conceptual, doctrinal y normativa que el derecho concede a los datos e informes probatorios según su origen o dicho en otras palabras la relación que tiene con hecho materia de litigio en la circunstancia de su producción, es decir en la forma que el juzgador logra percibir.

De tal manera, que existe una brecha sumamente extensa cuando nos referimos a los medios de prueba y los tipos de prueba, debido a que, los tipos de prueba vienen a determinar la naturaleza de la información, mientras que los medios probatorios mecanizan la información dentro de los procesos judiciales.

Con base en lo anterior, De Miranda Vázquez, (2015), ha manifestado lo siguiente: *"prueba directa a aquella en la que el juzgador entra en contacto personal y directo con dicha realidad de contraste. Mientras que en el caso de la prueba indirecta no se produce tal contacto personal y directo, sino que alguien —una persona— o una cosa —un instrumento o un hecho— se interponen entre el juzgador y el factumprobandum."*

Por consiguiente, la prueba directa responde a la acreditación inmediata de un hecho, sin la necesidad de la intervención de una tercera persona, mientras que la prueba indirecta o

indiciaria requiere de un razonamiento lógico a través del cual el operador de justicia analiza la existencia de un hecho principal en base a la demostración de hechos secundarios para inferir.

- **Código Orgánico Integral Penal (COIP)**

En artículo 616 se exponen las reglas acerca de la exhibición de contenidos digitales donde se definen los lineamientos clave para la evidencia digital en el contexto del Derecho Penal:

Se habla del contenido digital que debe guardarse en cualquier medio óptico o en sistemas de almacenamiento como memorias extras, discos y más, por otra parte, se indica que este se reproduce bajo su formato original en cualquier instrumento tecnológico según sea factible, sin antes primero ejecutarse la acreditación de la persona autorizada por medio del perito, quien articulará bajo la cadena de custodia, integridad, autenticidad, en cuanto al uso de técnicas forenses digitales (Código Orgánico Integral Penal, 2014). A su vez, en cuanto al contenido de estos medios se los hará bajo la Asistencia Penal de Tipo Internacional la cual inicia en el Centro de Acopio del Sistema Nacional de Investigación Integral, Medicina Legal y Ciencias Forenses, garantizando la cadena de custodia.

Agregando a lo anterior, en el mismo cuerpo normativo, en el artículo 475 detalla las disposiciones para la retención de correspondencia, donde se da el reconocimiento sobre la inviolabilidad de los medios electrónicos, así como se observa la necesidad de retenerlos, abrirlos y examinarlos con previa autorización motivada de forma judicial, entonces se definen reglas para la manipulación de las mismas involucrando a los peritos para identificar claves o traducciones.

El artículo 476 trata sobre la orden para la interceptación de comunicación y datos digitales, siendo posible regular esta situación en cuanto a los dispositivos móviles, correos, redes sociales y más instrumentos, cuando existe su correspondiente orden judicial, bajo normativas relevantes y proporcionales, más queda prohibida la interceptación de comunicación cuando se protegen por secreto o sigilo profesional o por religión, y se requiere eliminar la información no importante, así también el recurso de almacenamiento se debe conservar por el fiscal en un centro de acopio técnico.

- **Código Orgánico General de Procesos (COGEP)**

En el Ecuador, la inclusión de pruebas digitales está contenida en el COGEP (2018) dentro del artículo 117 en donde describe lo siguiente:

> *"Documentos digitalizados. A las peticiones y demás actos de impulso procesal que se realicen por medio electrónico se acompañarán digitalizados o escaneados documentos de diversa procedencia, estructura y formatos, textos, sonido e imágenes. Los documentos cuya digitalización sea inviable por su gran volumen o por su ilegibilidad deberán ser presentados físicamente en la unidad judicial a más tardar el día siguiente del envío de la petición electrónica".* (COGEP, 2015, Art, 117).

Adicionalmente, en el artículo 193 trata sobre la prueba documental, afirmando que al tratarse de documentación electrónica o no material, no necesita su materialización, mientras

que, el artículo 196 del mismo cuerpo normativo, detalla sobre la producción de la prueba documental en la audiencia, y ratifica que para producir documentos electrónicos la exhibición se ejecuta por medios idóneos, sin que requiera su materialización, así también se afirma que, las fotos, grabaciones, elementos audiovisuales, computadores y otros de tipo electrónico están aptos para producirse por cualquier medio para la percepción, así también los documentos electrónicos deberán tener su soporte tecnológico concreto e idóneo (COGEP, 2015).

Según el artículo 202 del COGEP (2015), se mencionan los documentos digitales, y se definen que estos son aquellos que se producen de forma electrónica con sus correspondientes anexos para los fines legales para los cuales se proceda, así también la reproducción digital de ellos sea públicos o privados y también el expediente electrónico tienen la misma fuerza probatoria inicial. Considerando que, los documentos que siendo originales se escanean deben conservarse en audiencia si así lo solicitan las autoridades, así también se admite como medio de prueba cualquier contenido digital según el Código en mención.

Al observar los artículos antes mencionados del COGEP estos se asocian con la inclusión de documentación digital y su utilización como medios de prueba dentro del proceso judicial en el Ecuador, lo que también constituye un avance crucial rumbo a la modernidad del proceso penal, así también se observa que los documentos digitalizados como imágenes, audios, videos y más tienen la misma validez legal que aquellos documentos originales cuando se adaptan a los requisitos solicitados.

- **Código Orgánico Administrativo (COA)**

Según el COA (2017), el artículo 146 de dicho marco normativo define al expediente electrónico, como aquellas reproducciones digitales o bajo escaneo de documentación pública o privada, que se agrega al expediente electrónico y dispone de la misma fuerza probatoria que el original, tomando en cuenta que, expediente electrónico se debe proteger por medio del uso de sistemas de seguridad en un instrumento que de garantía del cuidado e integridad con que se manipulan los datos.

- **Ley de Comercio Electrónico, Firmas y Mensajes de Datos**

En este marco normativo, según el artículo 52 se detalla los medios de prueba donde se describe que los mensajes de datos, firmas electrónicas, documentación electrónica y certificados nacionales o extranjeros que se emiten según esta disposición se consideran medios probatorios, de forma independiente a su procedencia, para su valor y efecto legal, se observa lo establecido en el Código Orgánico General de Procesos (COGEP) (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2021)

Dentro del artículo 53 y 54 por su parte se define lo siguiente:

Artículo 53, cuando se disponga de la firma electrónica certificada como medio de prueba por parte de una institución de certificación acreditada, se observa que se reúnan los requisitos indispensables que determina la Ley, y también la firma electrónica no puede ser alterada desde la emisión de la misma y debe verificarse su pertenencia al signatario (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2023)

Dentro del artículo 54, se trata sobre la práctica de la prueba, donde se emiten las regulaciones sobre la práctica para el caso de la prueba digital, pues se incluye un mensaje de datos dentro del proceso judicial, y a su vez debe ir adjunto el soporte de la información y la transcripción en papel electrónico, además de los mecanismos de verificación si se solicita (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2021).

Adicionalmente, las normativas anteriores a nivel local se respaldan en los siguientes instrumentos internacionales en cuanto a prueba o evidencia digital en los procesos judiciales:

- **Convenio de Budapest acerca de cibercriminalidad**

Este marco legal internacional se subdivide en tres ejes clave que son los descritos por el Consejo de Europa (2001):

1. Delitos informáticos, descritos y clasificados en categorías, los cuales tienen con propósito el uso de la tecnología que son aquellos que disponen de la tecnología como medio, los delitos asociados con contenido y los que se asocian con infracciones a la propiedad intelectual
2. Normas procesales, donde los procesos permiten el respaldo de la evidencia digital, además que otorga los lineamientos que tienen que ver con la manipulación de esta información.
3. Normas de cooperación internacional, que son lineamientos que se articulan en delitos informáticos o tradicionales donde se destaca el uso de evidencia científica e involucran disposiciones sobre la localización de sospechosos, envío de esta evidencia y su extradición.

Es así que, este Convenido define herramientas procesales adecuadas para la evidencia digital como son la conversación veloz de datos informáticos, la conversación rápida de datos asociados con el tráfico, orden, presentación, registro e incautación de datos informáticos almacenados, así como se detectan los datos asociados al contenido y tráfico.

En definitiva, el Convenio de Budapest es uno de los principales referentes que se asocia para que los Estados miembro articulen aspectos sobre derecho procesal digital, y en materia penal, debido a que esto incluye la recopilación de evidencia digital frente a delitos informáticos.

- **Norma ISO/IEC 27037:2012**

La norma ISO/IEC 27037:2012, es una normativa internacional que brinda direccionamiento en cuanto al tratamiento oportuno en el inicio del proceso de la evidencia digital, en una investigación forense o la causa de procesos judiciales concretos. Por lo tanto, de acuerdo a esta norma la evidencia digital se considera a cualquier medio de valor probatorio que se almacena en formato digital y se obtiene de computadoras, teléfonos móviles, servidores, cámaras, DVR, IoT, redes en la nube, dispositivos USB, etc. (ISO/IEC 27037, 2012)

Esta norma se aplica en el sistema de encendido, apagado, evidencia volátil como RAM o procesos activos, así como los mecanismos de almacenamiento de información internos o externos. En cuanto a la recopilación de información según esta norma se requiere el seguro

físico de la evidencia a partir de su etiquetado, registro de fotos, utilización de bolsas antiestáticas, aislamiento de redes como modo avión o jaula Faraday (ISO/IEC 27037, 2012).

Por otro lado, para preservar esta evidencia digital se debe procurar que no sea alterada, además que se encuentre íntegra hasta que se genere el juicio, mantener una cadena de custodia efectiva, un almacenamiento confiable y el control de acceso a la misma.

- **Deberes y actuaciones procesales de los operadores de justicia ante la evidencia digital.**

Los operadores de justicia deben tener clara su actuación en cuanto a la recopilación, manipulación y ejecutoria de la evidencia digital. El uso continuo de las tecnologías de la información, ha transformado a la evidencia digital en un elemento probatorio base de los procesos judiciales, y ante esto los jueces, fiscales, peritos, deben actuar según sus competencias y de acuerdo a los principios de legalidad, integridad y autenticidad que competen a tal evidencia.

- ***Cumplimiento de legalidad y respeto al debido proceso.-*** Los operadores de justicia deben garantizar el hallazgo y la evaluación de la evidencia digital de tal forma que se asocie a lo establecido en el marco legal y Constitucional vigente, siempre y cuando se respeten los derechos como la intimidad, protección de datos personales y la defensa, donde se insta a que cualquier tipo de irregularidad que suceda en la cadena de custodia o en los procesos técnicos puedan dar como resultado la exclusión probatoria (Carbonell, 2021)
- ***Preservación de la evidencia científica. -*** Una de las tareas principales es dar seguridad a la preservación de la integridad de la evidencia digital, de tal forma que se evite la alteración de la misma, por cuanto, según lo establecido por la norma ISO /IEC 27037:2012 define qué; las normativas para identificar, recopilar, adquirir y preservar la evidencia digital, deben ser analizadas integralmente por los operadores de justicia y peritos. De tal forma que en el caso de incumplir no se podría tomar la evidencia con valor probatorio, influyendo en el proceso que se está ventilando.
- ***Documentar y articular la cadena de custodia. -*** Los operadores de justicia tienen el deber de dar garantía de que se trata de documentación continua, en cada actuación de la evidencia digital, lo que involucra aspectos tales como la identidad del dispositivo, los métodos usados para su extracción, instrumentos forenses usados, que se asociaron con la evidencia. Por otra parte, la cadena de custodia representa un aspecto clave que demuestra que la evidencia digital que se presenta en el juicio es la misma que se recopiló al inicio y no se la ha manipulado (Casey, 2020)
- ***Competencia técnica y apoyo pericial. -*** Debido a que la evidencia digital requiere un trato exclusivo, los operadores de justicia deben apoyar a los peritos especializados, y deben estar al tanto de los principios técnicos que la representan, así también el juez tiene la necesidad de valorar la prueba digital usando el principio de razonabilidad, así el fiscal y la defensa pueden tener un control de los informes periciales (Velasco & Álvarez, 2022).
- ***Actuación procesal en la valoración de la evidencia digital, en la etapa de juzgamiento. -*** El juez es quien analiza la evidencia, y verifica su autenticidad, fiabilidad y pertinencia, para lo cual debe aplicar el principio de la sana crítica del juez, a tal efecto se recomienda una valoración que asocie aspectos tanto jurídicos como técnicos (Consejo de Europa, 2001).

A continuación, se exponen los principales actores involucrados en el tratamiento de la evidencia digital:

- **Primer interviniente o first responder**

El primer interviniente o *first responder* es aquella primera persona que evidenció el hecho, que se encuentran o no dentro del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, y en sus funciones hayan ingresado en contacto con los indicios que se relacionan en un hecho delictivo, y pueden actuar bajo la figura de primer actor o persona privada que ha sido testigo de la escena del delito, en donde se debe observar la existencia de indicios físicos o virtuales, que pueden contener la evidencia digital, de tal forma que el responsable debe asegurarse de preservar, proteger, informar la presencia del personal especializado en procesar la escena y el personal necesario para la investigación legal.

- **Interventor**

Los interventores directos representan aquellos servidores que pertenecen de forma directa al Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, quienes de acuerdo a sus competencias propias deben responsabilizarse por la ejecución de actividades de búsqueda, y recopilación de indicios físicos y electrónicos que pueden ser parte de la evidencia digital, tomando en cuenta que, estas actividades no incluyen para estos actores el tratamiento de la información, pero si se deben encargar de analizar las condiciones para que la evidencia pase a otro especialista de acuerdo al tipo de indicio hallado.

- **Primer responsable de la Evidencia Digital (DEFR)**

Son aquellos servidores que forman parte del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, que, en cuanto a sus competencias y formación académica, se responsabilizan en identificar, recopilar, preservar y tomar nota de la evidencia digital en la escena del crimen. Además de aquello, tienen la obligación de evitar toda alteración que podría influir en la validez del proceso penal.

- **Especialista en Evidencia Digital (DES)**

Constituye el profesional que se especializa según su formación y experiencia en dar sus conocimientos técnicos para el análisis e interpretación, por otra parte, también brinda el valor necesario a las conclusiones del tratamiento de evidencia digital, además se observan las disposiciones clave para el cumplimiento del Sistema Pericial Integral de la Función Judicial (Balla, Granja, & Freire, 2024).

Una vez localizados los actores involucrados, se procede a ejecutar las acciones que de acuerdo al nivel de gestión es posible tratar la evidencia digital, cumpliendo con las siguientes etapas, según Echeverría et al., (2024):

Primera Etapa. - Intervención directa en la escena del crimen. – En cuanto a la etapa de intervención inicial se realiza la identificación de los mecanismos electrónicos indispensables, además, que se debe documentar su diagnóstico inicial, sin manipular o alterar el mismo, así

también se debe realizar la intervención en la escena del delito sea en caso de delito flagrante o por disposición de la autoridad judicial, las acciones que se deben ejecutar involucra el proteger la escena, identificar indicios, inclusión de los indicios en el centro de acopio y si se requiere disponer de asistencia técnica especializada. Adicionalmente, se debe tomar en consideración que, la recopilación, preservación y tratamiento de los medios digitales y su información contenida en la escena se debe ejecutar en los casos a continuación mencionados:

1. *En un primer escenario.* - Se deben activar los protocolos por el Servicio Integrado de Seguridad ECU 911 del motivo de que existe un posible delito en el que involucra la recopilación, procesamiento y tratamiento de la evidencia digital.
2. *En un segundo escenario.* - El operador de justicia dispone o notifica la necesidad de búsqueda, registro y accesibilidad de información digital y en casos necesarios la incautación de los indicios tecnológicos recopilados.

En ambos casos los servidores del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, conforme a sus competencias, deben ir a la escena, es decir al sitio donde se dieron los hechos o llamado ‘’territorio digital’’ en donde deben procesar los mecanismos materiales probatorios, así como la transferencia de la escena o si hay indicios informáticos según la norma legal que se encuentren en vigencia y bajo la Cadena de Custodia para lo cual se llena el formulario único.

A su vez, tanto el primer interviniente (first responder) y el interventor tienen las siguientes funciones concretas dentro de la escena del delito:

a) Valoración del sitio. - En donde se suscitaron los hechos se debe evaluar el entorno, aspectos clave para aplicar las técnicas de protección de la escena con los medios necesarios para hacerlo, para esto deben usar el equipo de protección básico requerido, y no deben realizar ningún tipo de manipulación de los indicios, tampoco deben contaminar la escena o realizar actos que vulneren la integridad de los elementos probatorios.

