UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE CIENCIAS JURÍDICAS,

CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Tesis

Análisis del tratamiento de la evidencia digital en el proceso penal peruano

Asesor:

Mag. Kádagand Venero, Liliana

Autor:

Grajeda Farfán, Wilfredo

Para optar al Título Profesional de:

Abogado

Cusco - Cusco - Perú

2026

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE CIENCIAS JURIDICAS CONTABLES Y SOCIALES

ESCUELA PROFESIONAL DE DERECHO

Acta N°: 090-2026

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL

En la ciudad de Cusco, a los 15 días del mes de junio del 2026, siendo las 9:10 horas, se reunieron los integrantes del Jurado designado por Resolución Sub Directoral N° 483-2026-UTEA-F02-FCJCS-EPD de la Escuela Profesional de Derecho, Facultad de Ciencias Jurídicas Contables y Sociales:

Presidente	:	Dra. Rodriguez Ayerbe, Kathie
Dictaminante	:	Mgt. Saire Marcavillaca, Julio
Replicante	:	Dr. Jayo Silva, Carlos Eduardo

Para evaluar la sustentación, en la modalidad de:

☒ Tesis ☐ Trabajo de suficiencia profesional

Titulada:

Análisis del tratamiento de la evidencia digital en el proceso penal peruano

Desarrollado por el (los) Bachiller (es):

Br.: Grajeda Farfan, Wilfredo
(Apellidos y Nombres)

Br.: _____
(Apellidos y Nombres)

Para optar el Título Profesional de:

Abogado(a)
(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) (los) mencionado(a) (s) bachiller (es) fue (ron) APROBADO (S) ☒ o DESAPROBADO (S) ☐:

Emitiéndose el calificativo final de:

Bachiller (Apellidos y Nombres)	Nota	Detalle (**)
Br. Grajeda Farfan, Wilfredo	15	Aprobado

Siendo las 10:40 horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Dra. Rodriguez Ayerbe, Kathie
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Dictaminante: Mgt. Saire Marcavillaca, Julio
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Replicante: Dr. Jayo Silva, Carlos Eduardo
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Nota: Desaprobado: 0-10; Aprobado: 11-20
(**): 0 a 10: Desaprobado, 11 a 15: Aprobado, 16 a 18: Aprobado Notable, 19 y 20: Aprobado con Distinción, Art. 18 RGGAT.

14% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

10% Fuentes de Internet
2% Publicaciones
11% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos

Datos del Autor		
Apellidos y nombres	:	Grajeda Farfan, Wilfredo
Tipo de documento de identidad	:	DNI
Número de Documento de Identidad	:	47282532
URL ORCID	:	https://orcid.org/0009-0007-6783-2919
Datos del Asesor		
Apellidos y nombres	:	Mag. Kádagand Venero, Liliana
Tipo de documento de identidad	:	DNI
Número de Documento de Identidad	:	40869945
URL ORCID	:	https://orcid.org/0000-0001-6584-9732
Datos de la Investigación		
Facultad	:	Facultad de Ciencias Jurídicas, Contables y Sociales
Escuela Profesional	:	Derecho
Línea de Investigación	:	Derecho, Privado y Público
Rango de año en que se realizó la investigación	:	Junio 2025 – mayo 2026
Fuente de financiamiento	:	Autofinanciado
Porcentaje de similitud	:	14%
URL de OCDE	:	https://purl.org/pe-repo/ocde/ford# 5.05.01

Dedicatoria

A mi madre, cuyo inquebrantable apoyo y ejemplo de fortaleza han sido el motor de mi vida; a mi hijo Stephano, mi fuente de inspiración y motivación principal; y a la memoria de mi padre, cuya guía y enseñanzas han persistido espiritualmente, dándome la fuerza para enfrentar cada obstáculo.

Finalmente, esta obra se dirige al progreso del Derecho Procesal Penal peruano. Confío en que este análisis sobre la evidencia digital fomente una aplicación legal más técnica y rigurosa en el entorno tecnológico actual.

Bach. Wilfredo Grajeda Farfán

Agradecimiento

Al Área de investigaciones de Ciberdelincuencia del Departamento de Investigación Criminal Cusco de la Policía Nacional del Perú (PNP), por los conocimientos adquiridos en la lucha frontal contra la cibercriminalidad en sus diferentes formas y modalidades.

Bach. Wilfredo Grajeda Farfán

Resumen

La investigación analiza de qué manera el inadecuado tratamiento de la evidencia digital genera dificultades en su obtención, conservación, análisis y admisibilidad dentro del proceso penal peruano, para ello adopta un enfoque cualitativo y un diseño dogmático-analítico, orientado al examen de los marcos normativos, principios jurídicos y criterios técnicos vinculados a la evidencia digital, por otra parte la información se recopiló mediante el análisis documental de legislación nacional y comparada, doctrina especializada e informes institucionales, complementándose con entrevistas a operadores del sistema de justicia y especialistas, asimismo su principal conclusión es que el inadecuado tratamiento de la evidencia digital dificulta significativamente su incorporación válida y eficaz en el proceso penal, afectando su credibilidad probatoria y el respeto de las garantías procesales, por ende estas deficiencias evidencian la necesidad de adecuar el sistema penal a la realidad tecnológica actual mediante reformas normativas y administrativas, así como el fortalecimiento de la capacitación especializada de los operadores de justicia. La recomendación se dirige al Ministerio de Justicia y Derechos Humanos, a fin de promover e implementar una reforma normativa y administrativa integral en materia de evidencia digital, con el propósito de establecer reglas procesales claras sobre su obtención, conservación, análisis y valoración, así como fortalecer la capacitación especializada y continua de los operadores de justicia.

Palabras clave: Evidencia, digital, proceso, penal, admisibilidad

Abstract

The study analyzes how the inadequate handling of digital evidence generates difficulties in its collection, preservation, analysis, and admissibility within the Peruvian criminal process. It adopts a qualitative approach and a dogmatic-analytical design, aimed at examining the regulatory frameworks, legal principles, and technical criteria related to digital evidence. The information was collected through documentary analysis of national and comparative legislation, specialized doctrine, and institutional reports, complemented by interviews with justice system operators and digital evidence specialists. Its main conclusion is that the improper handling of digital evidence significantly hinders its valid and effective incorporation into criminal proceedings, affecting its probative credibility and the protection of procedural guarantees. These deficiencies highlight the need to adapt the criminal justice system to the current technological reality through regulatory and administrative reforms, as well as by strengthening the specialized training of justice operators. The recommendation is addressed to the Ministry of Justice and Human Rights, with the aim of promoting and implementing a comprehensive regulatory and administrative reform in the field of digital evidence, in order to establish clear procedural rules for its collection, preservation, analysis, and evaluation, as well as to strengthen the specialized and continuous training of justice system operators.

Keywords: Evidence, digital, criminal procedure, admissibility

Índice

Índice de tablas

Índice de anexos

I. Introducción

El acelerado desarrollo de las tecnologías de la información y comunicación ha generado profundas transformaciones en las dinámicas sociales, económicas y jurídicas contemporáneas, en el ámbito penal estas innovaciones han impactado directamente en la forma de comisión de los delitos y en los medios utilizados para su esclarecimiento, dando lugar a la creciente relevancia de la evidencia digital como instrumento probatorio; dispositivos electrónicos, sistemas informáticos, redes sociales y plataformas digitales se han convertido en fuentes recurrentes de información para la investigación penal, lo que exige respuestas normativas y técnicas acordes con su naturaleza particular; en este escenario, la correcta obtención, conservación, análisis y valoración de la evidencia digital resulta determinante para garantizar procesos penales eficaces y respetuosos de los derechos fundamentales.

En el Perú, pese al reconocimiento formal de la prueba digital dentro del proceso penal, su tratamiento normativo y práctico presenta serias limitaciones, ya que la ausencia de una regulación específica y sistemática, así como la aplicación de criterios probatorios tradicionales concebidos para la evidencia física, han generado vacíos legales, interpretaciones dispares y prácticas inconsistentes entre los operadores de justicia; estas deficiencias se ven agravadas por la insuficiente capacitación especializada de jueces, fiscales, efectivos policiales y peritos, lo que incide negativamente en aspectos esenciales como la cadena de custodia, la autenticidad, la fiabilidad y la admisibilidad de la evidencia digital, comprometiendo principios fundamentales como el debido proceso, la seguridad jurídica y la búsqueda de la verdad

material; en este contexto, la presente investigación titulada “Análisis del tratamiento de la evidencia digital en el proceso penal peruano” tiene como finalidad analizar de qué manera el inadecuado tratamiento de la evidencia digital genera dificultades en su obtención, conservación, análisis y admisibilidad dentro del proceso penal; a través de un enfoque cualitativo y un tipo de investigación dogmático-analítico, se examinan los marcos normativos vigentes, la doctrina especializada y las prácticas judiciales, complementadas con entrevistas a operadores del sistema de justicia, de modo que el estudio busca identificar los principales vacíos y deficiencias normativas y operativas, así como proponer lineamientos que contribuyan a fortalecer un tratamiento legítimo, confiable y eficaz de la evidencia digital, en armonía con los estándares internacionales y la realidad del sistema de justicia penal peruano, con especial atención a la experiencia de la Corte Superior de Justicia del Cusco. amplia.

Asimismo, la creciente utilización de tecnologías digitales en la comisión e investigación de delitos ha evidenciado la necesidad de adaptar los mecanismos procesales tradicionales a las nuevas exigencias de la era digital. La naturaleza intangible, volátil y fácilmente modificable de la evidencia digital plantea desafíos particulares para su preservación y valoración probatoria, requiriendo la aplicación de procedimientos técnicos especializados que permitan garantizar su integridad y confiabilidad.

En consecuencia, la ausencia de criterios uniformes para su tratamiento no solo dificulta la actividad probatoria dentro del proceso penal, sino que también puede generar cuestionamientos respecto de la legitimidad de las decisiones judiciales sustentadas en este tipo de evidencia.