Así mismo, deben realizar la correspondiente limitación del acceso al sitio del incidente de tal forma que se evite alteraciones de la evidencia digital, así también se debe recorrer los perímetros del sitio, con el fin de verificar sitios conexos o indicios, y además deben verificar los riesgos iniciales, por ejemplo, si necesita apoyo para neutralización de riesgos eléctricos, electromagnéticos y otros como la incorporación de aparatos explosivos.

b) Identificación. – Se debe identificar los indicios según el tipo de delito, se definen los dispositivos electrónicos o aquellos mecanismos que se encuentren como parte de la evidencia digital, que estén dentro de la necesidad de indagación según lo determinado en la clasificación por tipo y contenido de dispositivos electrónicos.

c) Ingreso de indicios dentro del centro de acopio. - Cuando se gestionan los dispositivos electrónicos o aquellos que involucra la evidencia digital y si no se necesita personal técnico para hacerlo se realiza el correspondiente Parte Policial, que dispone la narración de la escena y su foto, también se incluye la ubicación en la cual están los equipos, dispositivos y el resto de elementos a ser incautados, además del formulario único de la cadena de custodia.

d) **Solicitud de un interventor. -** Si se necesita que se encuentre en el sitio un profesional técnico se debe coordinar con las unidades que se encuentren adaptadas al procesamiento del sitio de la intervención

Segunda Etapa. - Procesamiento de la escena.- Luego de detallar la tipología del delito se ejecuta el correspondiente procesamiento del sitio de la escena, con uso de la metodología IOT en el sitio de los hechos, lo cual incluye el aseguramiento de los indicios y su ingreso en el centro de acopio, de igual manera si se necesita de personal técnico, es necesario solicitar al Primer Responsable de Evidencia Digital (DEFR) bajo quien se usa la metodología en mención de tal manera que se garantice la integridad de la evidencia.

A lo anterior hay que destacar que, la secuencia técnica para recopilar los indicios y verificar los elementos materiales probatorios de tipo lofoscópico y no lofoscópico, requiere la ayuda del perito en IOT quien debe aplicar el procedimiento con uso de reactivos y toma de muestras menos invasivas para no afectar al dispositivo que se analiza.

Si se observa la pertinencia, el perito de Inspección Ocular Técnica, tiene que pedir que le acompañe el Primer Responsable de Evidencia Digital (DEFR), para la preservación de la evidencia digital, además, no es necesaria la manipulación que no se requiere salvo cuando se necesiten datos volátiles.

Tercera Etapa. - Procesamiento de evidencia digital en laboratorio. - En cuanto a esta etapa, se observa la necesidad de practicar los principios para la gestión de evidencia digital, que son los siguientes:

- **Relevancia:** Donde la evidencia digital debe estar asociada con los hechos investigados, se hace importante para probar o no un elemento concreto
- **Veracidad:** La evidencia digital es un medio auténtico, confiable e íntegro que no ha sido manipulado ni alterado.
- **Suficiencia:** Se refiere a la cantidad y calidad de la evidencia digital, donde la suficiencia verifica que la información se recopile en relación al sustento del análisis forense según el objeto de la investigación.
- **Integridad:** La forma de uso de los indicios digitales no deben dar como resultado alteraciones que pueden reducir la validez o admisibilidad probatoria, pues la integridad debe implicar que la evidencia digital se encuentre completa, exacta y confiable en todas y cada una de las etapas del proceso forense donde se garantice su autenticidad y valor probatorio.
- **Auditabilidad:** Es aquella cualidad que ayuda a la trazabilidad en las etapas de obtención, preservación, análisis de la evidencia digital, involucra que existe registros documentados de cada accionar, lo que genera una evaluación del procedimiento ejecutado.
- **Disponibilidad:** Compete a la garantía en cuanto a la accesibilidad autorizada de la información que se obtuvo anteriormente, y se almacena en repositorio digital
- **Legalidad:** La manipulación de la evidencia digital involucra que se cumpla los altos estándares forenses en el cuerpo normativo legal vigente, lo que a su vez da la garantía de seguridad de la información cumpliendo con otros principios como la confidencialidad, integridad, disponibilidad.

A continuación, en la Tabla 1 se expone la clasificación por tipo y contenido que se pueden dar a los dispositivos electrónicos para considerarlos como parte de la evidencia digital, tomando en cuenta que su observación, búsqueda, localización, reconocimiento, pueden incluir categorías en cuanto a los dispositivos electrónicos, o las fuentes de evidencia digital y registros físicos como es el caso de contraseñas, usuarios y demás.

Tabla 1. *Clasificación por tipo y contenido de dispositivo electrónico*

CATEGORÍA	TIPO DE DISPOSITIVO	CONTENIDO
Sistemas informáticos	Computador de escritorio	Datos de archivos multimedia, cuentas de usuario, bases de datos, configuración, registros del sistema operativo, licencias de software y otros
	Computador portátil	
	Servidores físicos o virtuales	
	Sistema de video vigilancia	
	Sistemas automotrices	
	Consolas de videojuego	
	Cámara	
	Impresoras	
	Rig para minerías	
Dispositivos de almacenamiento	Discos duros externos	Ofimáticos como archivos multimedia, datos ocultos, volumen, número de serie, metadatos
	USB	
	Memoria externa	
	Dispositivos ópticos	
	Grabadora digital	
	Sistema de respaldo o reproducción multimedia	
Dispositivos telemáticos	Enrutador	Tablas de enrutamiento, configuración de protocolos de comunicación, red, registros y otros
	Conmutador	
	Módems	
	Equipos de seguridad	
	Telefonía satelital	
	Radio digital	
Dispositivos móviles	Smartphone	Registro de llamadas, mensajes, servicio de mensajería, redes sociales, correo electrónico, firma electrónica, respaldos de APP y otros
	Tablets	
	Dispositivos y consolas de navegación no tripulada	
	Reloj inteligente	Redes sociales, sitio web, mensajería instantánea, almacenamiento de
	Software (SaaS)	

		información, datos, tráfico y contenidos
Sistema basado en la nube (cloud)	Plataformas (PaaS)	Trazabilidad de transacciones, de billetera digital, datos de ubicación, inter operatividad, entrenamiento, otros.
	Infraestructura como servicio (IaaS)	
	Nube de datos pública, privada, híbrida	
Tecnologías disruptivas	Realidad aumentada	
	Blockchain	
	Computadora cuántica	
	Big data	
	Equipos IOT (Internet de las cosas)	

Fuente: (Avemañay, Avemañay, & Duarte, 2025)

Los administradores justicia al verse inmersos dentro de la globalización electrónica en el sistema judicial deberían conocer de esta categorización de dispositivos y del tipo de contenido que pueden almacenar estos instrumentos.

- **Relación jurídica entre la autenticidad de la evidencia digital y la administración de justicia.**

La evidencia digital es un elemento base de los procesos judiciales modernos, debido a su utilización generalizada en aspectos de tecnología de la información y comunicación en ámbitos diversos como el social y también el procesal-penal. Es así, que, al hablar de la autenticidad de la evidencia digital representa un aspecto clave para dar garantía de una adecuada administración de justicia, porque de esta va a depender la validez probatoria y también la calidad del sistema judicial.

Por otra parte, desde un contexto jurídico y procesal, la autenticidad de la evidencia digital hace énfasis según Casey (2019) en aquella posibilidad de identificar que un dato electrónico es efectivo, íntegro y adaptable a las necesidades para valorarlo en un juicio. Esto a su vez, se asocia con los principios como el debido proceso, seguridad jurídica y tutela judicial efectiva, mismos que constituyen elementos indispensables a tratarse sobre todo en *"Estados de derecho*" como el Ecuador.

A su vez, la administración de justicia necesita que los operadores de justicia fundamenten su toma de decisión en pruebas que sean comprobables y fiables, por eso es que, la evidencia digital, garantiza tanto el cumplimiento de estándares jurídicos y técnicos que permiten dar fe de su autenticidad, entre ellos están: la adecuada cadena de custodia, la utilización de metodología forense amplia y efectiva, y la necesidad de verificar por las partes la información (ISO/IEC 27037, 2012). Sin embargo, cuando estos aspectos no se cumplen

podrían llegar a ser una prueba inadmisible o ilegítima, que puede incluso dar la correspondiente nulidad al proceso.

En el contexto jurídico la prueba se describe como aquel medio que ayuda al conocimiento de la veracidad de los hechos en un proceso judicial específico, de acuerdo a Bonnier (2023) la prueba es aquel instrumento que se origina de la urgencia por identificar e investigar aquellos elementos de un litigio, cuyo propósito es el respaldo de las versiones de las partes involucradas. Es así que, la Corte Nacional de Justicia del Ecuador, antepone la importancia suprema de la prueba, porque ratifica que es el elemento que permite ejecutar los actos procesales y extraprocesales. Por lo tanto, afirma que; sin la existencia de la prueba el juez no puede disponer de un fallo correcto de la cosa juzgada, lo que imposibilita completamente la administración de justicia. (Balla et al., 2024).

A su vez, la prueba representa un aspecto clave para prevenir conflictos posteriores en la decisión judicial, porque le da soporte adecuado a los hechos y a su vez según Gorphe (2023) da importancia a la declaración que debe respaldarse por los hechos materiales que se comprueban en un proceso. Así también dentro del Código Orgánico General de Procesos (COGEP) en el artículo 158 se define el objeto de la prueba, mismo que indica que esta ayuda al juez a llegar a una conclusión específica sobre lo que se debate.

Por otra parte, en torno a los medios de prueba, el COGEP indica diversos tipos de actores procesales, que son parte de la presentación de las evidencias, y también detalla la existencia de pruebas documentales (artículo 193), que indica que son las que se presenta en escrito, también se detallan las pruebas testimoniales (artículo 174) de este marco normativo, que indica que son los testimonios de los hechos de quienes indican haberlos presenciado. Así también están las pruebas periciales (artículo 227) que son aquellas que dan los especialistas en áreas técnicas, médicas y otras ciencias, que dan información importante y técnica que pueden aportar a la evidencia.

Sin embargo, en este marco normativo no se realiza el análisis directo de la evidencia digital, lo cual promueve un vacío en la norma desde un entorno donde las pruebas digitales son indispensables. Es así que, con la venida de la tecnología digital, la evidencia digital ha tomado importancia, aunque todavía no del todo en el marco normativo ecuatoriano, pues no se define concretamente sobre su uso, sin embargo, autores como Labadía (2019) detallan que el soporte de la prueba no se debe condicionar en función al tipo de almacenamiento, y puede considerarse un medio válido o admisible para probar los hechos que se alegan en un juicio, el problema es que por su característica efímera e intangible, la evidencia digital todavía es cuestionada en cuanto a temas de manipulación e integridad, lo que implica un análisis especializado que de fe de su autenticidad absoluta.

Entonces, al mencionar sobre la asociación entre la autenticidad de la evidencia digital frente a la administración de justicia se enfatiza en la capacidad de generar la carga de valoración probatoria por el actor de justicia, pero cuando hay una prueba física tradicional, la evidencia digital puede manipularse, duplicarse o eliminarse, y esto hace que los jueces deban acudir a peritos técnicos especializados para determinar la autenticidad, por eso es que, la justicia no

únicamente se enfoca en la administración y aplicación de normas jurídicas sino que involucra los conocimientos técnicos requeridos para la toma de decisiones razonables.

UNIDAD II: Factores técnicos, jurídicos y procedimentales que afectan la autenticidad y fiabilidad de la evidencia digital.

- **Identificación de los principales riesgos y vulnerabilidades de la evidencia digital.**

El rol de los Sistemas de la Información y Comunicación es indispensable, tomando en cuenta que estos también forman parte de riesgos que se vuelven cada vez más comunes como el crimen cibernético, el que constituye un desafío en cuanto a la evidencia digital, porque es susceptible a cambios o manipulaciones, por lo tanto, es necesario que se enfrente a este riesgo de forma adecuada. De acuerdo a Global Security Report se evidenciaron distintos compromisos, y métodos de ataques de incidentes, y se observó que los principales métodos de ataque de la vulneración de la evidencia digital tienen que ver con los siguientes delitos (Avemañay et al., 2025):

Entre los principales riesgos existentes en cuanto a la posibilidad de vulneración de la evidencia digital, se encuentran los siguientes aspectos dichos por Bella et al., (2024):

- Phishing
- Acceso remoto
- Trabajadores con malas intenciones
- Inyecciones de código
- Ausencia de la configuración
- Carga de archivos de forma inadecuada
- Malware

Se destaca entonces que por lo menos el 43% de información se pierde por manipulación de actores que se encuentran dentro del mismo entorno de labores, lo que ratifica que las empresas deben prepararse para la gestión de la seguridad (Coronel y Arguello, 2025), siendo este proceso indispensable, según lo afirma la norma ISO 27002:2013 con relación a la urgencia de tener procedimientos para manejar la evidencia digital.

- **Manipulación de los datos (ciberespacio)**

Cabe mencionar que, con la venida del ciberespacio se ha gestionado una transformación continua del entorno y con él se presenta la evolución de la manera en cómo vive la sociedad, lo que a su vez produce un cambio de paradigmas, que es lo que hoy se conoce como revolución digital, ya que no solo se trata de una revolución industrial, sino que el ciberespacio ha permitido formar el entorno social que rodea a los individuos que se verifica en las actividades cotidianas, pues además de ser un sitio que se adapta a las comunicaciones, para muchos representa el sitio de labores, e inversiones (Mendoza, 2024).

Adicionalmente, se considera al ciberespacio como un conocimiento de la persona para realizar funciones digitales, y transmitir en un hiperespacio, que se refiere al ámbito comunicacional y de información global, es por eso que, a medida que la tecnología mejora y la

participación de los ordenadores aumenta de manera competente, navegar por el camino del ciberespacio se ha vuelto la actividad principal de las personas, como por ejemplo: la descarga de información, la lectura, la escritura de diversos blogs, el recibir y enviar mensajes de correo electrónico, es lo esencial que las personas realizan a diario.

Por lo tanto, al hablar de ciberespacio es aquel entorno globalizado que forma parte de una red amplia de información, infraestructura y datos, así como redes de telecomunicación, sistemas y controladores integrados tomando en cuenta que ayudan a interconectar a las personas por medio del uso de dispositivos digitales, sin tomar en consideración el sitio físico (Jones, 2022).

Un usuario en medio de la tecnología digital tiene que hacer frente a una verdadera revolución que, en gran medida, permite a la gente cruzar las barreras de tiempo y espacio cuando quieren acceder a la información. Al mismo tiempo, proporciona completamente nuevas formas de entretenimiento, abre nuevas oportunidades de empleo, facilita y acelera significativamente muchas de nuestras actividades cotidianas. Para los investigadores, sin embargo, "el ciberespacio no es todavía un campo explorado a fondo, ya que está lleno de nuevos retos y problemas que no han encontrado antes."

Existen diversos tipos de intercambios de información los cuales son: a) relaciones de intercambio de información entre máquinas; b) relaciones de intercambio de información entre hombres y artefactos; y c) relaciones de intercambio de información entre seres humanos a través de los diferentes tipos aparatos electrónicos; los cuales no hay que tomarlos como separados, debido a que en la actualidad y sobre todo en el ciberespacio la comunicación se da directamente con las máquinas, ya que, son ellas las que operan para facilitar las comunicaciones interpersonales. En consecuencia, el ciberespacio constituye un espacio cibernético donde "los artefactos electrónicos constituyen una red, que sirve de instrumento para que se establezcan comunicaciones entre las personas y de forma simultánea para lograr entablar contacto con otras personas que se encuentran en varios puntos y con redes distintas."

Es así que, el ciberespacio representa el nuevo medio de comunicación, ya que se ha sustituido a los métodos más tradicionales al momento de comunicarse, como ejemplo se puede observar que a menudo se envía mensajes de correo electrónico en lugar de cartas y cada vez con más frecuencia las personas son capaces de leer textos en línea, revistas electrónicas, en lugar de leer un artículo en papel; haciendo que los objetos físicos de comunicación tradicionales como cartas, libros, etc., estén siendo reemplazados por nuevos objetos electrónicos.

Hay que destacar que, conforme pasa el tiempo y evoluciona la tecnología, esta ha dado paso a que se fortalezcan nuevas organizaciones, así como a generado ataques y amenazas nuevos, porque el ciberespacio se ha convertido en una posibilidad de actuación delincuencial, que se aprovecha para el robo de identidad, fraude de gobiernos, instituciones y personas, lo que vulnera las seguridades comunes de los Estados.

El mundo de hoy está más interconectado que nunca, sin embargo, con todas sus ventajas, el aumento de la conectividad trae un mayor riesgo de robo, fraude y abuso, es por eso que, mientras las personas se vuelven más dependientes de la

tecnología moderna, también se vuelven más vulnerables a los ataques cibernéticos. (Dulaney, 2011, págs. 445-446)

Los ciberataques tienen dos objetivos, uno es modificar las redes afectándolas para que no den un buen servicio, es decir, se da el llamado terrorismo informático a los Estados que controlan su información a través de un Gobierno electrónico; y el segundo objetivo se basa en el robo de datos a los ciudadanos. Al ser dos acciones distintas, el tema central que se aborda en este trabajo es la prevención de los ciberataques respecto al robo de datos de los ciudadanos, de los cuales el Estado es responsable.