Este informe de investigación está conformado por cinco capítulos, de acuerdo con la norma establecida por la Universidad Tecnológica de los Andes, así se tiene:

Capítulo I: Introducción: En este apartado se menciona el contexto general del problema, se destaca su importancia jurídica. Se analiza la situación actual del fenómeno, y se identifican los vacíos normativos que justifican la investigación. Además, se aborda la pertinencia del estudio.

Capítulo II: Planteamiento del problema: Está dedicado a la formulación del problema de investigación, contienen la descripción de la realidad problemática, asimismo se presentan los objetivos que orientan el trabajo.

Asimismo, comprende la justificación y las categorías o temas eje de análisis.

Capítulo III: Marco teórico: Este apartado es el fundamento doctrinario de la investigación, comprende la revisión de los antecedentes de estudio, tanto nacionales como internacionales, que permiten situar el problema en su contexto histórico y jurídico.

Asimismo, comprende el desarrollo de las bases teóricas, que integra doctrina especializada, jurisprudencia y normativa.

Además, presenta la definición de los conceptos clave para evitar ambigüedades y asegurar precisión terminológica, para fortalecer la validez científica del estudio.

Capítulo IV: Metodología: En este capítulo se presenta el diseño metodológico utilizado, se especifica el tipo y nivel de investigación, el enfoque cualitativo adoptado, el ámbito temporal y espacial, la población y muestra, así como los instrumentos de recolección de datos.

Asimismo, se presentan los procedimientos y técnicas de análisis utilizados para garantizar la validez y confiabilidad de los resultados.

Finalmente, se incluyen las consideraciones éticas necesarias para asegurar el respeto a los principios de integridad académica.

Capítulo V: Resultados y discusión: Expone los hallazgos obtenidos a partir del análisis documental y fáctico, que abarca la normativa vigente, doctrina especializada, la discusión crítica, la detección de vacíos legales y los retos prácticos. Este análisis permitió elaborar conclusiones objetivas y formular recomendaciones bien fundamentadas.

II. Planteamiento del problema

2.1. Descripción y formulación del problema

A nivel mundial, el crecimiento acelerado de las Tecnologías de Información y Comunicación, junto con el alto grado de conectividad, ha cambiado la manera en que opera la delincuencia y también cómo se recogen las pruebas. De hecho, al investigar delitos, ya sean cibernéticos o formas más tradicionales de criminalidad apoyadas por la tecnología, las pruebas digitales se han convertido en un elemento clave. Los sistemas jurídicos de países como Colombia, México y España han adaptado sus marcos legislativos a estos cambios en el proceder de la ciberdelincuencia, estableciendo procesos que permitan salvaguardar las pruebas digitales y garantizar su autenticidad, trazabilidad e integridad a lo largo de su cadena de custodia.

En el Perú, la prueba digital en los juicios penales está reconocida legalmente, sin embargo su implementación está muy por detrás de los estándares internacionales. Surgen problemas de debido proceso debido a una regulación fragmentada y a la falta de protocolos técnicos estandarizados; la falta de previsibilidad jurídica socava la integridad de las pruebas; y los actores del sistema de justicia están en desacuerdo entre sí debido a la falta de alineación legislativa del Código de Procedimiento Penal con instrumentos como el Convenio de Budapest; la vulneración de derechos fundamentales como la intimidad o el derecho a la defensa, incluso la afectación del principio de verdad material y justicia penal efectiva.

En el sistema de justicia de nuestra región, ya sean los magistrados del distrito judicial de Cusco, Distritos Fiscales, personal policial de las oficinas de investigación de la REGPOL PNP Cusco, abogados defensores y procuradores tiene esta problemática del correcto tratamiento de la evidencia digital para ello es urgente realizar un análisis crítico y propositivo del marco normativo vigente y de las prácticas judiciales en torno al tratamiento de la evidencia digital. La presente investigación tiene como finalidad identificar los principales vacíos y deficiencias tanto normativas como operativas, y proponer mejoras o lineamientos que permitan fortalecer el tratamiento legítimo, confiable y eficaz de la prueba digital dentro del proceso penal peruano, asegurando la observancia irrestricta de los derechos fundamentales de las partes en litigio.

2.1.1 Problema general

¿De qué manera el tratamiento práctico de la evidencia digital en el proceso penal peruano garantiza su eficacia probatoria?

2.1.2 Problemas específicos

-¿Cuáles son las características particulares de la evidencia digital que exigen un tratamiento diferenciado respecto a la evidencia física en el proceso penal?

-¿Cómo afecta la falta de capacitación de jueces, fiscales y policías en el tratamiento de evidencia digital al desarrollo eficaz del proceso penal?

2.2. Objetivos

2.2.1. Objetivo general

Analizar de qué manera el inadecuado tratamiento práctico de la evidencia digital en el proceso penal genera dificultades en su obtención, conservación, análisis y admisibilidad dentro del proceso penal.

2.2.2. Objetivos específicos

-Precisar cuáles son las características particulares de la evidencia digital que exigen un tratamiento diferenciado respecto a la evidencia física en el proceso penal.

-Examinar cómo afecta la falta de capacitación de jueces, fiscales y policías en el tratamiento de evidencia digital al desarrollo eficaz del proceso penal.

2.3. Justificación e importancia

Justificación teórica

Este estudio refuerza y amplia el conocimiento jurídico acerca del tratamiento de las pruebas digitales en el sistema de justicia penal peruano, una zona en la que la teoría jurídica nacional adolece de una sistematización. Siendo el fin comprender de mejor manera las pruebas digitales en el contexto del debido proceso, para lo cual la tesis analiza críticamente conceptos, principios y categorías. Asimismo, se explica su naturaleza jurídica, sus criterios de validez y sus limitaciones, lo que posibilita la mejora del discurso académico.

Justificación práctica

En el aspecto práctico el estudio se justifica debido a que se centra en los retos a los que se enfrentan los profesionales del sistema de justicia penal en lo que respecta a la admisión, la evaluación y la supervisión de las pruebas digitales. Los resultados exponen las deficiencias

del sistema judicial, la policía y la fiscalía, y ofrecen sugerencias sobre cómo lograr que las pruebas sean más convincentes y menos propensas a ser desestimadas en los tribunales.

Justificación metodológica

El método y el enfoque cualitativo aplicado al derecho permiten una comprensión integral del tema objeto de estudio y ofrece un marco de investigación reproducible para futuros estudios sobre pruebas digitales y otras formas complejas de la actividad probatoria en el derecho penal.

Justificación social

La tesis presenta importancia social, debido a que se orienta a la protección de derechos fundamentales, como el derecho a la defensa, la presunción de inocencia y el debido proceso, en el ámbito relacionado con el manejo de las pruebas digitales. En efecto al definir criterios que refuerzan la credibilidad y la validez de este tipo de pruebas, el estudio propone una mejora en la transparencia y la eficiencia de la administración de justicia, satisfaciendo las necesidades de una sociedad digital.

Justificación normativa

Este estudio contribuye a determinar si es necesario introducir modificaciones en la normativa o en las interpretaciones para establecer normas más claras y coherentes en materia de pruebas digitales y determinar en qué medida se ajusta a las normas internacionales y a los principios constitucionales, así como identificar posibles vacíos, ambigüedades u otras deficiencias.

2.4. Hipótesis

No corresponde

2.5. Categorías

Categoría 1

La evidencia digital

Sub categorías

-La autenticidad de la evidencia digital.

-La integridad y la conservación de la evidencia digital

-La cadena de custodia digital

-La naturaleza indiciaria de la prueba digital

-Pertinencia probatoria de la evidencia digital

- Relevancia probatoria de la evidencia digital

Categoría 2

Sub categorías

El proceso penal peruano

-Admisibilidad de la evidencia digital

-Valoración judicial de la prueba digital

-Garantías del debido proceso

-Principio de proporcionalidad en la obtención probatoria

-Seguridad jurídica en el proceso penal

III. Marco Teórico

3.1. Antecedentes

3.1.1 A nivel internacional

Layana (2023), en la investigación denominada “El tratamiento de la evidencia digital en el proceso penal y la motivación de las decisiones judiciales de acuerdo con la ley y el derecho a la defensa”, sustentada para optar por el grado académico de maestro en la Universidad Central del Ecuador, la metodología utilizada fue de enfoque cualitativo, con un diseño dogmático-analítico y socio jurídico, empleando técnicas de análisis documental y entrevistas a operadores del sistema de justicia; se concluyó que la pandemia de COVID-19 ha acelerado el desarrollo de las tecnologías de la información y la comunicación, lo que ha situado a las pruebas digitales en el centro de los procesos judiciales. El derecho a la defensa se ve socavado en los tribunales ecuatorianos debido a la falta de uniformidad en la jurisprudencia y al continuo retraso normativo. Para colmo de males, el sistema judicial convencional simplemente no puede manejar los intrincados detalles de este tipo de pruebas. Según los entrevistados, hay una falta de normas doctrinales claras y una capacitación inadecuada entre los expertos legales. En consecuencia, el estudio destaca la necesidad de evaluar las pruebas digitales de acuerdo con los principios de legalidad, el razonamiento judicial y las normas internacionales de derechos humanos.

García (2023) su tesis “La incorporación de las pruebas digitales en el proceso penal acusatorio” en el marco de los estudios de posgrado para la obtención de la Maestría en la Universidad Autónoma de Guerrero. La metodología utilizada fue de enfoque cualitativo, con un diseño orientado al análisis jurídico de la inserción de los elementos materiales probatorios de naturaleza digital en el sistema de corte acusatorio y oral Mexicano, utilizando como método principal el dogmático jurídico, que permite interpretar, sistematizar y evaluar las normas contenidas en el Código Nacional de Procedimientos Penales; asimismo, se emplean métodos complementarios como el hermenéutico, empleando técnicas de análisis documental de legislación, doctrina y jurisprudencia, complementadas con el estudio de casos y el análisis de plataformas digitales. Concluyó que la creciente influencia de las tecnologías de la información y las redes sociales en los actos delictivos ha llevado a la conclusión de que las pruebas digitales deben ser admisibles. Las persistentes lagunas normativas en el ordenamiento jurídico mexicano ponen en peligro el debido proceso y la eficiencia de los procedimientos, y obstaculizan su uso efectivo. Las pruebas digitales obtenidas de plataformas como Instagram, WhatsApp o Facebook deben cumplir con las normas de legalidad, validez, conservación y cadena de custodia, teniendo en cuenta los aspectos técnicos únicos de cada red social.