Los ataques cibernéticos constituyen uno de los grandes retos del tiempo actual, debido a que es un tanto complejo establecer normativas que se instauren a nivel mundial para la transmisión de datos e información, para lo cual existe la oportunidad de garantizar un futuro pujante e innovador, pero también se corre el riesgo de que internet se utilice como fuerza negativa, por lo que la sociedad junto con las normativas adaptadas para la seguridad de información por parte del Estado e instituciones públicas que realizan el control y regulación de información, especialmente si se trata de aquella obtenida o registrada en la red, tenga como objetivo "preservar las grandes oportunidades que nos ofrece el desarrollo del ciberespacio". (Dulaney, 2011, pág. 448)

El ciberataque es un factor importante a tener en cuenta para protegerse de ataques maliciosos, sin adecuadas medidas de seguridad, a su vez, la tecnología informática podría obstaculizar a los usuarios en vez de ser una solución para ellos. Es importante tomar medidas de seguridad sobre todo en el ámbito estatal, debido a que es el Estado el responsable de un fichero o de una base de datos sensibles, por lo tanto, tiene el compromiso de precautelar los datos personales almacenados en sus ficheros, con la agravante de que estos son establecidos por ley, los cuales tienen tres niveles de seguridad: nivel alto (datos sensibles), nivel medio (datos comunes), nivel bajo (datos inocuos) (Jones, 2022).

El Estado debe garantizar la debida protección de datos personales, ya que es el principal órgano encargado del bienestar de las personas; es por eso que, para resguardar la seguridad nacional se necesita tomar ciertas medidas como: protección de información del sistema, reducir el robo de identidad, prevenir fraudes informáticos, impedir maliciosos ataques cibernéticos, evitar la violación de información confidencial y alteración de datos. Con los ataques cibernéticos en subida continua, las personas, instituciones y el Estado, tienen que entender y a su vez aprender diversas formas de prevenir estos ataques.

Los ciberataques pueden incluirse en varios contextos como, en la difusión de un código malicioso como virus, el robo de información personal, el uso de phishings y spams, etc., así también, los ataques cibernéticos pueden dar lugar a fraudes, robo de identidad, y muchos más delitos. Un importante concepto que cualquier usuario debe entender es que un ordenador conectado a Internet puede ser susceptible de ataques cibernéticos.

Los ataques en mención se envían por una red que pone en evidencia el peligro del destino de la información y de toda la red, siendo peligrosos por la capacidad de irse en contra de una víctima por la que los usuarios toman en consideración ciertos mecanismos que pone en

duda la forma de obtener información de tipo personal como el mantenimiento del software, sus instalaciones, antivirus, cifrado de datos de protección.

En el mundo cibernético existen los usuarios domésticos que son a menudo los más vulnerables y susceptibles a los ataques cibernéticos, debido a que este tipo de usuarios suelen ser los menos educados acerca de la seguridad cibernética, teniendo mucho más éxito dichos ataques cibernéticos al focalizarse en ellos y es por eso que estos usuarios se preguntan con frecuencia el significado de un ciberataque.

El usuario doméstico debe tomar las medidas necesarias para proteger su ordenador de los ataques cibernéticos, puesto que vivimos en una nueva era de la tecnología, en donde cada vez más información privada se almacena en computadoras y redes, las cuales son utilizadas todos los días para realizar diferentes tipos de actividades como: compras, envío de correos electrónicos, educación, entretenimiento, etc. "Educar a los usuarios domésticos no sólo aumentará la seguridad contra los ataques cibernéticos, sino también, permitirá el desarrollo de nuevas medidas de seguridad". (Tomás, 2015, p. 115).

El problema surge también debido a que las computadoras no vienen equipadas adecuadamente con suficiente software y antivirus que protejan de manera efectiva la información de los ataques cibernéticos. Es necesario a su vez que los usuarios domésticos estén capacitados y bien informados acerca de los tipos de amenazas que pueden existir lo que hace que los usuarios sean más vulnerables.

La guerra cibernética parece estar dominando los titulares en los últimos tiempos, ya se trate de grupos clandestinos de piratería, ordenadores para diversión o supuestas agencias gubernamentales que tratan de robar información clasificada.

- **MafiaBoy (año 2000):** Michael Calce alias MafiaBoy, causó daño en el ciberespacio, era sólo un estudiante de instituto canadiense cuando decidió dar rienda suelta a un ataque DDoS (Distributed Denial of Service, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos), en varios sitios web comerciales de alto perfil" como Amazon, CNN, eBay y Yahoo!. Un experto en la industria estima que los ataques dieron lugar a una cantidad de $ US1.2 millones de dólares". (Dulaney, 2011, pág. 12)
- **Google China fue golpeado por el ataque cibernético (año 2009):** Cuando las sedes chinas de Google detectaron una violación de seguridad a mediados de diciembre, de aquel año.

En este aspecto los hackers tenían diversos servidores empresariales de Google, siendo que su propiedad intelectual se vulneró, y en una nota o blog, Google aseguró tener pruebas donde se verificaba el objetivo de quienes realizaron esta situación, pues eran activistas de derechos humanos de China, se verificaron diverso Gmails enviados desde Estados Unidos, China y toda Europa, que se encontraban si permisos y los correos eran específicamente de los defensores de derechos humanos de China. (Aguirre, 2001, pág. 18).

- **Hacker roba decenas de millones de datos de la tarjeta de crédito (año 2009):**

Gonzales, un hacker de Miami, fue el responsable de uno de los casos de fraude más grande en la historia de los Estados Unidos. Gonzales fue responsable de "sellar decenas de

millones de números de tarjetas de crédito y tarjetas de débito de más de 250 instituciones financieras y había cortado la red de tarjetas de pago de grandes empresas como la cadena de tiendas de conveniencia 7-Eleven". (Vatis, 2001, p. 6-18)

Uno de los ataques más difundidos a nivel mundial es **el ataque a las Torres Gemelas en EE. UU el 11 de septiembre de 2001**, el cual alarmó no solo a la sociedad de Estados Unidos sino al mundo en general, motivo por el cual provocó una nueva urgencia para predecir futuras amenazas a los Estados Unidos y al mundo.

Es así, que en una época de crecimiento militar y de dependencia económica de la tecnología de información conectados por equipos en red, existe el temor de que algún día se pueda experimentar una situación como la del 11 de septiembre del 2001 a manos de terroristas, crimen organizado, piratería, o peor aún más devastador como un ataque sorpresa por otro país que pudiera eludir la identificación como autor gracias al camuflaje proporcionada por el ciberespacio.

En consecuencia, la rapidez con que se obtiene acceso a medios en línea, convergentes, móviles y en red no tiene precedentes en la historia de la innovación tecnológica. La investigación en ciberseguridad se centra principalmente en dos cuestiones: la protección de la información, tanto estratégica como económica, y la protección de las personas, debido a que el ciberespacio se lo está considerando como un lugar vulnerable a la perpetración de distintos ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual, hasta la integridad física y la vida. Aunque la mayoría de las conductas no son, en esencia, algo nuevo en sí mismas la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, confiere a estas conductas una especial configuración que obliga a romper los esquemas clásicos para su investigación y enjuiciamiento.

Por otra parte, si bien, la tecnología ha hecho que los usuarios accedan de forma fácil a servicios en línea incluyendo los financieros, es posible que los delincuentes se aprovechen de estas situaciones vulnerando las seguridades, lo que evidencia la fragilidad de las personas, tomando también en cuenta que la delincuencia virtual ha incrementado sobre todo en las últimas décadas, pues se define como un conjunto de habilidades que pueden aprenderse, pero representan amenazas a la seguridad nacional e internacional.

Las nuevas tendencias en la delincuencia informática están surgiendo todo el tiempo, con los costos estimados para la economía mundial que se ejecutan a miles de millones de dólares. En el pasado, se cometía el delito cibernético principalmente por individuos o grupos pequeños. Hoy en día, estamos viendo las redes de ciberdelincuentes altamente complejas, reuniendo a personas de todo el mundo en tiempo real para cometer crímenes en una escala sin precedentes. Las organizaciones criminales recurren cada vez más a Internet para facilitar sus actividades y maximizar su beneficio en el menor tiempo. Los delitos en sí no son necesariamente nuevos como, por ejemplo: el robo, el fraude, el juego ilegal, pero están evolucionando con las oportunidades que se presentan en línea y por lo tanto se van generalizando y perjudicando cada vez más.

Si bien existen varios tipos de amenazas, el tema de ensayo está enfocado principalmente en el ámbito Estatal teniendo en cuenta la importancia de la Seguridad Integral**,** por lo que hoy en día las amenazas a la seguridad no provienen solas y directamente de otros Estados ni de una facción del propio Estado, sino además y principalmente de organizaciones internacionales o transaccionales de crimen organizado, piratería y terrorismo, basadas o provenientes en muchos casos de Estados inviables que no ejercen el debido control sobre su propio territorio y población.

A todo esto y por la falta de seguridad aparecen los ciberdelitos que, según Rayón y Gómez, el ciberdelito o también conocido como cibercrimen, se lo considera como cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito. Es por eso que se reconoce su rápido crecimiento y se entiende que cada vez son más los criminales que están explotando la velocidad, conveniencia y anonimato de Internet.

La ciberseguridad consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. A su vez, la seguridad cibernética, también conocida como la seguridad informática, se centra en la protección de los ordenadores, redes, programas y datos contra el acceso no deseado o no autorizado, modificación o destrucción.

Se puede observar que la ciberdelincuencia va más allá y es por eso que Dorothy Denning, profesor de ciencias de la computación, ha presentado una admirable definición inequívoca en numerosos artículos acerca del ciberterrorismo indicando que es la convergencia del espacio cibernético y el terrorismo que se refiere a la ilegalidad de ataques y amenazas de ataques contra los ordenadores, las redes y la información almacenada en el mismo cuando se hace para intimidar o coaccionar a un gobierno o sus personas en consecución de objetivos políticos o sociales. Además, para calificar como ciberterrorismo, un ataque debe dar lugar a la violencia contra personas o bienes, o al menos debe causar bastante daño para generar temor en la sociedad.

El ciberterrorismo es una opción atractiva para los terroristas modernos sobre todo en cuanto a evidencia digital se refiere, por varias razones según Jones (2022):

• Es más económico en términos monetarios que los métodos tradicionales de terrorismo. Todo lo que necesita un terrorista es una computadora personal y una conexión en línea. Los terroristas no necesitan comprar armas de fuego y explosivos; en cambio, pueden crear y distribuir virus informáticos a través de una línea telefónica, un cable o una conexión inalámbrica.

• El ciberterrorismo es más anónimo que los métodos tradicionales de terrorismo. Como muchos navegantes de Internet, los terroristas utilizan en línea nicknames- "nombres de pantalla", o se conectan a un sitio web identificándose como un "invitado", por lo que es muy

difícil para las agencias de seguridad y las fuerzas de policía rastrear la verdadera identidad de los terroristas.

• La diversidad en el número de objetivos son enormes. El ciber terrorista podría tener como objetivo los ordenadores y redes informáticas de los gobiernos, los particulares, los servicios públicos, las aerolíneas privadas, y así sucesivamente. El gran número y complejidad de los posibles objetivos garantizan que los terroristas pueden encontrar debilidades y vulnerabilidades para explotar.

• El ciberterrorismo puede llevarse a cabo de forma remota, una característica que es especialmente atractivo a los terroristas. El ciberterrorismo requiere menos entrenamiento físico, la inversión psicológica, riesgo de mortalidad, y los viajes que las formas convencionales de terrorismo, por lo que es más fácil para las organizaciones terroristas reclutar y retener a los seguidores.

• El ciberterrorismo muestra tentáculos tiene el potencial de afectar directamente un mayor número de personas que los métodos tradicionales terroristas, generando de ese modo mayor cobertura de los medios, que en definitiva es lo que quieren los terroristas".

Así también el término ciberguerra es cada vez más controvertido. Un número de expertos en el campo de la seguridad informática y la política internacional cuestionan si el término caracteriza con precisión la actividad ilegal que ocurre en el ciberespacio.

Se conoce que toda nación puede iniciar una guerra en el tema cibernético que ponga en riesgo su propia integridad o la de otros países, ya que la mayor parte de información de fuerzas militares y policiales se encuentran en la red y con su correspondiente interconexión a la web, por lo que los colectivos no gubernamentales de personas pueden también violentar las seguridades del ciberespacio y con ello se inicia una guerra cibernética, lo cual requiere protección contra este tipo de ataques que muchas veces los gobiernos se quedan limitados para darlos (Computer fornesics, 2026).

Entonces, los gobiernos, las entidades públicas, militares, empresas, instituciones financieras, hospitales y otros negocios recogen, procesan y almacenan una gran cantidad de información confidencial propia y de sus ciudadanos en sus computadoras, y transmiten los datos a través de redes a otros equipos. Con el creciente volumen y sofisticación de los ataques cibernéticos, se requiere una atención continua para proteger la confidencialidad de la empresa y la información personal, así como salvaguardar la seguridad integral, por lo tanto, la valoración de las amenazas actuales y futuras es una parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad y a su vez, será preciso tener presente la prevención, detección, respuesta y recuperación junto con la cooperación internacional.

Ecuador, al ser un país en desarrollo, no veía necesario desarrollar una infraestructura segura en el ámbito de telecomunicaciones, exceptuando tal vez parte de su infraestructura militar, y es por eso que en 2011, el investigador de seguridad informática Dmitry Bestuzhev, declaraba que, a pesar de que se han hecho esfuerzos, en Ecuador todavía no se trabaja en seguridad de manera sistemática con políticas definidas, reconociendo que el Gobierno no tiene un plan de acciones para todas las entidades del país, debido a que muchas veces, es el

propietario o el administrador del sitio web el que decide qué hacer para que este sea seguro, por ello Ecuador llega a ser un blanco fácil de los atacantes, por lo que si bien en el Ecuador ya hablamos de Seguridad Integral, no hemos materializado ese concepto para la ciber protección frente a las ciber amenazas.

En base a lo dicho, se verifica que en los juicios del Ecuador ya es usual tratarlos en cuestión de la confiabilidad de las pruebas digitales, pero pueden generarse problemas en la no preservación de datos, donde existen defensores de los procesos penales que pueden obviar la facilidad con la cual se pueden alterar los registros digitales, lo que influye en los hallazgos y en la toma de decisiones, por lo que es posible desarrollar estrategias sólidas para casos de incidentes amplios asociados con ciberdelitos.

- **Cadena de Custodia**

La investigación científica desprendida por la comisión de un delito o infracción se lo realiza por medio de las ciencias forenses y de la medicina legal, la cual de manera sustancial aporta con los resultados concluyentes esgrimidos de los análisis ejecutados a elementos vinculados con la acción u omisión que infringe la ley penal, esto es, el hecho delictivo que se persigue.

Por otra parte, los medios o componentes examinados son en su mayoría extensos, debido a que, de manera general existen indicios biológicos; como máculas sanguíneas o secreciones salivales, que puedan ser encontrados en el lugar de los hechos, asimismo, se puede hallar la existencia de muestras no biológicas como un arma cortopunzante, el proyectil de un arma de fuego, o a su vez, la de información que reposa en un dispositivo móvil, cámara de seguridad o algún otro tipo de medio electrónico que capture, procese y transmita imágenes o videos, que permitan esclarecer los hechos. Por tanto, la recuperación de estos indicios y dichos resultados a través de un proceso de exámenes se transforman en evidencia.

En consecuencia, los resultados logrados bajo el análisis de estas evidencias, una vez presentados e incorporados en el juicio oral, constituyen elementos probatorios materiales orientados a demostrar los hechos. No obstante, para que dichas pruebas sean totalmente admitidas y valoradas debidamente conforme a derecho, resulta indispensable garantizar que las evidencias no hayan sido manipuladas de manera errónea y que sean resguardadas bajo procedimientos direccionales adecuados que aseguren su correcta conservación, así como el mantenimiento de su integridad e inalterabilidad desde el momento de su recolección hasta su pragmatización dentro del proceso judicial. (Bórquez, 2011). A este procedimiento técnico-legal se lo conoce como “cadena de custodia”.