Herrera (2023), en su estudio titulado “El papel de la prueba digital en los procedimientos penales en Ecuador”, examinó el rol de la prueba digital en los procesos penales ecuatorianos, enfocándose en su marco legal y desafíos principales. El método utilizado fue un diseño dogmático-analítico y comparado, usando las técnicas de análisis documental de normas, doctrina y jurisprudencia, así como el estudio de informes institucionales en relación con estándares internacionales. Sostiene que la falta de una norma específica, las limitaciones técnicas y la formación insuficiente del personal del sistema judicial limitan la evaluación y la admisión de las pruebas digitales, a pesar de que estas constituyen una parte esencial de la justicia penal, por ello la credibilidad, autenticidad e integridad de las pruebas digitales se ven

comprometidas. En consecuencia, se deben establecer normas para el manejo de estas pruebas, y el sistema legal debe armonizarse con los estándares internacionales.

Bujosa, et al. (2021) en su estudio titulado “La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia” para la Revista Brasileira de Direito Processual Penal, el cual hizo uso de un enfoque cualitativo, basado en el análisis de textos del ordenamiento jurídico español y colombiano relacionados con la prueba digital y la vigilancia secreta en el proceso penal; desarrolló una revisión de la jurisprudencia con la finalidad de identificar los riesgos y limitaciones de estas prácticas frente a los derechos fundamentales. La investigación sugiere que la ciberdelincuencia ha aumentado en la misma medida que la rápida expansión del panorama digital, lo que genera tensiones entre la necesidad de llevar a cabo investigaciones penales exhaustivas y la necesidad de proteger los derechos fundamentales de las personas acusadas. La vigilancia abierta mejorará las capacidades de investigación del sistema de justicia penal, el monitoreo oculto agrava las preocupaciones sobre la privacidad. Para finalizar el estudio sostiene que el equilibrio judicial entre pruebas digitales y protección de los derechos humanos se ve obstaculizado por las discrepancias normativas.

Eusebio (2020), en “La evidencia digital en el proceso penal de la provincia de Buenos Aires”, analizó el rol de la evidencia digital en el proceso penal bonaerense y la diferencia de la evidencia física evaluando su regulación desde la legislación comparada. El método utilizado tuvo un enfoque cualitativo, de tipo documental, con un diseño no experimental, basado en la revisión y análisis de fuentes bibliográficas especializadas, tales como textos jurídicos, estudios técnicos, normativa nacional e internacional y publicaciones académicas relacionadas con la evidencia digital. El sistema de justicia penal requiere una revisión completa a la luz de los avances tecnológicos pues la aplicación analógica de los conceptos jurídicos tradicionales vulnera derechos fundamentales, como el derecho a la privacidad.

Sostiene que ciertas normas permitirán que las investigaciones sean más transparentes y eficientes, sin dejar de proteger los derechos procesales, en cumplimiento de acuerdos internacionales como el Convenio de Budapest. A los efectos de evaluar las reformas legislativas en los contextos latinoamericanos, este caso ofrece criterios normativos y comparativos útiles.

3.1.2. A nivel nacional

Julca et al. (2025), en el artículo "El reto de la ciberjusticia: criterios de valoración de la prueba digital en el Perú", analizaron los criterios de valoración de la prueba digital en el marco de la legislación peruana, la metodología utilizada fue de carácter cualitativo, Se adoptó un enfoque cualitativo de tipo básico y se empleó la técnica documental y los métodos deductivo, hermenéutico y analítico. Concluyen que, ante la ausencia de una regulación específica, los jueces aplican el principio de libre valoración probatoria y los principios de legalidad, autenticidad, inalterabilidad, idoneidad y objetividad. Señalan que la doctrina y la jurisprudencia han desarrollado criterios progresivos para garantizar la legitimidad de la prueba digital, siempre que se obtenga de manera constitucionalmente válida y respetando los derechos fundamentales. Este antecedente aporta a la investigación al evidenciar la necesidad de un marco normativo autónomo y criterios específicos que fortalezcan la seguridad jurídica y la adecuada administración de justicia en el contexto de la ciberjusticia peruana.

Quispe (2024) en su investigación titulada "El impacto de la tecnología en el derecho a la prueba en el proceso penal: desafíos y perspectivas en la era digital" para optar el título de Segunda Especialidad en Derecho Procesal en la Pontificia Universidad Católica del Perú, desarrolló una investigación de enfoque cualitativo y de tipo jurídico-dogmático, empleó la técnica de análisis documental de normas, doctrina y jurisprudencia, así como el análisis crítico de la problemática del uso de la tecnología en los procesos penales. A pesar de la mejora en la

rapidez y la accesibilidad que ha traído consigo los avances tecnológicos en el sistema de justicia penal, el autor citado constató que han surgido nuevas preocupaciones que afectan al derecho a las pruebas y a la garantía de un juicio justo. Ello porqué las pruebas digitales pueden ser manipuladas fácilmente, y su integridad y su cadena de custodia se ven comprometidas, lo que pone en duda su fiabilidad y autenticidad. La confianza en el sistema de justicia se ve afectada por las preocupaciones sobre la privacidad y la protección de los derechos fundamentales al manejar datos personales en entornos digitales. Estas dificultades ponen de relieve las inconsistencias intrínsecas en el uso de la tecnología por parte del sistema de justicia penal contemporáneo.

Chávez (2024) en su tesis "La prueba digital y la validez probatoria en el proceso penal peruano" para optar por el título profesional de abogado en la Universidad Nacional Santiago Antúnez de Mayolo. La metodología utilizada fue dogmática normativa, bajo la técnica documental bibliográfica en especial sobre fuentes electrónicas. Los correos electrónicos, los mensajes instantáneos, los datos de redes sociales, los archivos multimedia y los datos de geolocalización son ejemplos de pruebas digitales que han cobrado mayor importancia en los procesos penales debido a los avances tecnológicos. La aplicación de estas pruebas plantea problemas debido a la falta de marcos normativos claros, lo que genera incertidumbre jurídica y posibles violaciones de los derechos fundamentales. La validez, integridad y verificabilidad de las pruebas digitales se ven afectadas por sus propiedades técnicas únicas, como su volatilidad, facilidad de duplicación y susceptibilidad al cambio. Debido a esto, ha habido diferentes fallos judiciales y desacuerdos sobre temas como la privacidad y el debido proceso, lo que pone de relieve el hecho de que el sistema de justicia penal peruano tiene un problema a la hora de evaluar sus pruebas.

Olivares y Ceras (2021), en el presente estudio "Delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020", en la presente investigación

abordaron el vínculo existente entre los tipos penales informáticos y la eficacia de la prueba electrónica en el Perú, la ruta metodológica se fundamentó en el paradigma científico, instrumentado a través de métodos de observación y experimentación y se categoriza como una investigación de carácter sustantivo (básica), con un alcance que transita desde lo exploratorio y descriptivo hasta la determinación de variables correlacionales, implementadas mediante un diseño transeccional no experimental. Según los resultados del estudio, no existe una correlación sólida entre la ciberdelincuencia y las pruebas digitales. Por lo tanto, podemos afirmar que el marco normativo que regula los rastros tecnológicos y su valor probatorio no es específico para cada delito. Es más, muestran que, aunque los abogados coinciden en que las pruebas digitales tienen mucho peso, las leyes tal como están son solo parcialmente suficientes. Esta investigación se suma a la literatura existente al poner de relieve la brecha entre los marcos normativos y la práctica judicial; además, enfatiza la necesidad de fortalecer el marco legislativo y los estándares para la valoración de pruebas en el sistema de justicia penal de Perú.

3.1.3 A nivel regional y local

Un análisis de las bases de datos académicas regionales y locales y de los repositorios institucionales revela una notable carencia de investigaciones específicas sobre las pruebas digitales en los procesos penales. Esto es particularmente cierto en el caso de los estudios que se centran en contextos locales o que tienen un enfoque empírico, lo que pone de manifiesto una importante laguna en la literatura científica existente. Los sistemas de información científica como QALISUS y las bases de datos internacionales de renombre como Scopus, así como los repositorios nacionales como ALICIA del CONCYTEC, corroboraron esta situación, ya que no presentan ningún hallazgo relacionado con el manejo probatorio de las pruebas digitales en un contexto local cusqueño.

Enlaces consultados:

https://www.scopus.com

https://alicia.concytec.gob.pe

https://qalisus.concytec.gob.pe

3.2. Bases teóricas

3.2.1 La evidencia digital

Este concepto se enmarca dentro de la transformación tecnológica del derecho probatorio, y su estudio requiere de bases teóricas que permitan comprender cómo los documentos electrónicos y la información digital adquieren valor jurídico, asímismo, cómo se garantizan su autenticidad e integridad, y qué principios doctrinales sostienen su admisibilidad en el proceso (Montece-Mosquera, 2020).

3.2.1.1 Teorías sobre la evidencia digital

3.2.1.1.1 La teoría de la equivalencia funcional

El concepto de equivalencia funcional implica que los documentos electrónicos pueden cumplir las mismas funciones jurídicas que los documentos físicos tradicionales; esta idea surge de la necesidad de actualizar la legislación para adaptarla a la era digital, pues los datos electrónicos pueden estar sujetos a las mismas implicaciones jurídicas que los documentos físicos. Siempre que cumplan con los estándares técnicos y jurídicos que garantizan su fiabilidad, los documentos electrónicos, los chats y los contratos pueden ser reconocidos como prueba. Esta visión se ha visto reforzada por la Ley Modelo de la CNUDMI (2017) y la doctrina Landáez (2007), que establecen que lo importante no es la forma material, sino la capacidad del documento para proporcionar pruebas, transmitir información y garantizar su conservación.

Así, la equivalencia funcional garantiza la seguridad jurídica en el ámbito digital al mediar entre el historial documentado y la innovación tecnológica.