Por otra parte, una de las posibles formas de vulneración de dichos indicios (ya sean estos biológicos o no biológicos), se produce cuando existe un quebrantamiento en los procesos técnicos de la cadena de custodia, situación que ocurre ante la ausencia de directrices adecuadas para su preservación, obtención o almacenamiento. Esta irregularidad puede comprometer de manera directa la autenticidad e integridad de los elementos probatorios, limitando o incluso impidiendo su admisibilidad y valoración dentro del juicio. (TN University, 2023)

En este sentido, esto puede ser generado por la falta de recopilación adecuada de la evidencia, lo cual es producido por ausencia u omisión de conocimientos técnicos especializados, por no considerar norma legal de regulación y directrices que efectivicen estos procesos. Además de los aspectos mencionados, se encuentra el uso de la tecnología emergente lo cual incluye a aquellos medios físicos equipados con software y conexión a internet. Por lo tanto, la aplicación de directrices eficientes y adecuadas para el manejo de la evidencia digital mitiga la falta de autenticidad y fiabilidad, donde la manipulación digital ingresa en tensión debido a la falta de protección de datos personales, así como la ausencia de marcos jurídicos adecuados, que podrían desencadenar vulneraciones de derechos o de la inadmisibilidad de la evidencia por motivos legales.

- **Comportamiento técnico–procesal de los operadores de justicia frente a la evidencia digital.**

Debido al constante desarrollo de las tecnologías de la información y la comunicación el cual está ligado de forma homogéneo con el uso masivo de dispositivos inteligentes, plataformas digitales y redes sociales, ha modificado significativamente la forma en que se produce, almacena y evidencia los elementos probatorios dentro de los procedimientos jurídicos. En base a ese contexto, la evidencia digital ha adoptado un papel cada vez más relevante, constituyéndose en un elemento intrínseco para lograr el esclarecimiento de los hechos frente a controversias contemporáneas.

Esta realidad pone de manifiesto las limitaciones que surgen en el sistema probatorio tradicional frente a la necesidad de incorporar nuevos mecanismos y criterios técnicos conducentes a garantizar la autenticidad, validez y admisibilidad de este medio probatorio. Bajo este aspecto, se presentan retos para los actores involucrados en el proceso jurídico, debido a que, la masificación exponencial de las tecnologías de la investigación son fundamentos constantes y presentes en un procedimiento jurídico. (Coronel & Arguello, 2025). No obstante, es preciso señalar que en base al principio *"iura novit curia"* es el juzgador quien conoce de derecho, por lo tanto, este último es el actor capacitado para determinar la validez probatoria de estos medios dentro de un proceso judicial.

Por otra parte, dentro del contexto ecuatoriano es evidente la capacitación que poseen los operadores de justicia frente a los delitos e infracciones informáticas, lo cual simboliza la clave de la tipificación conductual, a su vez, se observan otras normas en las que se rigen como la Ley Orgánica de Protección de Datos Personales (LOPDP), el Código Orgánico Integral Penal (COIP) y el reglamento que lo regula donde se fomentan los principios de consentimiento, proporcionalidad de uso de la información sensible, lo que verifica la manera de usar la evidencia digital (Coronel et al., 2023)

Por consiguiente, en el ámbito jurídico los operadores de justicia deben manejar con cautela y profesionalismo la evidencia digital por medio de la cadena de custodia como un principio sine qua non, de legitimidad con la que se debe contar en un proceso penal, debido a que, el juez debe verificar que la evidencia ya sea esta digital o de cualquier otra naturaleza no

haya tenido ninguna clase de alteración desde la etapa de identificación hasta la presentación dentro del juicio (Anna et al., 2023)

A su vez, el principio de legitimidad jurídica se encuentra contemplado en el artículo 457 del Código Orgánico Integral Penal, para valorar la prueba en cuanto a la autenticidad de la misma, la correspondiente cadena de custodia y la aceptabilidad técnico-científica, lo cual va de acuerdo a los criterios descritos por Daubert, quien afirma que las pericias deben tener reproducción, verificación y se deben basar en un método científico, donde los dos contextos articulan un rigor técnico de transparencia metodológica donde se verifica la admisibilidad juridicial de la evidencia digital.

Así también cabe destacar que, los operadores judiciales son profesionales capacitados que deben observar de manera permanente que se apliquen criterios estándares que garanticen la confiabilidad de la prueba. Así también el perito especialista en evidencia digital, es indispensable para generar los aspectos jurídicos y para valorar el ámbito judicial, sin embargo, la calidad del peritaje con el aspecto procesal muestra el condicionamiento de los procesos judiciales. (Avenmañay et al., 2025).

- **Impacto de la gestión inadecuada de la evidencia digital en el proceso penal y la cultura judicial.**

La globalización digital ha cambiado la perspectiva en la cual los sistemas de justicia penal examinan y ponderan las pruebas, generando un elemento probatorio de tipo complejo, sobre todo ahora que los procesos penales contemporáneos se ha indo renovando, debido al aspecto inmaterial, flexible y alterable con relación a las pruebas tradicionales lo que forma parte del derecho probatorio (Rosas & Pila, 2023)

En cuanto al ámbito ecuatoriano, este aspecto es importante porque no hay suficiente regulación que delimita los procesos técnicos y jurídicos para valorar la evidencia digital como parte del proceso penal. Se ha verificado que, en diversos países de Iberoamérica como España, Colombia, Chile y Perú no solo han avanzado con procedimientos concretos referentes a la cadena de custodia de los indicios digitales, sino también, que han aplicado ciertos parámetros y directrices orientadas a la extracción, preservación, y autenticidad de estos medios electrónicos, en los cuales reposa información eficiente para la resolución de controversias

Frente a esto, el Ecuador, no ha adoptado de manera general dichos estándares, lo cual puede generar inadmisibilidad probatoria, e incluso puede darse la nulidad definitiva de la prueba digital. Lo cual da como resultado la falta de eficiencia en el proceso penal, lo que perjudica también en las decisiones judiciales, así como en la seguridad jurídica.

Según Espinoza (2024) el estado del problema involucra un elemento que limita el ámbito jurídico, técnico e institucional debido a que el Código Orgánico Integral Penal, el Código Orgánico General de Proceso (COGEP), y demás códigos o leyes, no poseen normas supletorias o dentro de la mismas normativas aquellas directrices encaminadas a preservar la evidencia digital, así también se dan problemas en el ámbito técnico como la falta de infraestructura adaptada a los procesos digitalizados y protocolos para su ejecución.

Entonces, estas limitantes son opuestas con la necesidad de gestionar un modelo integral administrativo para el tratamiento de la evidencia digital fundamentado en la integridad, trazabilidad y proporcionalidad.

UNIDAD III: Evaluación del cumplimiento normativo y propuestas de mejora para fortalecer la autenticidad y fiabilidad de la evidencia digital

- **Análisis del cumplimiento normativo y técnico en el manejo de evidencia digital en Ecuador.**

Se conoce que, el tratamiento de la evidencia digital es de suma importancia especialmente en la investigación forense, donde es indispensable analizar los marcos legales y normativos disponibles para ejecutar su práctica como un proceso indagatorio efectivo, tomando en cuenta que esto es indispensable para su correcta recopilación, resguardo y análisis.

En cuanto al cumplimiento de la norma en el Ecuador, la reforma al Código Orgánico Integral Penal se ha tipificado en lo que tiene que ver con la evidencia digital es de igual veracidad probatoria de una de tipo común, si bien el sistema judicial del Ecuador exige un archivo de código fuente para validar la prueba (Ojeda, 2025).

Por otro lado, se observa también un avance con la instauración de la Ley Orgánica de Protección de Datos Personales (LOPDP), que ha sido promulgada en 2021, que exige sanciones en cuanto a aspectos relacionados con el cumplimiento de la licitud de la prueba, ya que toda evidencia digital que se obtiene y que ha sido alterada sin excepción es considerada prueba ilícita y se excluye del proceso.

- **Herramientas técnicas y jurídicas para el seguimiento del manejo de evidencia digital**

El cumplimiento de los estándares técnicos en el Ecuador se lo articula a partir de los estándares mencionados anteriormente como las normas ISO/IEC 27037 y ISO/IEC 27042, y de acuerdo a la necesidad de que se demuestre al juez por parte del perito la integridad de la prueba forense a partir del cumplimiento del siguiente proceso según Pita (2024):

1. Aislamiento físico y electromagnético. - Con utilización de bolsas de Faraday para que se prevenga una posible alteración de los dispositivos como el Google Find My Device
2. Demostrar que la evidencia no se la adquirió de forma invasiva: Con uso de bloqueos de escritura para garantizar que el sistema operativo no cambie los datos y metadatos para su adecuado acceso
3. Verificar con algoritmos (Hashing), a partir del uso de la huella digital única, ya que no puede alterarse ni un bit, porque de ser este el caso el hash cambiará y esto a su vez inhabilita automáticamente la prueba

- **Lineamientos estratégicos para fortalecer el rol técnico–jurídico del sistema penal frente a la evidencia digital.**

Si bien muchos son los desafíos a los que se enfrenta el sistema procesal penal en Ecuador al tratarse de la evidencia digital, es posible dar ciertos lineamientos para el fomento

del rol tanto técnico como jurídico en cuanto al marco normativo en el Ecuador sobre este tema, entre estos están:

1. La evidencia digital es subida a la nube (Cloud Forensics).

Según Pita (2024) indica que; los datos deben ser auténticos y para esto se debe mantener sigilo d ellos mismos, por lo que, en el momento en que la evidencia se encuentra por el exterior en otros países distintos al Ecuador como en Amazon, google y otros, el perito tiene la obligación de incluir técnicas para adquirirlas sin un disco duro físico sino que todo se sube de forma virtual en la nube, por eso es importante que esta subida se adapte también al cumplimiento de la norma, porque va a depender de la cooperación internacional y la forma cómo se preservan los logs para su correspondiente conectividad.

2. La ejecución de la cadena de custodia digital 2.0.

Se trata de la aplicación del Blockchain para registrar este proceso en el Ecuador, esto a su vez prevendría que se alteren datos cuando la evidencia sale e ingresa.

3. También según lo que refiere Echeverría et al., (2024) se puede usar herramientas como las siguientes:

- EnCase & FTK (Forensic Toolkit): estos mecanismos permiten crear imágenes forenses escaneando bit a bit y analizando en los sistemas
- X Ways Forensics: Se usa para recuperar archivos borrados y metadatos
- Cellebrite UFED: Este es un mecanismo que suele usar la Policía Nacional para verificar datos en smathphones, lo que permite un bypass que solo puede funcionar bajo autorización judicial
- HashCalc: Instrumento de generación de firmas digitales que son como un sello de seguridad ante la huella digital

4. Adicionalmente, es posible aplicar un protocolo de seguimiento según Torre et al., (2024) a partir de la estandarización de la exclusión de pruebas, entre las cuales se encuentran las siguientes:

- Lockdown: Es una técnica que permite la no invasión y contaminación de la red
- RFC 3227: Es una guía formal para verificar cómo la evidencia fue obtenida, en cuanto a los momentos primeros porque almacena en su memoria RAM antes que en un disco duro
- ISO/ IEC 27037: Es indispensable aplicar esta normativa internacional para tratar los dispositivos y evidencia digital, lo cual se encuentra autorizado desde el año 2021

5. Sería importante incrementar la seguridad en temas de trazabilidad de la información, por ejemplo, para inicios del 2025 el Consejo de la Judicatura ya instauró la aplicación llamada EFJ Digital con la resolución 057-2025, que da la potestad a los juristas y peritos para que por sí mismos validen credenciales con uso de códigos QR, de tal manera que se garantiza que quien manipula la evidencia tiene plenas facultades de ejecución de esta labor, así también se ha implementado el sistema SATJE que es un instrumento jurídico para registrar de forma cronológica los actuares de los procesos, si bien esto todavía está en inicios constituye un avance para el tratamiento de la evidencia digital en el proceso penal que debe continuar mejorando e innovándose, a partir del uso de cada vez nuevos mecanismos de seguridad.

El sistema de IA puede dar a conocer nuevas pistas en casos sin resolución, sobre todo en el momento en que las huellas dactilares que se encuentran en la escena del crimen son pertenecientes a dedos distintos a los archivados previamente, es así que, se sugiere que: *''el sistema basado en inteligencia artificial podría generar nuevas pistas en casos sin resolver, especialmente cuando las huellas dactilares encontradas en la escena del crimen pertenecen a dedos distintos a los archivados''* (Geek, 2024).

De acuerdo a los autores Caiza et al., (2024) se ha realizado una metodología con uso de una investigación cualitativa y documental, con utilización de un análisis de doctrina en torno al modo de investigación, de acuerdo al alcance descriptivo y explicativo, además de tipo transversal y documental, con su finalidad práctica.

Para ello se hizo un análisis y selección de información de bases de datos, textos y marco normativo al respecto, para luego realizar su análisis, discusión, contraste y generación del conocimiento adquirido para el tema en estudio. La técnica de investigación fue la recopilación y análisis de fuentes documentales bibliográficas con enfoque científico como son libros, revistas científicas, artículos, protocolos sobre el tema, teniendo en cuenta que, las ciencias forenses actualmente no se han estudiado profundamente en el país.

En cuanto a la identificación primaria se observó que, ha sido posible analizar el reconocimiento por parte de familiares directos o de documentos del fallecido (cédula de ciudadanía, licencia, credencial, carnets) (Ramírez, 2021). Además, se observa que, el reconocimiento debe ser principalmente por la familia, ya que son quienes dan información morfológica del cadáver como por ejemplo si este ha tenido cirugías, prótesis, cicatrices, tatuajes, heridas, incluso se detalla muchas veces la vestimenta con la que se encontraba en vida la última vez que se le vio a la persona, todos estos datos se deben comparar con el examen exterior del cuerpo, como un aspecto clave para lograr el reconocimiento.

También se sabe que, esto depende del estado en el que se encuentre el cadáver, debido a que, si, por ejemplo, *''se lo halla en estado de descomposición: hinchado, putrefacto o esqueleto, o con osamentas óseas fragmentadas, suele ser un desafío generar la identidad antes del examen''* (Caiza, et al, 2024, p.76).

Por lo tanto, cuando se da el reconocimiento por información de datos personales, la identidad que se brinda debe ser verificada según procesos: técnicos y científicos, tanto de rutina como personalizados según el caso, de tal forma que se categorice la identidad concreta del cadáver, ya que con estos resultados y con el mach positivo, es posible identificar al occiso, lo que aportará a la investigación.

Es así que, la identidad humana cadavérica constituye una especialidad de la ciencia forense indispensable, ya que tiene diversos análisis, pues se asocia la capacidad de incluir avances científicos y su relación con las técnicas de identificación humana en los cadáveres con enfoque macro, meso y micro.

6. Adicionalmente como otra estrategia para fortalecer la evidencia digital y evitar alteraciones es posible aplicar los nuevos alcances de la huellografía en escenas del crimen, para lo cual se disponen de tecnologías innovadoras que aplican este elemento:

Tecnología de la INTERPOL: De acuerdo a la Interpol (2020) para que las huellas dactilares deben tener la calidad necesaria, y el sistema tecnológico es el encargado de comparar y analizar los detalles dactiloscópicos usando un algoritmo profesional, es posible tener como resultado la identidad de los posibles candidatos del crimen. Adicionalmente, las huellas dactilares con alta calidad, que se envían por los países miembros, por medio del sistema I-link que dispone de las correspondientes notificaciones, difusión, mensajes I link que se dan por el Centro de Biometría y se almacenan en las bases de datos de SAID. Hay países miembros que pueden utilizar el Centro de Biometría para envío de solicitudes, cuando la investigación requiera el cotejo de huellas dactilares de un individuo de interés a nivel internacional.

Tecnología 2D y 3 D de estudio de huellas dactilares antiguas: Si bien, a lo largo del tiempo se ha analizado la huella dactilar, de tal forma que con el paso del tiempo puede alterarse o degradarse y esto puede destruir su compuesto químico usual, además la topografía, por ello una de las técnicas más usuales para ello es la de la cresta (ridge drifts), dicho fenómeno está demostrado por la naturaleza dinámica. Este dinamismo se lo usa como un movimiento de la cresta y es un hecho que tiene impacto en la identidad de la huella, pues se decía antes que, la huella era una copia fija de la piel desde su origen, pero las modificaciones de las crestas podrían generar cambios en su identificación.

A partir de este problema, han demostrado que al usar tecnología 2D como captura de fotos normales, para el descubrimiento de edad y procesos de degradación, en ese caso se observan las tres dimensiones que pueden tener cambios en el tiempo, incluyendo variaciones en el ancho de la cresta o que se pierda el color entre esta y los surcos. A partir de ello se ha necesitado evaluar el uso de la tecnología 3D o también el análisis de la composición química, sin embargo, todavía no se ha enfocado el estudio en el proceso de envejecimiento.

Para ello se suele usar perfilómetros ópticos que se utilizan para la medición de la superficie de los materiales, de tal forma que son adecuados para la detección micro abrasión y se usan para fabricar y controlar su calidad.