3.2.1.1.2 Teoría de la neutralidad tecnológica

En lugar de favorecer o discriminar a ningún medio tecnológico en particular, el principio de neutralidad tecnológica establece que la ley debe evaluar las pruebas en función de su credibilidad y aplicabilidad. En lo que respecta a las pruebas, esto significa que, si se garantiza su legitimidad, los archivos digitales, los mensajes instantáneos y los correos electrónicos deben tratarse con el mismo cuidado que los documentos físicos. Al desplazar el enfoque del medio en sí hacia la calidad de las pruebas, este método pretende evitar que el sistema jurídico se quede rezagado con respecto a los avances tecnológicos. Según Reyes (2024), los jueces deben poder evaluar las pruebas digitales sin sesgos ni limitaciones formales para que el derecho probatorio pueda progresar. Gracias a esta idea, la gente tendrá más confianza en la digitalización del sistema legal, ya que garantiza que el sistema seguirá abierto a nuevas formas de prueba.

3.2.1.1.3 Teoría de la cadena de custodia

Para garantizar que las pruebas digitales sean legítimas y no hayan sido alteradas, la cadena de custodia es esencial. El término se refiere al registro documentado y continuo de todos los accesos, transferencias y gestiones de las pruebas, desde su recogida hasta su presentación en el juicio. Este concepto cobra mayor importancia en el ámbito digital, ya que los datos pueden modificarse o copiarse fácilmente. Montece-Mosquera (2020) destaca la importancia de la cadena de custodia para evitar nulidades procesales y garantizar que las pruebas presentadas sean coherentes con la recopilación inicial. El uso de herramientas forenses aprobadas, la documentación exhaustiva de cada operación y las medidas de

preservación estrictas forman parte de este proceso. La cadena de custodia es un componente esencial de la justicia digital, ya que garantiza que las pruebas permanezcan intactas y genera confianza entre el tribunal, las partes y el proceso.

3.2.1.1.4 Teoría de la prueba indiciaria

El material digital no siempre proporciona pruebas directas, sino más bien indicios que deben evaluarse junto con otras pruebas, según el principio de la prueba circunstancial. Se necesitan más pruebas para respaldar la idea de que un registro de acceso al sistema indique la participación en un hecho. El uso de la lógica y la justicia en la prueba circunstancial permite al juez extraer conclusiones a partir de información indirecta, tal como explica Castañeda (2021). En lo que respecta al ámbito digital, esta idea es particularmente relevante, ya que la mayoría de los datos técnicos (metadatos, registros de actividad) constituyen más una prueba circunstancial que una prueba fehaciente. Los datos digitales se contextualizan mediante el análisis conjunto de diversos componentes, lo que evita conclusiones apresuradas y garantiza un examen exhaustivo de los hechos.

3.2.1.1.5 Teoría de la proporcionalidad

El uso proporcionado de las pruebas digitales implica encontrar un equilibrio entre las necesidades de la investigación y la protección de los derechos fundamentales, como la libertad de decidir sobre la propia información y la privacidad. Por lo tanto, los procedimientos de obtención de pruebas digitales deben ser necesarios, adecuados y proporcionados al objetivo. Dado que la recopilación de demasiados datos podría vulnerar los derechos de las personas, Quispe (2024) sostiene que este concepto es crucial para prevenir los usos indebidos en las investigaciones penales. De acuerdo con el principio de proporcionalidad, los tribunales deben determinar si existen formas menos invasivas de alcanzar el mismo objetivo antes de decidir si

intervenir tecnológicamente. Al encontrar un punto medio entre las garantías constitucionales y la eficacia procesal, este concepto asegura que las pruebas digitales se recojan y evalúen dentro de un marco que respete la dignidad humana.

3.2.1.1.6 Teoría de la pertinencia probatoria

Según el principio de la pertinencia probatoria, las pruebas digitales solo pueden utilizarse en los tribunales si guardan relación directa con el caso y contribuyen a aclarar los hechos. Por lo tanto, las pruebas deben ser pertinentes para el caso en cuestión, además de válidas y creíbles. Dado que un exceso de datos puede generar confusión, Osco (2021) sostiene que la pertinencia es un filtro esencial para reducir la sobrecarga de información digital en los procedimientos judiciales. Dado que en el ámbito digital pueden mostrarse cantidades aparentemente infinitas de datos, la relevancia es de suma importancia. Por lo indicado, las pruebas digitales deben ser relevantes para el caso con la finalidad de que puedan utilizarse de manera efectiva y evaluarse de acuerdo con las normas del debido proceso.

El reconocimiento legal de las pruebas digitales se ve favorecido por la equivalencia funcional y la neutralidad tecnológica, su validez práctica está garantizada por la cadena de custodia y la proporcionalidad, y su valoración judicial se guía por las pruebas circunstanciales y la relevancia probatoria. De lo precisado se tiene que, el derecho probatorio contemporáneo reconoce las pruebas digitales como una herramienta legítima y confiable.

3.2.1.2 Los elementos de la evidencia digital

Las pruebas digitales poseen naturaleza intangible y dependen de mecanismos tecnológicos que requieren una gestión especializada, por ello un proceso legal eficaz y conforme a la ley deberá cumplir una serie de criterios fundamentales que garanticen su validez, integridad y aplicabilidad (Montece-Mosquera, 2020).

3.2.1.2.1. Elementos de la evidencia digital

a. Origen de la evidencia

La procedencia constituye una condición principal para la legalidad de las pruebas digitales en los procedimientos judiciales, es decir se debe de conocer de dónde provienen los datos para facilitar la verificación de su legitimidad y validez, ya sea que se trate de un dispositivo, un servidor, una red o la propia nube. Para disipar las dudas sobre la validez de los datos, la trazabilidad del origen es fundamental en el ámbito de las pruebas. Según Osco (2021), una forma de evitar la confusión causada por el auge de los medios digitales es atribuir correctamente las fuentes para que las personas puedan ver cómo se relacionan las pruebas con los hechos en cuestión. Además, es más probable que el tribunal dé crédito a las pruebas, ya que la fuente facilita la identificación de quién es responsable de qué en cuanto a la generación y el almacenamiento de datos. Sin esto, es imposible demostrar que las pruebas son relevantes para el asunto en cuestión, lo que las deja sin fundamento.

b. Autenticidad

Para que una prueba digital se considere auténtica, debe ser una representación fiel e inalterada de la realidad objeto de investigación. Este aspecto garantiza la credibilidad y la veracidad de la prueba de conformidad con las normas probatorias. Dado que la autenticidad garantiza que el archivo o documento digital refleja fielmente la realidad que pretende establecer, Quispe (2024) sostiene que es fundamental que la prueba sea genuina para que sea admitida. Para establecer la autenticidad, se combinan procedimientos de verificación técnica, certificados electrónicos y firmas digitales. Pues al no ser genuina, la prueba será cuestionable, lo que abrirá la puerta a impugnaciones.

c. Integridad

Las pruebas digitales deben de permanecer inalteradas a lo largo de todo el proceso judicial; cualquier alteración de las pruebas disminuirá su valor probatorio y dará lugar a una moción para excluirlas por contravención del debido proceso. Puesto que en el mundo digital es fácil modificar la información sin dejar rastros detectables, al respecto Montece-Mosquera (2020) sostiene que la integridad es especialmente relevante en este ámbito. Para garantizar que el contenido no se modifique, se utilizan técnicas como el hash criptográfico. Al asegurar que las pruebas presentadas sean indistinguibles del original, la integridad le da al tribunal más razones para creer que las pruebas son auténticas. Sin esto, las pruebas digitales son inútiles, ya que no se puede confiar en que reflejen con precisión los hechos en cuestión.

d. Cadena de custodia

Esta idea garantiza que las pruebas digitales permanezcan inalteradas a lo largo de todo el proceso judicial; cualquier cambio o alteración de las pruebas disminuiría su valor probatorio y podría dar lugar a una moción para excluirlas por violación del debido proceso. Dado que en el mundo digital es fácil modificar la información sin dejar rastros detectables, Montece-Mosquera (2020) sostiene que la integridad es especialmente vital en este ámbito. Para garantizar que el contenido no se modifique, se utilizan técnicas como el hash criptográfico. Al asegurar que las pruebas presentadas sean indistinguibles del original, la integridad le da al tribunal más razones para creer que las pruebas son auténticas. Sin esto, las pruebas digitales son inútiles, ya que no se puede confiar en que reflejen con precisión los hechos en cuestión.

e. Fiabilidad técnica

Las normas de fiabilidad técnica exigen el uso de instrumentos forenses reconocidos para la recopilación y el análisis de pruebas digitales. De conformidad con la norma ISO/IEC 27037 sobre la detección y recopilación de pruebas digitales, este rigor metodológico garantiza

resultados con un alto nivel de fiabilidad y reproducibilidad. Las pruebas digitales deben ser técnicamente fiables para que sean admitidas en los tribunales, ya que esto garantiza que los resultados puedan ser examinados por expertos imparciales (Landáez, 2007) . En un contexto legal, la fiabilidad técnica implica el uso de software aprobado, normas reconocidas y métodos aceptados internacionalmente. Esto con la finalidad de garantizar que las pruebas digitales estén protegidas contra cambios no autorizados o errores técnicos, lo que incrementa su valor como prueba.

f. Relevancia jurídica

Las pruebas digitales deben estar estrechamente relacionadas con los hechos relevantes del caso y proporcionar información referida directamente hacia la cuestión. Según Castañeda (2021), los procesos judiciales deberían enfocarse en la relevancia para evitar la sobrecarga de información digital, porque cuando hay demasiados datos se generan complicaciones que en realidad no hacen falta. Al dejar fuera información irrelevante que solo alarga el proceso, se logra que las pruebas digitales se usen de manera más justa y eficiente. En efecto, si las pruebas no son relevantes, pierden sentido y terminan siendo material que no aporta nada.

g. Admisibilidad procesal

El uso de pruebas digitales en los procesos judiciales depende de que se cumplan ciertos requisitos legales y se respeten derechos fundamentales, como la privacidad y el debido proceso. Si cumplen con criterios de autenticidad e integridad, los documentos electrónicos pueden aceptarse como prueba. En realidad, para que las pruebas digitales sean válidas en los tribunales, su obtención tiene que hacerse de manera correcta y conforme a las garantías constitucionales. Esto da lugar a asegurar su validez y respaldo teórico; pero si por alguna razón no son admitidas en el proceso, aunque sean auténticas o relevantes, al final no servirán de mucho.

h. Neutralidad tecnológica

En coherencia con el principio de neutralidad tecnológica, lo importante no es el soporte en sí, sino la credibilidad del sistema que genera las pruebas digitales. Los jueces pueden valorar estas pruebas de manera objetiva y sin trabas procesales, como señala Reyes (2024), quien afirma que esta técnica es clave para modernizar el derecho probatorio. En otras palabras, la neutralidad tecnológica asegura que los datos digitales, correos, mensajes instantáneos, etc., se traten con la misma seriedad que los documentos físicos, siempre que se garantice su autenticidad e integridad. Al permitir que las leyes se adapten a los avances tecnológicos, este enfoque crea un marco probatorio más abierto y flexible. Sin embargo, si las pruebas digitales se analizan con prejuicios y sin neutralidad, pierden fuerza y su utilidad en los procesos judiciales se verá reducida.

h. Temporalidad

Para poder reconstruir con éxito la secuencia cronológica de los hechos, la creación, modificación o acceso a las pruebas digitales debe documentarse con precisión. Según Osco (2021), se debe de tener en cuenta el factor tiempo para determinar el orden de los hechos y el papel desempeñado por los distintos actores. En ese sentido el uso de metadatos y registros de actividad mejorará el proceso de verificación de la exactitud de la información al preservar su orden cronológico en el entorno digital. En efecto, al proporcionar un marco histórico, este aspecto refuerza la fiabilidad de las pruebas. Se agrega que, las pruebas digitales perderán su capacidad explicativa y se convertirán en datos sin sentido y sin valor probatorio cuando no se presenten en un contexto histórico.

Asimismo, la fiabilidad y el valor del rastro digital como prueba ante los tribunales se verá directamente afectados por sus características, pues, las pruebas solo pueden considerarse válidas si se ha confirmado su validez, procedencia, cadena de custodia e integridad. Por ello

se debe de mantener la aplicación de la ley y la legitimidad en los procedimientos judiciales requiere fiabilidad técnica y neutralidad tecnológica, mientras que la pertinencia, la admisibilidad y la oportunidad garantizan su aplicabilidad en la era digital.

3.2.1.3. Concepto de evidencia digital

Se conoce como evidencia digital a cualquier información digital o electrónica que puede ser introducida como evidencia en un juicio para apoyar las declaraciones o acusaciones realizadas. Pueden ser actividades registradas en línea, correos electrónicos, chats, archivos y otros artículos digitales que ayudan a demostrar que un ciberdelito ocurrió o para revelar a los criminales.

"La evidencia digital es "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" (Grosh, 2004, p. 22).

Nessi, (2017) considera que, "la evidencia digital es un tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" (p. 22).

Según Nessi (2017):

> La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación. Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático –computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales. (p. 15)

Evidence, (2003) esta revista define que, “Consiste en cualquier información que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático, entendiéndose que el único fin de la evidencia es saber con la mayor exactitud posible los hechos facticos, encontrándonos como ejemplos de evidencias: a) Un disco duro, Pendrive, etc, b) Restos de instalación, c) Archivos temporales, d) Un proceso en ejecución, e) Un fichero en disco, f) El Uptime de un sistema, g) Una cookie en un disco duro, h) Un log en un fichero, i) El último acceso a un fichero”.

Desde nuestra concepción después del análisis, inferimos que la evidencia digital es toda información o dato almacenado, procesado o transmitido mediante dispositivos electrónicos o sistemas informáticos, que puede ser recolectado, preservado y presentado en un proceso judicial con valor probatorio, esta evidencia incluye archivos, registros de actividades, correos electrónicos, mensajes, logs, cookies, procesos en ejecución, entre otros, y se caracteriza por su naturaleza intangible, codificada en impulsos electrónicos y campos magnéticos, lo que exige herramientas y técnicas especializadas para su análisis y validación.

3.2.1.3.1. Naturaleza de la Evidencia Digital

Numerosas investigaciones han tratado de desarrollar la cuestión de si la evidencia digital puede ser identificada con la prueba documental y enmarcar el principio de equivalencia funcional a la hora de analizarla, así pues, es necesario mencionar que la evidencia digital se considera un grupo de prueba separado con una serie de funciones específicas que le otorgan un estatus especial en el proceso probatorio.

Algunas de las técnicas más comúnmente utilizadas para empresas este tipo de prueba son las capturas de pantalla o “pantallazos”, que implican congelar una imagen de una situación particular como conversaciones digitales o la transferencia de contenido multimedia para ser presentado como evidencia documental ante un proceso penal.

3.2.1.3.2. Principios de la Evidencia Digital

Según ISO/IEC 27037 (2012) la evidencia digital posee tres principios fundamentales:

La relevancia. - El proceso se centra en evidencias vinculadas al objeto de estudio para validar la premisa inicial, excluyendo los componentes que carezcan de relevancia.

La confiabilidad. - Para legitimar el proceso, los métodos deben ser sujetos a auditoría y replicables, asegurando que cualquier ejecución posterior arroje resultados consistentes.

Suficiencia. - las evidencias digitales recolectadas y analizadas son elementos suficientes para sustentar los hallazgos y verificar las afirmaciones de la investigación.

3.2.1.3.3. Características de la evidencia digital

La evidencia digital contiene algunas características propias que la distinguen de cualquier otra evidencia tradicional, (evidencia física) entre otras, contiene las siguientes particularidades:

- Volátil: Si no se asegura la prueba en el momento oportuno y bajo las condiciones adecuadas, existe un alto riesgo de pérdida o degradación de los datos.
- Duplicable: Dado que es posible generar múltiples duplicados exactos, resulta imposible distinguir el archivo original de sus copias.
- Alterable: Los datos son vulnerables a alteraciones o eliminaciones accidentales o intencionadas que no dejan rastro de su manipulación.
- Anónima: A veces es imposible identificar al creador real, sin embargo, los archivos contienen metadatos (información oculta) que las aplicaciones comunes no muestran, como la ubicación GPS, el modelo del dispositivo, fechas de acceso o el historial de envío de un correo.

> Según (Sosa, 2023), La integridad y confiabilidad de la evidencia dependen de cumplir rigurosamente con los tiempos y métodos de recolección, garantizando así su fuerza legal al momento de actuar en juicio oral.

3.2.1.3.4. Fuentes de la evidencia digital

Los datos probatorios se encuentran en diversas fuentes: desde el almacenamiento permanente y la memoria temporal del sistema, hasta el flujo de información en red que debe recolectarse en tiempo real. Desde este punto de vista, es posible categorizar los orígenes de la evidencia digital en los siguientes apartados:

a. Sistema de computación abierta: Comprende el hardware informático estándar, incluyendo estaciones de trabajo, equipos portátiles, servidores y todos sus dispositivos complementarios.

b. Sistemas de comunicación: Abarca toda la infraestructura de conectividad, incluyendo redes de datos, sistemas de transmisión inalámbrica y la red global de internet.

c. Sistemas convergentes de computación: Se limita exclusivamente a tecnologías móviles y portátiles, como teléfonos inteligentes, asistentes digitales (PDA) y tarjetas con chip.

3.2.1.3.5 Importancia de la evidencia digital en el proceso

Cabe señalar que, según Molina (2020, como se citó en Casey, 2011), la evidencia digital puede definirse como los datos digitales con valor legalmente probatorio que se encuentran almacenados o transmitidos, de esta manera, se resalta la importancia que tiene la información contenida en diferentes dispositivos electrónicos para el ámbito jurídico. Desde una perspectiva legal, este tipo de evidencia constituye una forma de prueba tangible, Se basa en señales electrónicas y campos magnéticos, los cuales se procesan con herramientas forenses para servir como medio de prueba en un juicio.

En esa misma línea Nessi (2017) afirma que la relevancia de esta evidencia digital radica en la necesidad de presentar al juez pruebas concluyentes que establezcan la culpabilidad del sospechoso (…). Por ello queda en evidencia que el valor de la evidencia digital radica en su capacidad para proporcionar pruebas sólidas que establezcan la culpabilidad o inocencia de un sospechoso ante el tribunal. Por ello, es esencial que el experto encargado seleccione cuidadosamente la evidencia relevante, facilitando la labor del juez.

La importancia en los procesos penales actuales de las pruebas digitales es cada vez mayor dado que estas constituyen un medio probatorio concluyente, técnicamente verificable y legalmente admisible que puede determinar la culpabilidad o inocencia de un acusado. Aunque estas pruebas son técnicamente intangibles (se trata de datos codificados electrónicamente), se consideran tangibles desde el punto de vista jurídico, ya que pueden recopilarse, almacenarse y presentarse de acuerdo con determinadas normas tecnológicas.

Por lo dicho se tiene que, la evidencia digital no solo amplía las fuentes de prueba en el proceso penal moderno, sino que también refuerza la eficacia y precisión de la administración de justicia en delitos informáticos y convencionales en los que intervienen tecnologías de la información.

3.2.1.3.6 Aseguramiento de la escena del delito frente a las evidencias digitales

La preservación de la escena del crimen será realizada por personal de la Policía con conocimientos técnicos especializados en el manejo de evidencia digital, quienes deberán informar de inmediato al Fiscal. Bajo la dirección del Fiscal, la Policía Nacional podrá realizar las siguientes actividades:

-Recolectar y resguardar objetos e instrumentos relacionados con el delito.

-Elaborar planos, capturar fotografías, realizar grabaciones, entre otras acciones similares.

-Llevar un registro detallado de los elementos incautados o asegurados, especialmente en situaciones de flagrancia o cuando exista un riesgo inminente de que se cometa el delito.

- La conducción de la investigación corresponde al Ministerio Público, siendo crucial el respaldo de expertos técnicos para garantizar la eficacia de esta etapa. El aseguramiento del lugar de los hechos demanda medidas de protección y delimitación estrictas para evitar la degradación de los indicios digitales; de omitirse los protocolos vigentes esto invalidaría la integridad de la prueba.