En el estudio de Carreno (2018) se utiliza objetivos que dividen la luz de dos trayectorias: una que se refleja por la muestra y otra por un espejo. Una vez que las dos longitudes se equiparan es cuando se muestran las franjas, y, por lo tanto, allí es cuando se utiliza el software para la determinación de la altura de cada punto en la imagen que ayuda a hacer una reducción de nanometría, para lo cual se da una nube de puntos, siendo que, el conjunto de puntos que detalla la ubicación (x, y), en la superficie y la altura (z) para la creación del perfil en 3D.

Para la toma de huellas en el estudio mencionado se generó de la siguiente manera:

1. Se lavaron las huellas con agua y jabón
2. Se frotó las manos contra el antebrazo, frente y la nariz

3. Se frotó las manos entre ellas
4. Impresión de las puntas de dedos en el sustrato

Las huellas se dejaron en un portaobjetos de microscopio de vidrio y en la cubierta transparente de plástico de CD, para lo cual se tomaron huellas de dedos: índice, medio y anular, también se controló la presión en el proceso y la toma se ejecutó en una habitación con temperatura de 22°C con 23% de humedad.

Las huellas cumplieron con el proceso de envejecimiento en una cabina cerrada oscura, y se conservó en un año a temperatura de 21° a 24°C y de 22 a 26% de humedad, se obtuvo 13 imágenes de cada donante y se usó el perfilómetro óptico ZeScape de Zygo, con aumento de 0.63 x de maximización de la zona de visualización para cada impresión. Se hizo un análisis cualitativo y cuantitativo de variaciones topográficas en las huellas dactilares. En los resultados obtenidos se verificó que hubo cambios en la calidad visual de las crestas entre las dos superficies de análisis, pero también hubo similitudes en los patrones de degradación, luego de la recolección electrónica se verificó que, el perfilómetro óptimo es más sensible que el TiO2, pues detectó la diferencia entre las huellas frescas y antiguas sobre sustratos de plástico y cristal (Carreno, 2018).

Fue posible identificar que, el uso de perfilómetro en 3D es una excelente opción para comparar la diferencia entre huellas nuevas y antiguas, de tal forma que se obtienen resultados más precisos, para prevenir cualquier tipo de anomalía en la detección de huellas producto del envejecimiento de estas.

Sistema automatizado de identificación de huellas dactilares (AFIS): Es posible usar la identificación automática de huellas dactilares, como aquel proceso que de forma automática da las similitudes entre una o diversas huellas dactilares desconocidas y una base de datos de impresiones que pueden o no ser conocidas. Los sistemas de identificación criminal se originaron a finales del siglo XIX, que se apareció con el Sistema Henry de clasificación de huellas dactilares, en el cual se clasificaron de acuerdo a características de carácter fisiológico y antropométrico que también se lo llamó sistema Bertillon, por el cual las mediciones se dieron de los sospechosos y se archivaban. En el Reino Unido, la Policía Metropolitana inició al uso de la biometría para identificarla en 1901, así en Estados Unidos la Policía de Nueva York inició a utilizar este sistema desde 1902, y la de Francia inició a finales de este mismo año (Thales, 2021).

Ya para los años 1920, se creó el primer Departamento de identificación, con un repositorio de bases de datos de identidad criminal para las agencias de aplicación de la ley de los Estados Unidos, pero todavía se debía clasificar de forma manual por un equipo de trabajo en continuo crecimiento. Esta tecnología innovadora se dio por primera ocasión en la década de los 80s, cuando se usaron los Sistemas Automatizados de Huellas Dactilares (AFIS) usados para identificar escenas del crimen y hoy representa un mecanismo base de trabajo policial y otras agencias que se encargan del cumplimiento de la ley a nivel mundial.

Al aumentar de forma potencial la identificación de un sospechoso con estos sistemas, se ha concebido una nueva forma en la cual las autoridades abarcan la investigación de manera

más amplia, ya que el principio clave que utiliza la tecnología moderna para la automatización, de las huellas dactilares de un sospechoso o en la escena del crimen involucra una evolución continua (INTERPOL, 2020).

Así, según Thales (2020) la evolución del AFIS representa un instrumento efectivo y eficiente, que analiza grandes cantidades de bases de datos y brinda coincidencias de huellas dactilares en minutos, siendo el resultado de tareas de investigación y desarrollo, además ofrece un proceso continuo, esta tecnología biométrica incluye el reconocimiento fácil y del iris, por lo que el AFIS está transformándose en los últimos tiempos en ABIS (Sistema de Identificación Biométrica Automática), de tal forma que se obtiene una herramienta aún más poderosa que la anterior versión.

Figura 1. Sistema ABIS



En la Figura 1, se observa capturas de pantalla tomado al nuevo sistema ABIS, donde tan solo al incluir las huellas digitales o el escaneo del iris de la persona es posible revelar sus datos personales, fotografías recientes y demás información pertinente para el personal de criminalística, además que se arroja en tiempo real.

Cabe mencionar que, la identidad biométrica se fundamenta en el principio de que cada persona podría disponer de un conjunto de datos de reconocimiento y verificación auténticos y personalizados, en ese caso las huellas dactilares según Francis Galton, dijo que la probabilidad de encontrar dos huellas dactilares similares es una en cada 64 mil millones, incluso cuando las personas sean gemelas. Es así que, la utilización de huellas dactilares como producto para la identificación delincuencial se remonta incluso antes de la venida del AFIS.

Uso de la IA para identificar huellas dactilares: Esta tecnología permite optimizar la detección de huellas incluyéndola en dispositivos con computadores, smarthphones, dichos modelos reconocen la huella dactilar de manera rápida y precisa, siendo ideal para diversas aplicaciones en las cuales la velocidad y eficiencia son la clave. Adicionalmente, cuenta con

integración de software con compatibilidad multiplataforma, de tal forma que, se diseña la tecnología para ser integrada con servidores de alta gama hasta microcontroladores de bajo consumo (id3 Technologies, 2020).

Dicha tecnología involucra diversos pasos:

1. Se adquiere huellas dactilares para capturar patrones únicos en la yema del dedo

2. Análisis y extracción de características de distinción como: cresta, valles, puntos minuciosos con uso de algoritmos avanzados y redes neuronales (id3 Technologies, 2020)

El proceso antes indicado hace que los datos de las huellas dactilares se plasmen en una representación digital y se compare con una base de datos que se almacena para su correspondiente autenticación, lo que le hace un mecanismo de seguridad. A su vez este modelo de IA tiene como característica principal disponer de un diseño ligero y con una pronta capacidad de proceso de información en tiempo real.

Entre los nuevos desafíos de los nuevos sistemas de detección de huella digital, que evolucionó el AFIS moderno, pero todavía se requieren nuevos avances tecnológicos acoplados a las nuevas realidades y al aumento de las olas delincuenciales y de crimen organizado (Thales, 2021).

Por ello es importante que sea posible:

- Leer y capturar una imagen tradicional de la huella dactilar en segundos
- Detección de características distintivas más detalladas en la imagen
- Comparación de un conjunto de datos de minucias, tomados de un sospechoso y su comparación con una amplia base de datos de registros similares
- Mejoras en el ingreso de huellas palmares, la interconexión de AFIS con otros sistemas de información de justicia penal, con fotos digitales, dispositivos lectores de huella, uso de biometría multimodal (facial, iris)

En resumen, si bien, los sistemas AFIS, ABIS, han incurrido en nuevas propuestas y ya incluyen aspectos como vincular su sistema con instituciones de justicia, dar a conocer información en tiempo real, vincular con otras huellas de registros multimodal, y otros, todavía son situaciones que están en el etapa de prueba, por ello es importante que se sigan actualizando pero también perfeccionando los sistemas existentes que incluso pueden incluir el uso de la Inteligencia Artificial para detección de huellas.

CAPÍTULO III. METODOLOGÍA

3.1 Tipo de diseño de la investigación

Por la selección de cada uno de los objetivos planteados, la presente investigación es de carácter jurídico exploratoria y dogmática.

Dogmática

El enfoque principal se dirigió hacia el efectivo análisis y adecuada interpretación de cada una de las normas jurídicas vigentes, sin otorgar relevancia al contexto de carácter social o histórico en el cual son aplicadas; el principal propósito es sistematizar, explicar y clasificar cada una de las normas y principios legales, "según su establecimiento en códigos, leyes normativas de carácter nacional, internacional y jurisprudencia, con el fin de comprender su alcance, aplicación y coherencia interna". (Román, 2023, p. 37)

Jurídica exploratoria

La investigación de carácter jurídica exploraría se manifiesta cuando el contexto o temática a abordar es nuevo o existe escasa información del mismo, se utiliza principalmente al abordar un tema poco explorado o novedoso en el campo del derecho; con la finalidad de identificar problemas, variables y áreas de carácter relevantes en el área legal a estudiar. (Rivadeneira, 2024, p. 28). Además, La investigación jurídica exploratoria es útil para este estudio porque la regulación y el tratamiento de la evidencia digital en el proceso penal ecuatoriano aún presentan vacíos normativos y escasa sistematización doctrinaria.

Dado que se trata de un campo en desarrollo dentro del Derecho, este tipo de investigación permite identificar problemas poco estudiados, reconocer falencias en la cadena de custodia digital, examinar cómo los operadores de justicia aplican criterios de autenticidad y fiabilidad, y explorar áreas donde no existe suficiente investigación previa. Así, facilita obtener una visión inicial clara y fundamentada que sirva de base para futuros estudios y propuestas de mejora.

La interconexión de los tipos de investigación previamente mencionados, la dogmática y la exploratoria, permite acoger el problema de carácter jurídico desde diversas aristas, otorgando una análisis profundo y efectivo del tema a tratar.

3.2 Enfoques de investigación

Enfoque Cualitativo. – El presente enfoque analizó cada uno de los fenómenos de carácter jurídicos, junto a sus significados y realidad; mediante la incorporación del presente enfoque se estudia e interpreta cada una de las normas, doctrinas y material bibliográfico de manera exacta, profunda y analítica, emparejando cada una de las causas y consecuencias en el contexto jurídico y social que acogen el problema jurídico a investigar; este enfoque ofreció

adaptabilidad en el tiempo en que la investigación se realice, por la incorporación de hallazgos nuevos y emergentes en el contexto jurídico.

Enfoque Cuantitativo. – Se realizó un análisis de carácter sistemático y objetivo de cada uno de los fenómenos jurídicos por medio de la recolección de datos duros o numéricos; el presente este enfoque de investigación facilitó la individualización de tendencias y relaciones entre cada uno de los rasgos informativos y estadísticos recolectados en las encuestas.

El enfoque cuantitativo se aplicó para obtener y analizar datos numéricos relacionados con el manejo de la evidencia digital en el proceso penal ecuatoriano. A través de encuestas dirigidas a fiscales, jueces, peritos y abogados, se recopiló información objetiva sobre el nivel de capacitación, frecuencia de errores en cadena de custodia digital y criterios utilizados para valorar la prueba electrónica. Este enfoque permitió identificar patrones, medir la incidencia de falencias técnicas y determinar tendencias que influyen en la autenticidad y fiabilidad de la evidencia digital, aportando datos verificables que complementen el análisis jurídico de la investigación.

3.3 Técnicas de recolección de datos

Encuesta. - La técnica de investigación que se implementó fue la encuesta; con la finalidad de determinar cada uno de los efectos que genera la autenticidad y fiabilidad de la evidencia digital.

Revisión bibliográfica. - Se usó revistas científicas de repositorios de artículos indexados, así como doctrina y textos jurídicos que prestan información relevante y trascendente al respecto del tema en cuestión.

3.4 Población de estudio y tamaño de la muestra

La presente investigación tuvo como población de estudio a 5 jueces, 5 fiscales, 5 peritos y 5 abogados de la provincia de Chimborazo, mismos participantes que otorgaran eficiencia y pertinencia a la investigación, se seleccionó una muestra intencional no probabilística por conveniencia, aplicando criterios de inclusión y exclusión relacionados con su exposición referente a la autenticidad de la evidencia digital.

3.5 Métodos de análisis

Para el sistema de investigación, se implementaron los métodos inductivos, deductivos, jurídico-analítico, otorgando un enfoque de carácter integral y completo a la investigación.

3.5.1 Método deductivo

El método de carácter deductivo "se efectuó al considerar principios o preceptos en el contexto general, aplicables para determinar conclusiones de características particulares en la rama" (Palmero, 2022, p. 23). Además, el método deductivo es adecuado para esta investigación porque permitirá partir de principios generales del Derecho, como el debido proceso y la autenticidad probatoria, para aplicarlos al análisis específico de la evidencia digital en el proceso penal ecuatoriano. A través de este enfoque es posible verificar si las actuaciones de fiscales, jueces, peritos y abogados se ajustan a estos criterios jurídicos generales y, con ello, determinar si la evidencia digital cumple con los requisitos de fiabilidad y validez procesal.

3.5.2 Método inductivo

El método de carácter inductivo se materializó al analizar principios o estatutos en el contexto particular del caso, hasta llegar al análisis general del contexto a cada una de sus conclusiones. Así mismo, el método inductivo es pertinente para esta investigación porque permitió analizar la situación jurídica, práctica y situaciones específicas relacionadas con el manejo de evidencia digital en el proceso penal ecuatoriano, para luego extraer conclusiones generales sobre su autenticidad y fiabilidad. A partir de la observación de actuaciones de fiscales, jueces, peritos y abogados, así como de casos reales y normativa aplicada, es posible identificar patrones, falencias y criterios recurrentes que permitan comprender cómo se gestiona la prueba digital y qué aspectos deben fortalecerse para garantizar su validez procesal.

3.5.3 Método jurídico-analítico

Por otro lado, el método jurídico-analítico "aportó la comprensión a cada una de las normas jurídicas en el estrato social y legal de la realidad actual, otorgando una interpretación integral a la norma" (Cruz, 2023, p. 17). Seguidamente a ello, El método jurídico-analítico es pertinente porque permitió examinar de manera detallada las normas, principios y criterios doctrinarios que regulan la autenticidad y fiabilidad de la evidencia digital en el proceso penal ecuatoriano. Este método facilita interpretar el alcance de disposiciones del COIP, la Constitución y estándares internacionales, para comprender cómo deben aplicarse en la práctica judicial. Gracias a ello es posible identificar vacíos, inconsistencias y necesidades de mejora en el tratamiento jurídico de la evidencia digital.

3.5.4 Método dogmático

El método dogmático dentro de la investigación ayuda a interpretar el derecho basándose en análisis estructurales y ordenados del derecho positivo tras el estudio de textos legales y principios doctrinales; por lo tanto, busca aplicar estas disposiciones sin poner en tela de duda su validez fundamental. El propósito que se busca es crear un sistema normativo coherente y razonable que permuta resolver problemas específicos bajo la ley vigente.

3.6 Procesamiento de datos

Para el efectivo tratamiento de la información se utilizó el análisis de datos direccionado por la secuencia de las preguntas cerradas aplicadas en el cuestionario a la población seleccionada. La interpretación de los datos se efectivizó mediante la incorporación de Microsoft Excel, con la finalidad de analizar, sintetizar tablas y estadísticas, utilizando cada uno de datos recabados y de interés direccionados por los objetivos planteados en la investigación. Para ello se siguió el proceso que se menciona a continuación:

1. Toma de consentimiento informado y permiso de toma de información
2. Toma de datos mediante Google forms
3. Análisis de datos con tablas de frecuencia y porcentajes
4. Elaboración del gráfico estadístico por pregunta
5. Interpretación de resultados
6. Conclusiones de los hallazgos

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 Resultados de la encuesta a los cinco jueces y cinco abogados

Pregunta No. 1

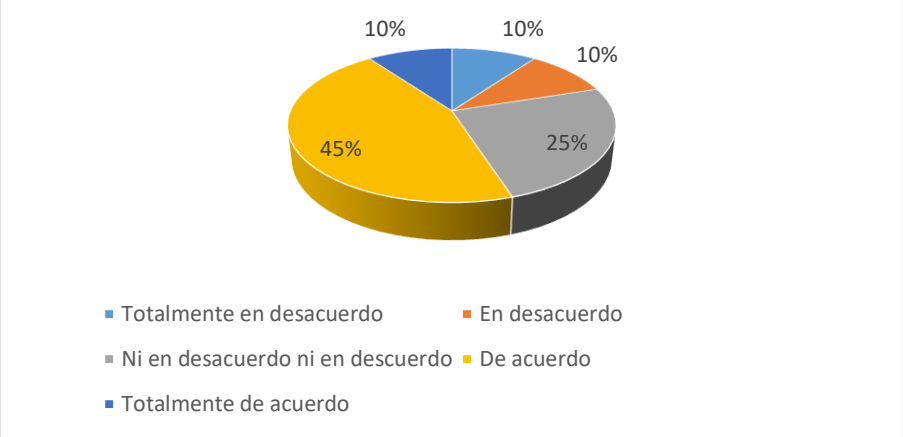
1. ¿Usted considera que la normativa legal en Ecuador se presenta de manera clara y precisa acerca de cómo tratar a la evidencia digital dentro del proceso penal?