-Al acudir a la escena del delito el personal policial o del Ministerio Publico deben seguir ciertos procedimientos para una adecuación de la preservación de la evidencia digital.

3.2.1.3.6.1. Definición de los parámetros de la escena

Al intervenir el personal que intervenga debe realizar primero un reconocimiento exhaustivo del entorno físico e identificar la infraestructura de red y todos los sistemas informáticos que se encuentren presentes.

a. Observación, evaluación y planificación

Es sumamente importante la planificación de las actividades antes de intervenir en la escena del delito. Lo cual incluye la identificación de escenarios primarios y secundarios, la definición de prioridades y la garantía de seguridad para los especialistas. Asimismo, se debe verificar y registrar la presencia de sistemas de videovigilancia o monitoreo, tanto en las zonas interiores como en el exterior del lugar.

b. Delimitación de la escena del crimen

Resulta necesario demarcar o delimitar el área donde se halla la evidencia, incluyendo accesos, salidas, zonas aledañas, vehículos y otros elementos relevantes. Esta información deberá ser documentada mediante fotografías, videos, croquis y/o planos.

c. Identificación del personal presente

Se debe garantizar el registro detallado y la filiación de todas las personas presentes en la escena, incluyendo testigos, personal policial, Ministerio Publico y personal de emergencias.

d. **Implementación de medidas de seguridad**

La seguridad operativa y la intangibilidad del perímetro son requisitos esenciales para que la labor de investigación sea viable y segura.

e. Proporcionar primeros auxilios

Es fundamental que el personal de emergencia brinde atención médica inmediata a las víctimas del delito, asegurando al mismo tiempo la preservación de las evidencias presentes en la escena.

f. Protección física de la escena

Durante esta fase, es importante asegurar la trazabilidad y preservación de la cadena de custodia para evitar cualquier impugnación, para ello, las evidencias deben ser correctamente identificadas, etiquetadas y manejadas conforme a los principios y métodos establecidos.

3.2.1.3.7 Donde se encuentra la evidencia digital

Los soportes de almacenamiento donde reside la prueba digital se categorizan principalmente de la siguiente manera:

a. Dispositivos de almacenamiento

Discos duros internos: Se trata de unidades de almacenamiento mecánico que utilizan platos de aluminio o cristal con una capa magnética y cabezales móviles para la gestión de datos.

Discos duros externos: Estas unidades operan con suministro eléctrico independiente y se integran al sistema mediante interfaces USB, FireWire, Ethernet o protocolos de red inalámbricos.

Medios extraíbles: Incluyen dispositivos diseñados para almacenar, archivar y transportar información, como: Pendrives (USB), Unidades portátiles de almacenamiento conectadas mediante puertos USB.

Tarjetas de memoria: Estos soportes de almacenamiento son estándares en una amplia gama de ecosistemas digitales, que incluyen desde dispositivos móviles y cámaras hasta centros de entretenimiento y equipos de cómputo portátiles.

Entre las posibles evidencias que pueden recuperarse de estos dispositivos se encuentran, por ejemplo, mensajes de correo electrónico, entre otros datos relevantes para la investigación.

b. Dispositivos portátiles

El ecosistema de dispositivos móviles y portátiles incluye terminales de telefonía, relojes inteligentes, agendas electrónicas (PDA), equipos multimedia, cámaras, receptores de GPS, reproductores de audio y cámaras de video.

En el marco de una investigación, es posible encontrar una amplia variedad de evidencias digitales almacenadas en diferentes dispositivos, entre las más relevantes se incluyen.

Mensajes de comunicación:

- Correos electrónico enviado y recibido.
- Mensajes de texto.
- Chats en aplicaciones de mensajería instantánea o servicios de Internet.
- Mensajes de voz almacenados en dispositivos o aplicaciones.

Registros de actividad:

- Historial de navegación por Internet.
- Listado de llamadas realizadas y recibidas.
- Páginas web visitadas.
- Logs o registros del sistema y de las aplicaciones.
- Redes Wi-Fi detectadas o a las que se ha conectado el dispositivo.

Contenido multimedia y archivos:

- Fotografías y archivos de imagen en diversos formatos (JPG, PNG, GIF, BMP, TIF, entre otros).
- Documentos y archivos de texto.
- Archivos de bases de datos y registros almacenados localmente.
- Metadatos vinculados a archivos y documentos.

Información técnica y de sistema:

- Datos de localización geográfica (GPS).
- Aplicaciones instaladas y su actividad.
- Contraseñas almacenadas en memoria.
- Claves de cifrado y configuración de seguridad.

Estas evidencias pueden ser clave para reconstruir eventos, identificar responsables y establecer conexiones entre los elementos de un caso. Su recolección, análisis y preservación debe realizarse conforme a protocolos forenses para garantizar su validez legal.

Dispositivos de almacenamiento informático

Los dispositivos de almacenamiento informático serán aquellos componentes o equipos utilizados para guardar y recuperar datos digitales, estos pueden ser internos o externos, y se clasifican en varias categorías según su tecnología, capacidad, velocidad y portabilidad.

Tipos de Dispositivos de Almacenamiento.

- Dispositivos de almacenamiento primario (memoria principal).

-RAM (Memoria de Acceso Aleatorio): Memoria volátil, se borra al apagar el equipo. Se usa para almacenar datos temporales mientras se ejecutan programas.

-ROM (Memoria de Solo Lectura): Contiene instrucciones esenciales para el arranque del sistema. No se borra al apagar el equipo.

- Dispositivos de almacenamiento secundario. Almacenan datos de forma permanente o a largo plazo.

-Discos duros (HDD - Hard Disk Drive).

- Almacenamiento magnético.
- Gran capacidad (varios TB).
- Más lento que otros tipos, pero económico.

-Unidades de estado sólido (SSD - Solid State Drive).

- Sin partes móviles.

- Mucho más rápidas que los HDD.
- Más caras por GB, pero con mayor rendimiento.

-Unidades ópticas.

- CD, DVD, Blu-ray: Usan láser para leer/escribir datos.
- Menor capacidad comparada con HDD/SSD.
- Hoy en día en desuso, pero aún presentes en algunos entornos.

-Memorias flash.

- USB (pendrives), tarjetas SD, etc.
- Portátiles, pequeñas, y bastante rápidas.
- Usadas para transferencia rápida o almacenamiento temporal.

-Almacenamiento en la nube.

- Espacio virtual ofrecido por servidores en internet (ej. Google Drive, Dropbox).
- Accesible desde cualquier dispositivo con conexión.
- Depende del proveedor y la conexión a internet.

Dispositivos portátiles de Computación.

Entendemos por aquellos equipos completos, con capacidad de procesamiento y conexión de redes.

-Laptops o portátiles.

- Computadoras completas y compactas.
- Autonomía por batería, conexión Wi-Fi, Bluetooth, etc.

-Tabletas (tablets).

- Pantalla táctil, sin teclado físico (aunque se puede añadir).
- Ligeras, ideales para lectura, navegación, multimedia, trabajo básico.

-Teléfonos inteligentes (smartphones).

- Dispositivos multifunción: comunicación, navegación, apps, cámara, etc.
- Alta capacidad de almacenamiento interno.

-Smartwatches y pulseras inteligentes.

- Se llevan en la muñeca.
- Registran actividad física, notifican mensajes, entre otros.

-Consolas portátiles de videojuegos.

- Ej. Nintendo Switch, Steam Deck, PS Vita.
- Diseñadas para jugar en cualquier lugar.

-Redes de computadoras.

Una red se define como un conjunto de nodos interconectados (vía cable o señal inalámbrica) que intercambian recursos mediante hardware de gestión como switches o routers, en estos entornos, la evidencia digital es vasta: abarca desde metadatos de software y tráfico de red hasta registros de navegación, bases de datos y comunicaciones por correo o chat, desde nuestra óptica son aquellas que están compuesta por dos o más computadoras conectadas a través de cables de datos o enlaces inalámbricos, lo que permite el uso compartido de recursos, tales como impresoras, periféricos y dispositivos de enrutamiento de datos (como hubs, switches y routers).

Los repositorios de evidencia digital abarcan desde registros de ejecución de software y bases de datos hasta artefactos de comunicación, tales como correos electrónicos, historiales de navegación, registros de mensajería instantánea (chats) y archivos multimedia almacenados en unidades externas.

3.2.1.3.8 Procedimientos de obtención, preservación y cadena de custodia (como recopilar la evidencia digital).

Dado que el escenario del crimen es dinámico, es imperativo recolectar los indicios en su estado primigenio. Esto previene la contaminación y asegura la integridad y mismidad de la prueba, requisitos indispensables para su admisión y valoración en el juicio oral.

Asimismo, es imperativo que el encargado de la recolección documente de manera adecuada todo lo acontecido, ya que, en los delitos de naturaleza informática, la obtención de la evidencia suele estar vinculada al uso de equipos de cómputo. Por ello, dichos dispositivos deben ser manipulados con especial cautela, considerando tanto sus estructuras internas como externas, incluidas las pantallas y demás mecanismos disponibles, de modo que se asegure la fidelidad de la información y se preserve su valor probatorio en la determinación de los hechos delictivos.

3.2.1.3.8.1 Asegurar la escena donde se encuentra una evidencia digital.

Es un paso crucial para garantizar la integridad, legalidad y validez de la información que podría ser utilizada como prueba en un proceso judicial. Este procedimiento debe seguir protocolos técnicos y jurídicos estrictos para evitar la alteración, pérdida o contaminación de los datos. ¿Qué entendemos por asegurar la escena con evidencia digital? Consiste en proteger, documentar y controlar el entorno físico y digital en el que se encuentra la evidencia electrónica

(como computadoras, teléfonos, servidores, routers, etc.), para preservar su estado original y permitir su análisis forense sin comprometer su valor legal.