Tabla 2. Pregunta 1

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	2	10%
En desacuerdo	2	10%
Ni en desacuerdo ni en descuerdo	5	25%
De acuerdo	9	45%
Totalmente de acuerdo	2	10%
TOTAL	**20**	**100%**

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 2. Pregunta 1



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 45% afirma estar de acuerdo con que la normativa legal en el Ecuador es clara y precisa sobre el tratamiento de la evidencia digital en el proceso penal. El 25% afirma que no está ni de acuerdo ni en desacuerdo con esta apreciación, el 10% está totalmente en desacuerdo con ello, el otro 10% también en desacuerdo y el 10% está totalmente de acuerdo con esto.

Lo antes mencionado indica que, la mayor parte de encuestados están de acuerdo o se mantienen neutrales sobre la consideración de que la normativa legal en el Ecuador hoy es clara

sobre cómo tratar la evidencia digital dentro del proceso penal, lo que indica avances según la percepción de los actores jurista.

Pregunta N°. 2.

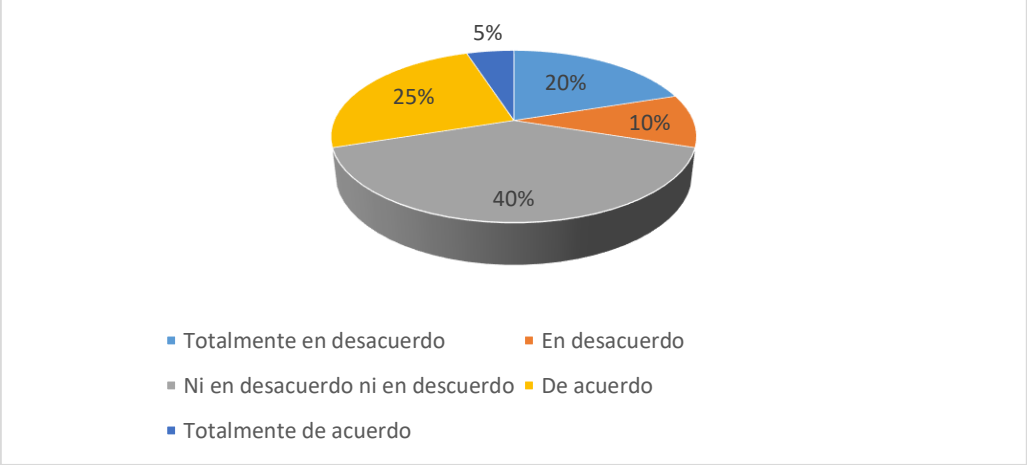
2. ¿El COIP brinda los elementos propicios y suficientes para dar garantía de la autenticidad de la prueba digital?

Tabla 3. Pregunta 2

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	4	20%
En desacuerdo	2	10%
Ni en desacuerdo ni en descuerdo	8	40%
De acuerdo	5	25%
Totalmente de acuerdo	1	5%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 3. Pregunta 2



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 40% es imparcial sobre el hecho de que el COIP brinda los elementos propicios y suficientes para dar garantía de la autenticidad de la prueba digital, el 25% está de acuerdo con esto, el 20% está totalmente en desacuerdo, el 10% está en desacuerdo y el 5% totalmente de acuerdo.

Lo antes mencionado indica que, la mayoría de encuestados que conforman parte de la evidencia digital son imparciales sobre la idea de que el COIP da los elementos propicios para garantizar la autenticidad de la prueba digital, lo que indica que la mayoría de actores

involucrados todavía no están convencidos de que el COIP tiene los elementos claros para garantizar una prueba digital auténtica.

Pregunta N°. 3.

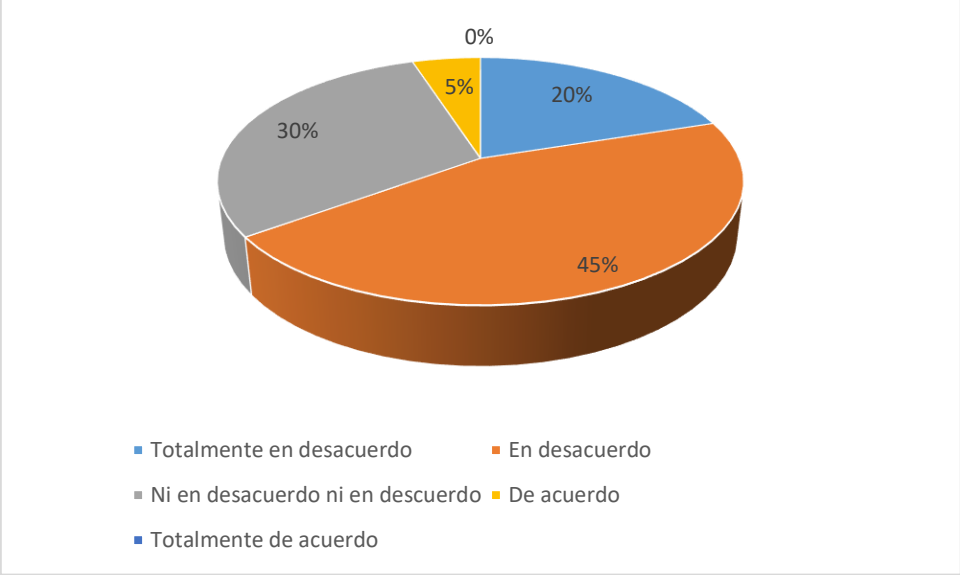
3. ¿En su cotidianidad profesional, ha verificado que hay protocolos estandarizados de tratamiento de evidencia digital?

Tabla 4. Pregunta 3

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	4	20%
En desacuerdo	9	45%
Ni en desacuerdo ni en descuerdo	6	30%
De acuerdo	1	5%
Totalmente de acuerdo	0	0%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 4. Pregunta 3



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 45% está en desacuerdo con que en la vida cotidiana profesional se aplican protocolos estándar de tratamiento de evidencia digital, mientras que, el 30% no está ni de acuerdo ni en desacuerdo con esta afirmación, el 20% indica estar totalmente en desacuerdo con ello, el 5% está de acuerdo.

Lo antes mencionado indica que, la mayoría de jueces, penalistas, peritos están en desacuerdo con el hecho de que se aplica protocolos actualmente para tratar la evidencia digital.

Pregunta No. 4

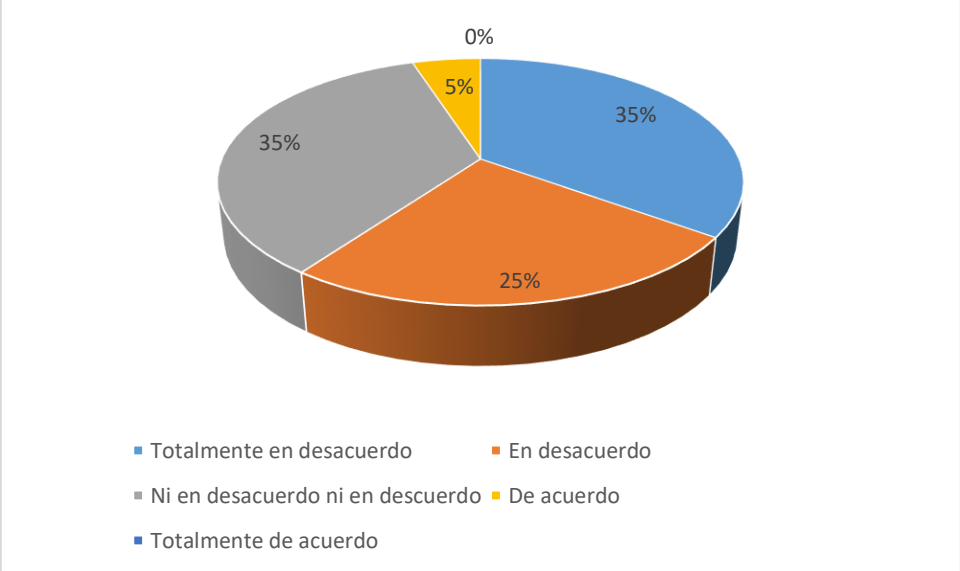
4. La cadena de custodia digital se respeta en las diferentes etapas del proceso penal

Tabla 5. Pregunta 4

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	7	35%
En desacuerdo	5	25%
Ni en desacuerdo ni en descuerdo	7	35%
De acuerdo	1	5%
Totalmente de acuerdo	0	0%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 5. Pregunta 4



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

De los encuestados, el 35% está totalmente en desacuerdo y el otro 35% son imparciales sobre la idea de que la cadena de custodia digital se respeta dentro de las etapas del proceso penal en Ecuador, el 25% afirma que está en desacuerdo con esto, el 5% está de acuerdo.

Lo antes mencionado ratifica que, la mayor parte de actores involucrados del proceso penal están totalmente en desacuerdo a su vez se abstienen en responder sobre el respeto de la

cadena de custodia digital en el proceso penal, lo que indica que queda mucho por hacer en este ámbito.

Pregunta N°. 5

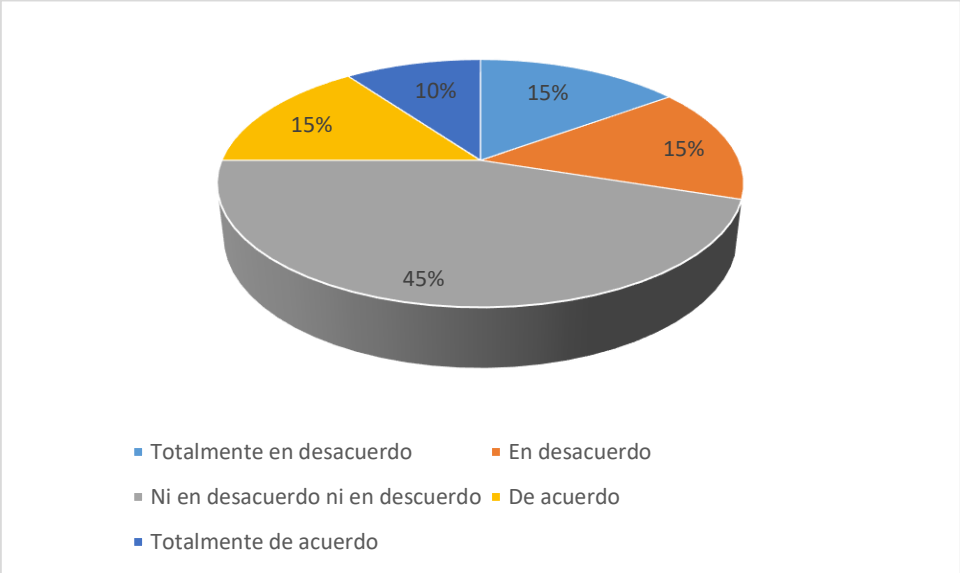
5. ¿Usted cree que los operadores de justicia tienen la capacitación necesaria en el ámbito procesal y técnico para la valoración de la evidencia digital?

Tabla 6. Pregunta 5

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	3	15%
En desacuerdo	3	15%
Ni en desacuerdo ni en descuerdo	9	45%
De acuerdo	3	15%
Totalmente de acuerdo	2	10%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 6. Pregunta 6



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 45% afirma ser neutral en el hecho de que los operadores de justicia tienen la capacitación requerida en el contexto procesal y técnico para valorar la evidencia digital. Mientras que, el 15% está totalmente de acuerdo con esto, el 15% en desacuerdo y el 15% de acuerdo, mientras que, el 10% está totalmente de acuerdo con esta aseveración.

Lo antes mencionado indica que, la mayoría de actores involucrados en el proceso penal creen que los juristas no presentan la capacitación requerida en el contexto procesal y técnico para dar su valoración de la evidencia digital.

Pregunta N°. 6

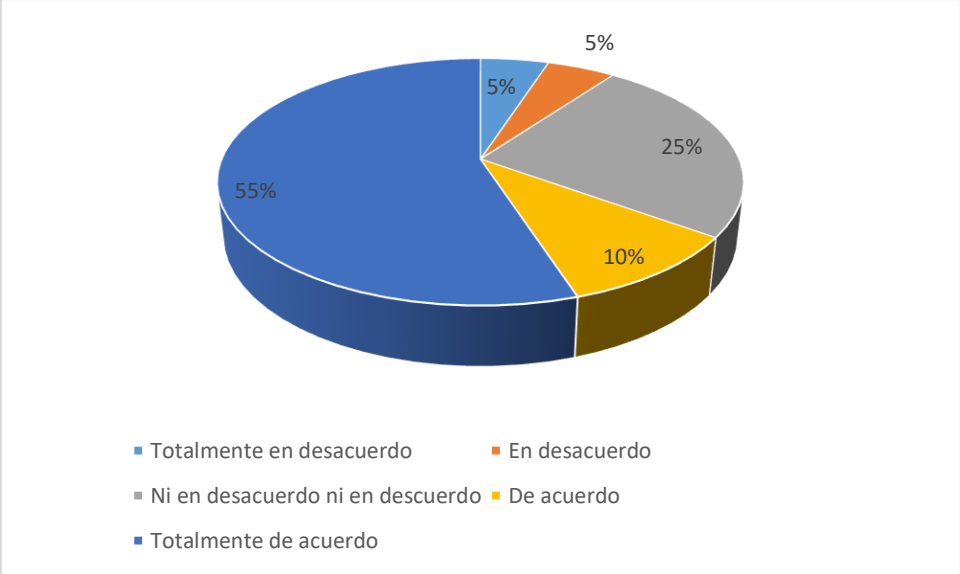
6. ¿Usted considera que se deberían estandarizar procesos técnicos para dar fiabilidad a la prueba digital en el sistema penal?

Tabla 7. Pregunta 6

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	1	5%
En desacuerdo	1	5%
Ni en desacuerdo ni en descuerdo	5	25%
De acuerdo	2	10%
Totalmente de acuerdo	11	55%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 7. Pregunta 6



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

El 55% de encuestados están totalmente de acuerdo con que consideran se debe estandarizar los procesos técnicos para dar fiabilidad a la prueba digital en el sistema penal, el

25% es neutro a esta idea, el 10% está de acuerdo con ello, el 5% está totalmente en desacuerdo, el 5% en desacuerdo.

Lo antes mencionado indica que, la mitad de encuestados están totalmente de acuerdo con que se debería estandarizar los procesos técnicos que den fiabilidad a la prueba digital en el sistema penal, y también hay un gran porcentaje de neutralidad en esta pregunta, lo cual debe solventarse a partir de la propuesta de estandarización de procesos técnicos de la prueba digital.

Pregunta N°. 7.

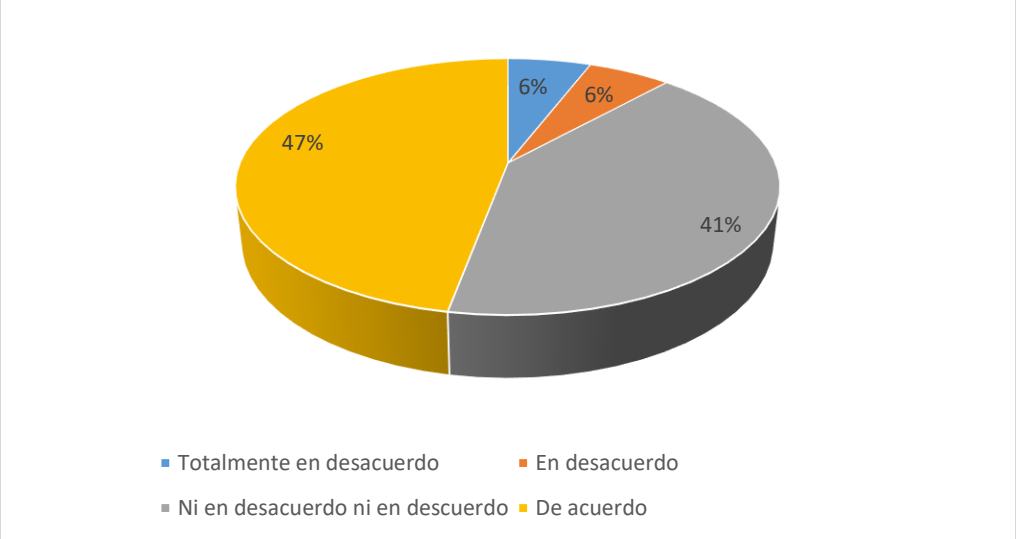
7. ¿En su práctica ha observado que la prueba digital ha sido excluida del proceso penal por omisiones en el manejo o en su obtención?

Tabla 8. Pregunta 7

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	1	5%
En desacuerdo	1	5%
Ni en desacuerdo ni en descuerdo	7	35%
De acuerdo	8	40%
Totalmente de acuerdo	3	15%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 8. Pregunta 7



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

De los encuestados, el 40% afirmó que está de acuerdo con que en la práctica continua ha verificado que la prueba digital ha sido excluida del proceso penal debido a omisión en el

manejo o manipulación o en la obtención de esta, el 35% es neutral a esta aseveración, el 15% está totalmente de acuerdo, el 5% está en desacuerdo y el otro 5% totalmente en desacuerdo.