3.2.1.3.9. Pasos para asegurar correctamente la escena digital.

3.2.1.3.9.1. Preservar el entorno inmediato

a. Restringir el acceso a personas no autorizadas.

b. Evitar que los dispositivos sean manipulados, apagados o desconectados sin medidas adecuadas.

c. Si el dispositivo está encendido, evaluar si debe mantenerse encendido (para conservar información volátil) o apagado (para prevenir daños).

3.2.1.3.9.2. Documentar la escena

Tomar fotografías y notas detalladas de la disposición de los dispositivos y cables.

a. Registrar ubicación, hora, fecha y personas presentes.

b. Identificar todos los posibles dispositivos con capacidad de almacenamiento o conexión.

3.2.1.3.9.3. Evitar alteraciones

a. No interactuar con los sistemas si no se cuenta con personal forense capacitado.

b. Utilizar herramientas forenses para el análisis y recolección (como bloqueadores de escritura en discos duros).

3.2.1.3.9.4. Asegurar la cadena de custodia

a. Etiquetar correctamente los dispositivos recolectados.

b. Registrar cada movimiento o cambio de custodia.

c. Garantizar almacenamiento seguro y acceso controlado.

3.2.1.3.9.5. Recolección y traslado

a. Embalar los dispositivos con protección antiestática.

b. Utilizar cajas seguras para el transporte.

c. Asegurar que se cumplan las normas legales locales o internacionales sobre evidencia digital.

3.2.1.3.9.6. Errores comunes a evitar

a. Apagar un equipo encendido sin antes realizar un análisis de la memoria RAM.

b. Conectar dispositivos sospechosos a otros sistemas sin protección.

c. Acceder a cuentas, archivos o programas antes de clonar los discos.

d. No documentar adecuadamente los procedimientos realizados.

3.2.1.3.9.7. Importancia legal

Una evidencia mal asegurada puede ser impugnada en juicio por pérdida de integridad, violación a la cadena de custodia o por no cumplir principios de legalidad y proporcionalidad. Por eso, todo el proceso debe estar alineado con estándares forenses y normativas procesales.

3.2.1.3.10 Análisis integral de la evidencia digital.

Existen diversas técnicas y herramientas especializadas en el ámbito forense que se emplean para el análisis de evidencias digitales, las cuales deben ajustarse a las formalidades establecidas por normas y estándares internacionales, así como a los procedimientos de buenas prácticas desarrollados por organismos gubernamentales y expertos reconocidos en la materia. Entre estas herramientas destacan:

• Computer Forensic: disciplina forense dedicada a la identificación, recuperación e interpretación de información almacenada en medios informáticos, con el objetivo de reconstruir los hechos y formular hipótesis que relacionen la evidencia con el caso investigado.

• Mobile Forensic: técnica que permite extraer, analizar e interpretar datos almacenados en dispositivos móviles tales como teléfonos inteligentes, tabletas y otros aparatos similares.

• Network Forensic: herramienta fundamental para el análisis de las operaciones y el tráfico en redes informáticas. Siguiendo protocolos específicos y principios de la criminalística, esta técnica facilita la comprensión y seguimiento de actividades delictivas a través de redes de comunicación digital.

3.2.1.3.11 Código hash en el tratamiento de la evidencia digital

Según Casey (2011), el código hash es fundamental para garantizar la integridad de la evidencia digital durante todo el proceso forense.

La función hash permite "verificar que los datos no hayan sido alterados, asegurando así la autenticidad de la evidencia" (Jones, 2018, p. 45).

Como establece el NIST (National Institute of Standards and Technology, 2015), los algoritmos SHA-256 ofrecen una mayor seguridad para el tratamiento de datos digitales en procesos judiciales.

Desde nuestra óptica podemos inferir que en la investigación forense digital, el código hash se ha consolidado como una herramienta fundamental para garantizar la integridad y autenticidad de la evidencia electrónica, desde la parte conceptual un código hash es un valor alfanumérico generado mediante una función matemática que transforma una entrada de datos, de cualquier tamaño, esta cadena actúa como una "huella digital" única del contenido original.

El uso de funciones hash en el tratamiento de la evidencia digital tiene varias aplicaciones clave:

1. Verificación de Integridad: Permite comprobar que la evidencia no ha sido alterada durante su recolección, transporte o almacenamiento, es por eso que al calcular el hash de un archivo original y compararlo con el hash del mismo archivo en otro momento, se puede detectar cualquier modificación, por mínima que sea.

2. Cadena de Custodia Digital: al momento de la generación y registro de códigos hash en cada etapa de manejo de la evidencia es una práctica esencial para mantener una cadena de custodia ininterrumpida, así, se puede demostrar durante el juicio que la prueba digital presentada es idéntica a la obtenida en la escena del hecho o en la fuente original.

3. Optimización del Análisis Forense: Los códigos hash facilitan la identificación rápida de archivos duplicados o irrelevantes, lo cual es crucial cuando se manejan grandes volúmenes de datos en una investigación digital.

Las funciones hash más comúnmente utilizadas en forense digital incluyen algoritmos como MD5 (Message Digest 5) y SHA-1, SHA-256 (Secure Hash Algorithm), aunque la comunidad técnica y jurídica ha recomendado migrar hacia algoritmos más robustos como SHA-256, debido a vulnerabilidades identificadas en versiones anteriores.

El uso correcto y sistemático del código hash fortalece la validez probatoria de la evidencia digital, y también contribuye a la transparencia y confiabilidad del proceso judicial en materia tecnológica. Por ello, su aplicación está ampliamente respaldada en la doctrina forense y regulaciones internacionales vinculadas a la materia.

3.2.1.3.12 Admisibilidad y valoración de la evidencia digital en el proceso penal

La inmediatez, la publicidad, el carácter contradictorio y la oralidad son las características que deben cumplirse al presentar pruebas en la fase oral del juicio. Las pruebas almacenadas en soportes digitales deben presentarse durante la vista oral, según Lluch y González (2013), a fin de mantener el principio del proceso contradictorio.

Todas las pruebas deben ser pertinentes, necesarias y útiles para que sean admitidas como tales ante un tribunal. En particular, en la valoración de las pruebas durante los juicios, la Ley de Enjuiciamiento Civil (LEC) de España ha tenido una influencia significativa en algunos aspectos del proceso penal peruano. El artículo 299, párrafo 2, de la LEC establece que, de conformidad con las leyes pertinentes, se podrán admitir dispositivos que puedan registrar, procesar o reproducir información, como datos, cifras u operaciones relevantes para el proceso, así como soportes que puedan reproducir el habla, el sonido y las imágenes. La admisibilidad de estos criterios dependerá de la evaluación que haga el tribunal de los mismos durante el juicio. No se podrán celebrar alegatos orales si no cumplen con las condiciones básicas. De acuerdo con la misma legislación, no se podrá incluir ninguna prueba que no sea relevante para el proceso (artículo 283, párrafo 1).

En los procesos penales relacionados con delitos informáticos, es fundamental realizar una evaluación técnica previa a la admisión de la prueba digital. Castillo (2015) señala que esta evaluación debe considerar varios aspectos: identificar el equipo desde el cual se originó el documento digital, comprobar el correcto funcionamiento del mismo, establecer que el resultado se deriva de los datos ingresados, justificar la fiabilidad del sistema que almacena y emite la información, y, finalmente, identificar a las personas que participaron en la elaboración del documento. Dada la complejidad de estos elementos, en muchos casos se hace necesaria la

intervención de una pericia informática para asegurar la validez de la prueba (Castillo, 2015, p. 48).

Frente a ello, Parra (2017) al referirse de la prueba nos da mayores alcances que a continuación detallamos:

La Conducencia: Para que una prueba sea admitida, debe gozar de legalidad, lo que implica que su obtención y uso estén expresamente permitidos por la normativa vigente. Asimismo, debe cumplir con el principio de pertinencia, manteniendo una relación directa y necesaria con los hechos controvertidos en el litigio; de lo contrario, será rechazada de plano (in limine) por carecer de utilidad procesal.

La utilidad: Según la doctrina contemporánea, la finalidad de la prueba es impulsar el proceso para generar una convicción plena en el juzgador; si el elemento probatorio no contribuye a crear esa certeza, procede su rechazo liminar.

Pertinencia: La pertinencia constituye un criterio fundamental para determinar si una prueba debe ser admitida en el proceso penal, esta exige que el medio probatorio esté vinculado de forma directa con los hechos que se buscan acreditar o esclarecer durante el juicio. En consecuencia, no se aceptan pruebas sobre aspectos ajenos o irrelevantes al objeto procesal, ya que el proceso debe centrarse únicamente en lo que resulta esencial para la decisión judicial. Como establece la normativa procesal, la prueba impertinente debe ser excluida, por no aportar elementos útiles para el esclarecimiento del caso (Céspedes, 2018).

3.2.1.3.13 Retos y problemáticas en el manejo de la evidencia digital

En los delitos relacionados con la tecnología o el ciberespacio, las pruebas digitales son hoy en día fundamentales para los procesos de investigación y enjuiciamiento. Los obstáculos

logísticos, jurídicos y técnicos que impiden su plena incorporación al sistema de justicia penal peruano merman su valor probatorio y dificultan las evaluaciones judiciales.

Un problema importante es que no existen protocolos específicos u organizados para supervisar la recopilación, el almacenamiento, la transferencia y el examen de las pruebas digitales. Si bien la Ley de Delitos Cibernéticos N.º 30096 y el Código de Procedimiento Penal (Decreto Legislativo N.º 957) abordan algunas de las cuestiones que pueden surgir en el ámbito digital, no logran resolverlas todas (Quintana, 2020).

Un obstáculo importante es la falta de capacitación adecuada en informática forense y tecnología de la información entre el personal del sistema judicial, incluidos jueces, fiscales y agentes de policía. Esta deficiencia provoca que las pruebas digitales se manejen de manera incorrecta en cada etapa de su ciclo de vida, desde la recolección hasta la presentación ante el tribunal, lo que puede llevar a su rechazo por falta de las garantías procesales adecuadas (Vargas, 2019).

Por otro lado, garantizar la autenticidad, la integridad y la trazabilidad de los datos digitales no está exento de retos técnicos. A menudo resulta imposible demostrar que las pruebas no han sido alteradas o manipuladas durante su obtención y análisis, debido a la falta de normas específicas para garantizar la cadena de custodia digital (López, 2021).