Lo antes mencionado, afirma que la mayoría de actores del proceso penal creen en que en la práctica diaria la prueba digital se excluye del proceso penal por problemas en su obtención o manejo, algo que por supuesto debería cambiar para disponer de mayor veracidad de este tipo de evidencia en el proceso penal.

Pregunta N°. 8.

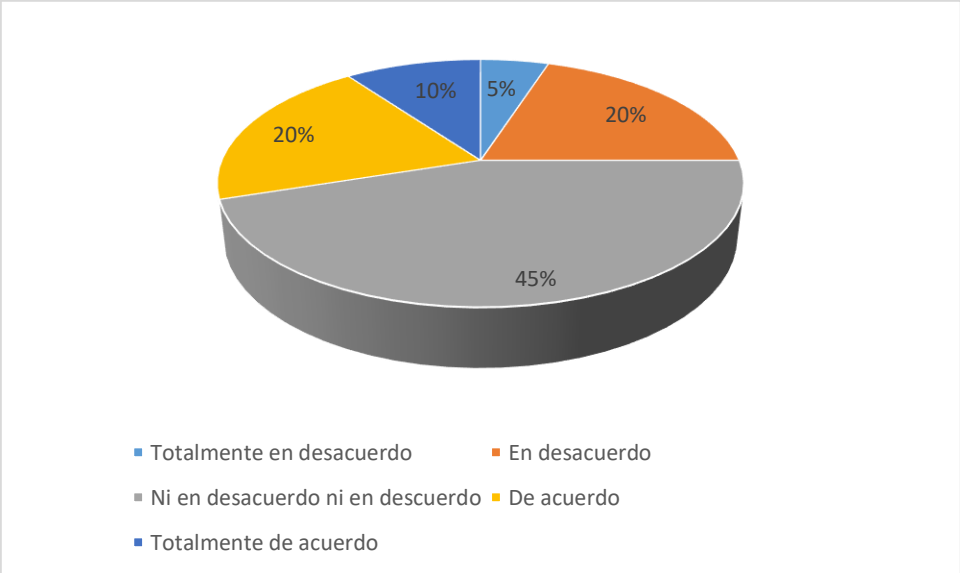
8. ¿La prueba digital es más objetiva e imparcial que la prueba tradicional en delitos comunes e informáticos?

Tabla 9. Pregunta 8

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	1	5%
En desacuerdo	4	20%
Ni en desacuerdo ni en descuerdo	9	45%
De acuerdo	4	20%
Totalmente de acuerdo	2	10%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 9. Pregunta 8



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 45% indicó ser neutral a la idea de que la prueba digital es más objetiva e imparcial que la prueba tradicional en delitos comunes o que tienen que ver con elementos informáticos, el 20% está en desacuerdo, el 20% de acuerdo, el 10% totalmente de acuerdo y el 5% totalmente en desacuerdo.

Lo antes mencionado ratifica que la mayoría de actores del proceso penal indican ser neutrales sobre el hecho de que la prueba digital es más objetiva que la prueba tradicional en delitos comunes o informáticos, ya que todavía existe escepticismo en su aplicación.

Pregunta N°. 9

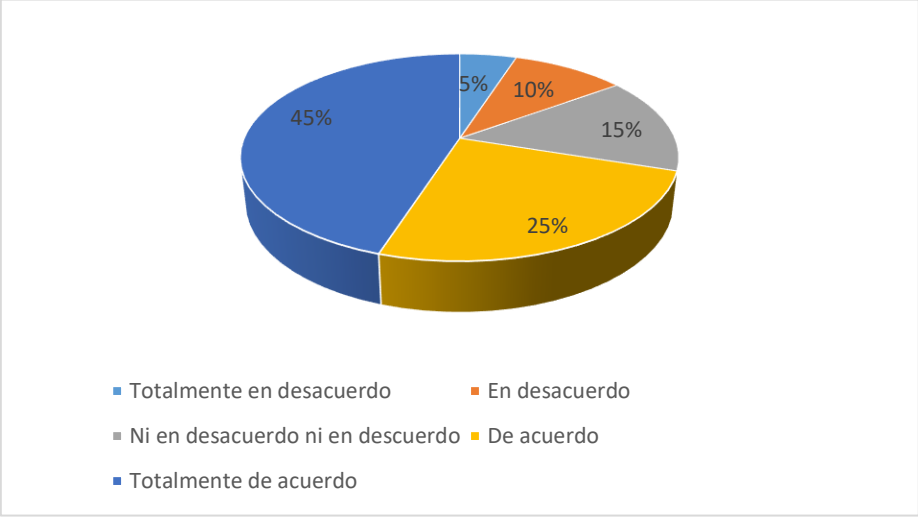
9. ¿La aplicación de normativa internacional permitiría el mejor tratamiento de la prueba digital en Ecuador?

Tabla 10. Pregunta 9

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	1	5%
En desacuerdo	2	10%
Ni en desacuerdo ni en descuerdo	3	15%
De acuerdo	5	25%
Totalmente de acuerdo	9	45%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 10. Pregunta 9



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de los encuestados, el 45% indicó que está totalmente de acuerdo con que la aplicación de la normativa internacional ayudará a un mejor tratamiento de la prueba digital en Ecuador, el 25% está de acuerdo, el 15% es imparcial, el 10% está en desacuerdo, el 5% está totalmente en desacuerdo.

Lo dicho indica que, la mayoría de penalistas, jueces, peritos encuestados están totalmente de acuerdo con la aplicación de la norma internacional que puede aportar a tratar mejor la prueba digital en el Ecuador.

Pregunta N°. 10

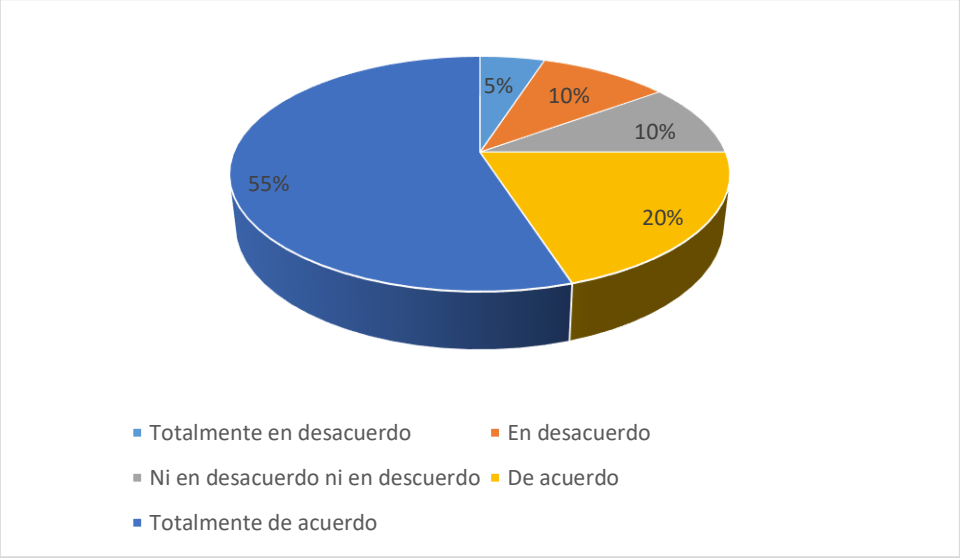
10. ¿Usted considera que se debe ejecutar una reforma que regularice la fiabilidad de la prueba digital en el país?

Tabla 11. Pregunta 10

DETALLE	FRECUENCIA	PORCENTAJE
Totalmente en desacuerdo	1	5%
En desacuerdo	2	10%
Ni en desacuerdo ni en descuerdo	2	10%
De acuerdo	4	20%
Totalmente de acuerdo	11	55%
TOTAL	20	100%

Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Figura 11. Pregunta 10



Fuente: Jueces, fiscales, peritos y abogados de Chimborazo.

Del total de encuestados, el 55% está totalmente de acuerdo con que considera que se debe ejecutar una reforma que regularice la fiabilidad de la prueba digital en el Ecuador, el 20% está de acuerdo, el 10% en desacuerdo, el 10% neutro y el 5% está totalmente en desacuerdo.

Lo antes mencionado indica que, la mayor parte de encuestados están totalmente de acuerdo en que si se debe hacer reformas que regulen la confiabilidad de la prueba digital en el Ecuador, algo que debe ser parte de la inclusión de mejoras para considerar a la evidencia digital como un elemento apto en el proceso penal.

4.2 Discusión de resultados

De acuerdo a los resultados arrojados indican que la prueba digital constituye un elemento clave en el proceso judicial penal del Ecuador, sobre todo en cuanto al ámbito que permite la valoración de la misma, pues de ello depende la toma de decisiones de los jueces y de fiscalía en la etapa de investigación. A su vez esto lo confirma Ormazábal (2018) en cuanto a que la prueba representa la clave de todo por proceso judicial, de tal forma que se garantice su valoración adecuada para conocimiento de la verdad procesal, Tomando en cuenta su proceso de obtención, preservación y mantenimiento para formar parte de la evidencia como tal.

Uno de los problemas que se evidenciaron es que existe limitada capacitación técnica y jurídica de los actores jurídicos en cuanto a la manipulación y observancia de la evidencia digital, lo que se relaciona con lo dicho por Molina (2021) quien ratifica que la falta de conocimiento en la utilización de la información no permite la adecuada valoración probatoria y esto a su vez puede influir en la eficacia de todo el proceso penal, ya que la falta de formación técnica aumenta la posibilidad de cometimiento de errores o no adecuado uso de las pruebas digitales, lo que podría dar paso a la falta de valor jurídico.

En cuanto al problema planteado inicialmente y de los resultados arrojados por las encuestas se concluye que existe una discusión real referente a la ausencia técnica y jurídica que afectan la autenticidad y fiabilidad de la evidencia digital, además, de elementos sustanciales y directrices específicas que coadyuben a la obtención de indicios que posteriormente determinen si existe o no un delito o infracción penal. Asimismo, es preciso señalar que es imperativo añadir y utilizar normativa internacional que ayude a la resolución de controversias en el ámbito jurídico.

Esto se observa como uno de los retos en cuanto a que los juristas no siempre disponen de la capacitación en términos técnicos y legales en cuanto a cómo manejar la evidencia digital, de igual forma esto tiene que ver con lo dicho por Ormazábal (2018) quien indica que, en el mundo complejo de hoy, se requiere que los actores de justicia dispongan de las competencias pertinentes para prevenir posibles manipulaciones innecesarias o no aptas en cuanto a dar validez probatoria, pues cuando no existe una formación adecuada, puede que esto incida en la falta de cumplimiento de principios mínimos en el proceso jurídico penal, entre ellos está el debido proceso y la tutela efectiva.

Anna et al., (2023) indica que, toda prueba debe cumplir con los principios de legalidad, pertinencia y autenticidad para la correcta convicción judicial, es por esto que, en el campo digital al tener mayor oportunidad de manipular la información podría resultar complejo cumplir con estos requerimientos porque podría generarse con mayor facilidad la alteración, manipulación o pérdida de la información.

Sin embargo, no existen actualmente protocolos estándar para el adecuado uso de la evidencia digital, lo cual es una situación negativa que perjudica la consistencia del sistema jurídico ecuatoriano, lo que coincide con lo dicho por De la Torre et al., (2024) quienes afirman que la evidencia digital por su naturaleza, necesita la instauración de la normativa técnica adaptada a este aspecto, que es la ISO/ICE 27037:2012 que da la garantía de la autenticidad de la misma. Tomando en cuenta que, cuando no hay normas claras puede perjudicar también la veracidad de la cadena de custodia.

Además, en los resultados se puede observar que, en el campo legal nacional, si existe reconocimiento de los medios electrónicos como parte de la prueba, que se materializan en el COIP, sin embargo, en el momento de la aplicación todavía se verifican vacíos legales y falta de una adecuada interpretación. Lo cual requiere que como dice Anna et al., (2023) sea valorado con criterio racionales y adaptándose al entorno nacional y tecnológico de la actualidad. También lo ratifica Álvarez (2025) quien destaca que la falta de regularización reduce la veracidad de las firmas digitales, metadatos y formatos digitales en el campo penal.

Por lo tanto, es necesario entender que, la evidencia digital hoy requiere mejor trato en cuanto a acudir a protocolos estandarizados propuestos a nivel internacional para que alcance su nivel probatorio de acuerdo a los alcances tecnológicos y jurídicos pertinentes y como parte del proceso penal en Ecuador.

Además, tomando en cuenta que, los resultados alcanzados, identifican que la evidencia digital actualmente constituye un mecanismo fundamental para el esclarecimiento de los hallazgos de un proceso penal, pero su uso depende de la correcta integración entre la norma, capacitación de los operadores de justicia y la aplicación efectiva de los protocolos técnicos para facilitar su veracidad y viabilidad, tomando en cuenta que se requiere fortalecer el marco legal ecuatoriano al respecto, implementar también protocolos estándar y la promoción de la capacitación continua sobre manejo de evidencia digital por los operadores de justicia, fomentando el adecuado proceso y la valoración óptima de la prueba.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se determinó que la evidencia digital goza de reconocimiento y eficacia probatoria dentro de los procesos penales ecuatorianos, debido a que, se encuentra positivada por el ordenamiento jurídico nacional como un medio de prueba admisible. No obstante, se ha logrado identificar barreras vinculadas con la ausencia de directrices específicas y estandarizadas para su correcta obtención, preservación y valoración, que producen dificultades interpretativas y criterios disimiles en su aplicación dentro de la sustanciación de un procedimiento judicial.
- Se dedujo que uno de los obstáculos más trascendentes para garantizar la autenticidad y fiabilidad de la evidencia digital reside en la insuficiencia de protocolos direccionados en la capacitación técnica y jurídica de quienes dirigen la investigación apoyados por la Policía Judicial y los peritos expertos en recolectar los indicios. Esta situación incide de manera desproporcional en las fases de recopilación, obtención, custodia, análisis y posteriormente a la valoración de la prueba digital, afectando en gran medida la eficacia probatoria de estos elementos, lo cual limita la tutela judicial efectiva y el debido proceso dentro de los procesos penales.
- En definitiva, se concluyó, que el cumplimiento estricto de la cadena de custodia y la implementación de procedimientos técnicos tanto nacionales como internacionales constituyen factores necesarios e imprescindibles para asegurar la integridad, autenticidad y fiabilidad de la evidencia digital. Además, se observó que el fortalecimiento de estos protocolos y mecanismos consolidan una práctica efectiva y homogénea en la administración de justicia, fomentando una mayor eficacia en la resolución de conflictos penales dentro del contexto jurídico-tecnológico.

5.2 Recomendaciones

- Se sugiere enfáticamente fortalecer el marco normativo y técnico procedimental aplicable a la evidencia digital dentro de los procesos penales en el Ecuador, a través de actualizaciones estándares de directrices relacionadas con su obtención, preservación, autentificación, incorporación y valoración. Esta medida permitirá garantizar la eficacia probatoria y admisibilidad de la prueba digital, en concordancia con los principios del debido proceso y la seguridad jurídica.
- Se recomienda reforzar la infraestructura tecnológica que se desprende de la investigación penal, mediante la implementación de herramientas digitales forenses especializadas para la identificación, recuperación y conservación de evidencia digital. La aplicación de tecnologías avanzadas en informática forense posibilitara la optimización de los procedimientos investigativos, mejorando la precisión en el tratamiento de indicios digitales y garantizar una mayor autenticidad de la evidencia y elementos probatorios practicados dentro del proceso penal.
- Como proyección de este estudio, se propone impulsar la trascendencia interdisciplinaria entre las ciencias jurídicas, la informática forense y las instituciones encargadas de la investigación penal, en concordancia de una idónea optimización digital de recursos especializados en la materia, permitiendo consolidar procedimientos homogéneos para el tratamiento de la evidencia digital, fortalecer la capacidad investigativa del sistema de justicia penal y responder de manera eficiente a los desafíos resultantes de la globalización tecnológica en el ámbito jurídico.

BIBLIOGRAFÍA

Adrianna, L. V. (2013). *La Guerra Inexistente, la Ciberguerra.* Madrid: Académica Española.

Aguirre, J. (19 de julio de 2001). *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI*. Recuperado el 12 de septiembre de 2016, de https://pendientedemigracion.ucm.es/info/especulo/numero27/cibercom.html

Álvarez, A. (2025). *Desafios de la prueba digital en el proceso penal.* https://ciencialatina.org/index.php/cienciala/article/view/21212: Universidad Estatal Península de Santa Elena.

Anna, T. D., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The Chain of Custody in the Era of Modern Forensics: From the Classic Proccedures for Gathering Evidence to the New Challenges Related to Digital Data. *Healthcare, 11 (5), 634*, https://doi.org/10.3390/healthcare11050634.

Avemañay, S., Avemañay, A., & Duarte, M. (2025). *La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica.* DOI: https://doi.org/10.37811/cl_rcm.v9i6.21212: Ciencia Latina Revista Multidisciplinar, Vol. 9, Núm. 5.

Avenmañay, S., Avemañay, A., & Duarte, M. (2025). La prueba digital en el proceso penal ecuatoriano, desafíos constitucionales, técnicos y comparados frente a los estándares iberoamericanos de evidencia tecnológica. *Ciencia Latina, vol. 9, núm. 5*, DOI: https://doi.org/10.37811/cl_rcm.v9i6.21212.

Balla, F., Granja, F., & Freire, E. (2024). *Principios de oportunidad y contradicción de la prueba en las garantías jurisdiccionales en Ecuador.* https://doi.org/10.33996/revistalex.v7i26.230: Revista Lex, 7 (26), 1063-1083.

Blázquez, F. (2001). *Sociedad de la Información.* Mérida: Junta de Extremadura.

Cabanellas de Torres, G. (1993). *DICCIONARIO JURIDICO ELEMENTAL* . Buenos Aires: EDITORIAL HELIASTA S.R.L.

Carbonell, M. (2021). *Derechos fundamentales y prueba digital en el proceso penal.* Tirant to Blanch.

Carreno, S. (2018). *Aplicación de la tecnología 3D al estudio de las huellas dactilares antiguas. Club de Ciencias Forenses.* https://evidentiauniversity.com/blogs/es/clubforenses/aplicacion-de-la-tecnologia-3d-al-estudio-de-las-huellas-dactilares-antiguas-club-de-ciencias-forenses/: Evidentia University.

Casey, E. (2020). *Digital evidence and computer crime.* Academic Press.

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito: COIP.

Código Orgánico Administrativo COA. (2017). *Registro Oficial N°. 31.* https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/11/COA.pdf: Asamblea Nacional.

Código Orgánico General de Procesos. (2018). *Código Orgánico General de Procesos.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Org%C3%A1nico-General-de-Procesos.pdf: COGEP.

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito: Asamblea Constituyente.

Computer fornesics. (2026). Por qué la evidencia digital es importante para la defensa legal. *Computer Forensicslab*, https://computerforensicslab.co.uk/digital-evidence-matters-legal-defence/?utm_source=chatgpt.com.

Consejo de Europa. (2001). *Convenio sobe la ciberdelincuencia* . COnvenio de Budapest.

Constitución del Ecuador. (2008). *Constitución del Ecuador.* Montecristi: Asamblea Constituyente.

Coronel, J., & Arguello, E. (2025). Análisis forense digital: la eficacia de la legislación ecuatoriana ante el cibercrimen. *Polo del Conocimiento, Vol. 10. N°. 11*, DOI: 10.23857/pc.v10i11.10748.

Coronel, J., & Arguello, E. (2025). Análisis forense digital: la eficacia de la legislación ecuatoriana ante el cibercrimen. *Polo del Conocimiento, Vol. 10, N°. 11*, DOI: 10.23857/pc.v10i11.10748.

Costas, J. (2010). *Seguridad Informática.* Madrid: RA-MA.

De la Corte Ibáñez, L., & Blanco Navarro, J. (2014). *Seguridad nacional, amenazas y respuestas.* LID: Milán.

De Miranda Vázquez, C. (2015). Prueba directa vs. Prueba indirecta (un conflicto inexistente). *Doxa. Cuadernos de Filosofía del Derecho.*, 76.

Delgado, A. (14 de noviembre de 2014). *Gobernanza de Internet en Ecuador: infraestructura y acceso.* Recuperado el 15 de septiembre de 2016, de Encuentro Nacional de Gobernanza de Internet en Ecuador: http://delgado.ec/research/es/Gobernanza_Internet_Ecuador_2014.pdf

Dulaney, E. (2011). *Seguridad Informática.* Madrid: ANAYA MULTIMEDIA.

Echandia, H. D. (2012). *Compendio de la Prueba Judicial* . Buenos Aires : RUBINZAL - CULZONI EDITORES.

Echeverría, E., & Álvarez, M. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. Una revisión sistemática. *Investigaciones Estudios Empíricos, vol. 9, núm. 6*, https://www.593dp.com/index.php/593_Digital_Publisher/article/view/2775.

Enghelberg, H. (2003). *Ciberterrorismo: Ciberguerra, Infoguerra, Cyberterrorismo.* Munich: Enghelberg.

Espinoza, A. (2024). La neurodidáctica para desarrollar la atención en niños de primer año de educación básica de la Unidad Educativa Vigotsky. *Universidad Nacional de Chimborazo*, http://dspace.unach.edu.ec/bitstream/51000/13233/1/Espinoza%20G%2C%20Ana%20

G.%282024%29.%20La%20nuerodid%C3%A1ctica%20para%20desarrollar%20la%20atenci%C3%B3n%20en%20ni%C3%B1os.pdf.

Firtman, S. (2005). *Seguridad Informática; las amenazas y vulnerabilidades más peligrosas, al desnudo.* Buenos Aires: MP Ediciones.

Geek. (2024). *Según la IA las huellas dactialres no son únicas.* https://estacionk2.com/segun-la-ia-las-huellas-dactilares-no-son-unicas/#:~:text=El%20sistema%20de%20IA%20puede%20servir%20para%20m%C3%A1s%20investigaciones&text=Sugieren%20que%20el%20sistema%20basado,dedos%20distintos%20a%20los%20archivados.

Gorphe, F. (2023). *Apreciación judicial de las pruebas.* Ediciones Olejnik.

Guglieri, C. (1997). *Reingeniería y Seguridad en el Ciberespacio.* Madrid: Díaz de Santos S.A.

id3 Technologies. (2020). *id Technologies*. Obtenido de https://id3technologies.com/fingerprint-recognition/#:~:text=Fingerprint%20recognition%20technology%20is%20an,on%20their%20unique%20fingerprint%20patterns.

Interpol. (2020). *Aspectos científicos de la dactiloscopía.* https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares#:~:text=Aspectos%20cient%C3%ADficos%20de%20la%20dactiloscopia&text=Adem%C3%A1s%2C%20no%20cambian%20a%20lo,arcos%2C%20curvas%20y%20espirales).: Interpol.

INTERPOL. (2020). *Huellas dactilares.* INTERPOL. España: INTERPOL.

ISO/IEC 27037. (2012). *Information technology — Security.* https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf.

Jones, S. (2022). El Ciberespacio como un entorno de interacciones. *Sello Editorial ESDE*, https://doi.org/10.25062/9786287602137.01.

Labadía, J. (2019). *Comentario a la sentencia absolutoria del fundador de seriesyonkis desde el prisma de los deltios contra la propiedad intelectual.* Diario la Ley (9528), 1.

Lessig, L. (2001). *El código y otras leyes del ciberespacio.* Madrid: Grupo Santillana.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2021). *Ley de Comercio Electrónico, Firmas y Mensajes de Datos.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf: Registro Oficial Suplemento 557.

Lidón, J. M. (2007). *Delito e informática: algunos aspectos.* Universidad de Deusto: Bilbao.

Luna Mora, H. G., & Toro Garzón, L. O. (2022). Prueba y verdad. Reflexiones desde la obra de Michele Taruffo. *Revista Temas Procesales* , 65.

Mendoza, M. (2024). Interpretación y desafíos de la evidencia digital en la investigación criminal. *Código Científico Revista de Investigación, 5 (E3), 480-498*, https://doi.org/10.55813/gaea/ccri/v5/nE3/328.

Molina, M. (2021). *Las tecnologías de la información y comunicación y la prueba en el proceso penal del Ecuador.* http://repositorio.ucsg.edu.ec/handle/3317/17113: Universidad Católica Santiago de Guayaquil.

Navas, E., & Vásquez, D. (2025). La importancia de la prueba digital en los procedimientos penales en Ecuador. *Polo del Conocimiento, 10 (4), 1745-1755*, https://www.polodelconocimiento.com/ojs/index.php/es/article/view/8778.

Ojeda, M. (2025). Evidencia tecnológica en el sistema judicial ecuatoriano: alcances normativos y desafíos en su implementación procesal. *Sociedad y Tecnología, 8 (4)*.

Pita, J. (2024). Análisis de vulnerabilidades y evidencia digital en servicios de nube. *Repositorio Digital UIDE*.

Ramírez, J. (2021). *Identificación de cadáveres y aplicaciones en radiología forense.* https://repository.unad.edu.co/handle/10596/44958: UNAD.

Rayón, M., & Gómez, J. (2014). *Cibercrimen: particularidades en su investigación y enjuiciamiento.* Madrid: AJEE.

Rosas, G., & Pila, G. (2023). *The protection of personal data in Ecuador: a historical-normative review of this fundamental right in the South American Country.* https://doi.org/10.37467/revvisual.v10.4568: Revista Internacional de Cultura Visual, 13 (2), 1-16.

Sánchez, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del siglo XXI. *CENIPEC*, 239-267.

Smith, M., & Kollock, P. (2003). *Comunidades en el ciberespacio.* Barcelona: UOC.

Suárez, A. (2015). *El quinto elemento: Espionaje, ciberguerra y terrorismo. Una amenaza real e inminente.* España: Grupo Planeta .

Taruffo, M. (2008). *La prueba.* Madrid: Marcial Pons.

Thales. (2021). *Sistema automatizado de identificación de huellas dactilares (AFIS) - una breve historia.* https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/biometria/historia-afis.

TN University. (2023). Errores comunes en la Auditoría Forense Digital. *TN University*, https://www.tnuniversity.edu.mx/editorial/articulo/errores-comunes-en-la-auditoria-forense-digital/?utm_source=chatgpt.com/.

Tomás, S. (2015). *Retos del Derecho ante las nuevas amenazas.* Madrid: DYKINSON.

Torre, M. d., Puertas, A., & Burbano, C. (2024). Manejo de la evidencia digital con visión en normas internacionales aplicables por los primeros interventores y peritos forenses en Ecuador. *Innovación y Saber, 4 (2), 39-52*, https://innovacionysaber.isupol.edu.ec/index.php/innovacion/article/view/280.

Universidad Técnica del Norte de Ibarra. (2020). *Investigación Forense Digital: análisis de evidencias electrónicas.* https://repositorio.utn.edu.ec/bitstream/123456789/17200/1/Investigaci%C3%B3n%20Forense%20Digital.pdf: UTN Ibarra.

Vatis, M. (2001). *Cyber attacks during the war on terrorism: a predictive analysis.* Hanover: Lyme Road.

Velasco, J., & Álvarez, P. (2022). Valoración judicial de la prueba digital y estándares forenses. *Revista de Derecho Penal y Criminología, 27 (2), 89-112*.

ANEXOS

Anexo 1. Formato de la encuesta a operadores de justicia

La siguiente es una encuesta que pretende identificar la percepción de los operadores de justicia (jueces, fiscales, peritos, abogados) acerca de cómo se ejecuta el tratamiento de la evidencia digital dentro del proceso penal en Ecuador, no se dará a conocer nombres, apellidos, teléfonos y otros datos personales de los encuestados para mantener el sigilo en la información, considerando que esta investigación se llevará específicamente al ámbito académico para la Universidad Nacional de Chimborazo.

Objetivo del instrumento: Identificar la percepción de los actores de justicia acerca de la fiabilidad, manipulación procesal y técnica de la evidencia digital en el proceso penal del Ecuador.

Instrucciones:

- Responder con una X en una sola opción por pregunta
- No tachar en más de una opción
- Ser lo más objetivos y sinceros posible
- Se aplica la siguiente escala de respuesta:

Totalmente en desacuerdo (1)
En desacuerdo (2)
Ni de acuerdo ni en desacuerdo (3)
De acuerdo (4)
Totalmente de acuerdo (5)

Tiempo estimado de respuesta: 7 minutos

Datos generales

Función profesional:
Juez ( )
Fiscal ( )
Perito ( )
Abogado ( )

Preguntas

Número	Detalle	1	2	3	4	5
1	¿Usted considera que la normativa legal en Ecuador se presenta de manera clara y precisa acerca de cómo tratar a la evidencia digital dentro del proceso penal?					
2	¿El COIP brinda los elementos propicios y suficientes para dar					

	garantía de la autenticidad de la prueba digital?					
3	¿En su cotidianidad profesional, ha verificado que hay protocolos estandarizados de tratamiento de evidencia digital?					
4	La cadena de custodia digital se respeta en las etapas diferentes del proceso penal					
5	¿Usted cree que los operadores de justicia tienen la capacitación necesaria en el ámbito procesal y técnico para la valoración de la evidencia digital?					
6	¿Usted considera que se deberían estandarizar procesos técnicos para dar fiabilidad a la prueba digital en el sistema penal?					
7	¿En su práctica ha observado que la prueba digital ha sido excluida del proceso penal por omisiones en el manejo o en su obtención?					
8	¿La prueba digital es más objetiva e imparcial que la prueba tradicional en delitos comunes e informáticos?					
9	¿La aplicación de normativa internacional permitiría el mejor tratamiento de la prueba digital en Ecuador?					
10	¿Usted considera que se debe ejecutar una reforma que regularice la fiabilidad de la prueba digital en el país?					

Anexo 2. Consentimiento Informado

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE CIENCIAS POLÍTICAS Y ADMINISTRATIVAS

CARRERA DE DERECHO

FORMULARIO DE CONSENTIMIENTO INFORMADO PARA PARTICIPANTES DE INVESTIGACIÓN

Título de investigación: Autenticidad y Fiabilidad de la evidencia digital en el proceso penal ecuatoriano.

Investigador principal: Brayan Alexander Cañizares Jácome (Estudiante de la carrera de Derecho)

Tutora: Dra. Rosita Elena Campuzano Llaguno.

Introducción:

Se le invita a participar en un proyecto de investigación académico realizado como trabajo de titulación precio a la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador por la Universidad Nacional de Chimborazo.

Objetivo del Estudio:

El objetivo principal de este instrumento es identificar la percepción de los actores de justicia (jueces, fiscales, peritos y abogados) acerca de la fiabilidad, manipulación procesal y fiabilidad de la evidencia digital en el proceso penal del Ecuador.

Procedimiento:

En caso de contar con su participación, se lo solicitará responder una encuesta. El cuestionario consta de 10 preguntas cerradas con una escala de respuesta tipo LIKERT (desde "totalmente en desacuerdo" hasta "totalmente de acuerdo"). El tiempo estimado para completar la encuesta es de aproximadamente 7 minutos.

Las preguntas abordarán temas como la claridad de la normativa actual, el respeto a la cadena de custodia digital, la capacitación de los operadores de justicia y la necesidad de aplicar normativas externas referente al tratamiento de la evidencia digital.

Voluntariedad:

Su participación en este estudio es estrictamente voluntaria. Usted tiene el derecho de negarse a participar o de retirar su consentimiento y suspender su participación en cualquier momento, sin que ello acarree ningún perjuicio en su desempeño profesional o relación con la Universidad.

Riesgo y beneficio:

No se prevén riesgos físicos ni legales por su participación. El beneficio principal es de carácter académico, contribuyendo a la generación de conocimiento sobre falencias normativas y técnicas que afecten la valoración probatoria digital, con miras a fortalecer la administración de justicia.

Confidencialidad:

Se garantiza la absoluta confidencialidad y el anonimato de sus respuestas. Además, no se solicitarán ni dirán a conocer nombres, apellidos, números de teléfono u otros datos personales específicos que permitan su identificación.

Los datos recopilados se utilizarán exclusivamente con fines académicos y de investigación para la Universidad Nacional de Chimborazo.

Contactos:

Si usted tiene alguna pregunta sobre este proyecto, puede contactar al investigador principal Brayan Alexander Cañizares Jácome, o a la tutora, Dra. Rosita Elena Campuzano Llaguno, a través de la Universidad Nacional de Chimborazo en la facultad de Ciencias Políticas y Administrativas de la carrera de Derecho.

Declaración de consentimiento:

He leído la información proporcionada anteriormente.

He tenido la oportunidad de hacer preguntas y mis preguntas han sido respondidas satisfactoriamente.

Consiento voluntariamente participar en este estudio bajo las condiciones de confidencialidad mencionadas.

Al marcar la opción "SI" a continuación se procederá a completar la encuesta adjunta, certifico que soy mayor de edad, que actúo como funcionario de la función judicial, fiscalía o abogado en libre ejercicio (Juez, Fiscal, Abogado o Perito) y que otorgo mi consentimiento libre e informado para participar en esta encuesta y proporcionar mis conocimientos en favor de la investigación.

Si, acepto participar voluntariamente ( )

No acepto participar ( )

Fecha: _____ de _____ de 20___