Además, las capacidades normativas e institucionales del Estado no están a la altura del ritmo de los avances tecnológicos. Esto da lugar a situaciones jurídicas complejas que requieren interpretación judicial y crea vacíos legales en relación con las nuevas formas de delito digital, lo que podría generar incertidumbre jurídica (Castillo, 2018).

Dadas estas dificultades, es fundamental establecer protocolos estandarizados para el manejo adecuado de las pruebas digitales de manera que sean consistentes con los principios

del proceso penal, tales como el debido proceso, la inmediatez, la legalidad y el proceso contradictorio. Además, es necesario mejorar las capacidades técnicas.

3.2.1.3.14 Ventajas del uso de IA para la investigación forense de la evidencia digital.

La inteligencia artificial (IA) se ha convertido en una herramienta poderosa para el análisis forense de pruebas digitales como parte de la revolución digital del sistema de justicia penal. Sin embargo, su aplicación solo es posible si se respetan las normas establecidas por la ley, que protegen los derechos fundamentales, garantizan el debido proceso y aseguran la admisibilidad de las pruebas.

Aunque en Perú no existe una ley específica que prohíba el uso de la IA en las investigaciones forenses, las leyes ya vigentes permiten que el uso de la IA se interprete de acuerdo con ciertos principios generales. Los principios de legalidad, contradicción, inmediatez y tutela judicial efectiva se recogen en el Código de Procedimiento Penal (Decreto Legislativo N.º 957), que establece que todas las pruebas deben recabarse de conformidad con la ley (Ministerio de Justicia y Derechos Humanos, 2004).

La Ley N.º 30096, conocida comúnmente como la Ley de Delitos Informáticos, autoriza el uso de herramientas tecnológicas para la recopilación y el procesamiento de pruebas como respuesta al aumento de los delitos digitales. Aunque la inteligencia artificial (IA) no se menciona expresamente en el documento aprobado por el Congreso peruano en 2013, este sí contempla la posibilidad de su incorporación a través de procesos técnicos que mejoren la eficacia de la detección, el almacenamiento y el análisis de datos digitales.

De conformidad con la Resolución Legislativa n.º 30399 de Perú, el país ha ratificado el Convenio de Budapest sobre la Ciberdelincuencia. Este convenio fomenta el uso de tecnología de vanguardia y la cooperación internacional en la investigación de los delitos

cibernéticos, siempre y cuando se protejan los derechos humanos y se respeten los principios de proporcionalidad y necesidad (Consejo de Europa, 2001).

La aplicación de la inteligencia artificial en las investigaciones forenses digitales ofrece beneficios tales como la automatización de la clasificación de datos, la identificación rápida de tendencias delictivas y la minimización del error humano en el procesamiento de pruebas (Martínez y Ríos, 2022). Sin embargo, el uso de esta tecnología debe regirse por normas que garanticen la trazabilidad de los algoritmos, la transparencia de los procesos analíticos y la posibilidad de impugnación defensiva.

Por lo tanto, aunque el Perú aún carece de una regulación específica sobre el uso de IA en procesos penales, es posible enmarcar su uso dentro de los principios generales del proceso penal, en armonía con los estándares internacionales de derechos humanos y prueba tecnológica.

3.2.1.3.15 Respecto a las diferencias entre la prueba digital y evidencia digital

La diferencia entre prueba y evidencia digital radica principalmente en su naturaleza jurídica y técnica, así como en el proceso de incorporación al juicio: Evidencia digital Definición: Es toda la información o dato de interés probatorio que se encuentra almacenado, transmitido o procesado a través de dispositivos electrónicos o digitales (como computadoras, teléfonos, servidores, redes, etc.). Ejemplos: Correos electrónicos, registros de acceso, mensajes en redes sociales, archivos de audio o video, direcciones IP, metadatos, etc.

Características:

Puede ser fácilmente alterada o destruida.

Requiere técnicas especiales de recolección, preservación y análisis (cadena de custodia, peritaje informático). Por sí sola no es prueba, sino un posible indicio que debe ser validado.

Prueba: Es la información o elemento que ha sido admitido formalmente en un proceso judicial con el fin de acreditar o desacreditar hechos relevantes. Incluye: Testimonios, documentos, peritajes, inspecciones, confesiones, y también evidencias digitales, si son admitidas conforme a las reglas procesales.

Proceso: su requisito es que la evidencia (incluida la digital) sea legalmente obtenida, preservada y presentada. Es evaluada por el juez o tribunal para formar convicción sobre los hechos.

Debido a la naturaleza de los delitos informáticos, la prueba es el eje central para la aplicación de la ley. Al cumplir con los requisitos de pertinencia, conducencia y utilidad, la evidencia permite acreditar el dolo, el lugar del hecho y la afectación de bienes jurídicos. Esto fundamenta la imputación contra el autor mediante una motivación probatoria sólida, garantizando así una correcta administración de justicia.

3.2.2 El proceso penal peruano

3.2.2.1. Conceptos

El proceso penal peruano es el conjunto de actos jurídicos ordenados y regulados por el Estado, cuyo fin es la averiguación de la verdad, y la determinación de la responsabilidad penal de los imputados, garantiza el derecho fundamental tanto de los acusados como de las víctimas, este proceso se rige por los principios de legalidad, contradicción, publicidad, celeridad y debido proceso.

Según el Código Procesal Penal peruano, tiene por objeto "la averiguación de la verdad, la justicia en la aplicación del Derecho penal y la pronta reparación del daño causado por el delito" (Congreso de la República del Perú, 2004, art. I).

El sistema procesal penal vigente en el Perú se caracteriza por ser acusatorio y garantista, promoviendo una estructura donde el juez actúa como tercero imparcial, mientras que las partes fiscalía y defensa sostienen la acusación y defensa respectivamente, esta transformación responde a un modelo que busca superar las deficiencias del sistema inquisitivo anterior (García, 2018).

3.2.2.2. Principios fundamentales del proceso penal peruano

El sistema de justicia penal peruano se fundamenta en una serie de pilares esenciales que definen cómo debe organizarse, operar y cumplir sus objetivos, por lo cual estos principios no solo tienen carácter normativo, sino también constitucional y convencional, ya que derivan de la Constitución Política del Perú, del Código Procesal Penal (Decreto Legislativo N.º 957), y de los tratados internacionales de derechos humanos ratificados por el Estado peruano.

De acuerdo con López (2019), los principios procesales penales son fundamentales para asegurar que el proceso sea justo, equilibrado y respetuoso de los derechos de todas las partes, en especial del imputado y de la víctima. A continuación, se muestran los principales principios que rigen el proceso penal en el Perú.

a. Principio de legalidad procesal

El principio de legalidad se basa en que que toda actuación procesal deberá estar prevista en la ley. Ninguna persona puede ser sometido a proceso penal sin que exista una norma que expresamente lo habilite. Este principio garantiza la seguridad jurídica y evita

arbitrariedades por parte de los órganos jurisdiccionales (Ministerio de Justicia y Derechos Humanos, 2004).

b. Principio de presunción de inocencia.

Reconocido en el artículo 2 inciso 24 de la Constitución, este principio establece que toda persona es inocente mientras no se demuestre lo contrario mediante una sentencia firme. En consecuencia, la carga de la prueba recae en quien acusa, y cualquier duda razonable debe resolverse a favor del imputado (Castillo, 2021).

d. Principio de contradicción

según (García, 2020), el proceso penal peruano se estructura sobre el principio de contradicción, que garantiza a las partes la posibilidad de conocer, controvertir y contradecir las pruebas y alegatos del adversario. Es una manifestación del derecho a la defensa y de la igualdad.

e. Principio de imparcialidad judicial

El juez debe actuar con plena independencia e imparcialidad, sin favorecer a ninguna de las partes. La neutralidad del órgano jurisdiccional es indispensable para garantizar un proceso equitativo. Cualquier afectación a este principio puede acarrear la nulidad del proceso (Gonzales, 2018).

f. Principio de oralidad

El proceso penal se desarrolla principalmente de forma oral, especialmente en la etapa de juicio. La oralidad permite mayor transparencia, inmediación, concentración y contradicción entre las partes, elementos esenciales del proceso acusatorio (Pérez, 2017).

g. Principio de publicidad

Toda audiencia debe ser pública, salvo que razones de seguridad, moral u orden público justifiquen su reserva. Este principio permite el control ciudadano del actuar judicial y refuerza la legitimidad del proceso penal (Quintana, 2020).

h. Principio de concentración

Las actuaciones procesales deben realizarse en el menor número de sesiones posibles, evitando dilaciones innecesarias, el objetivo es asegurar una justicia pronta y eficaz, en respeto al principio del plazo razonable (López, 2019).

i. Principio de economía procesal

Este principio exige que el proceso penal sea ágil, eficiente y que evite actuaciones innecesarias o redundantes, siempre respetando los derechos fundamentales. Busca racionalizar el uso de recursos judiciales y humanos (García, 2020).

j. Principio de defensa

El derecho a la defensa técnica y material del imputado es una garantía irrenunciable. Desde el inicio del proceso, toda persona tiene derecho a contar con un abogado y a ser escuchado en igualdad de condiciones (Ministerio de Justicia y Derechos Humanos, 2004).

3.2.2.3. Fines del proceso penal peruano

La finalidad del proceso no es castigar, sino solucionar, pacificar la sociedad, y solo cuando eso no puede ser logrado es que el castigo aparece y puede tener justificación (Guardia, 2016).

En principio se dice que, a lo largo de la historia, el proceso penal se erige como un medio para encontrar una solución frente a las disputas que se presentan, para lo cual se utiliza

un medio racional y no violento; el mismo que sustituirá la utilización de la fuerza que originó el conflicto intersubjetivo de intereses y que se busca resolver, en ese sentido la vía pacífica resulta razonable dado la organización y constitución del sistema jurídico y político que apuesta por el diálogo como un estilo de vida (Ríos, 2019).

Para abordar este acápite empezaremos por señalar que un fin busca la consecución de un objetivo, en ese entender se ejecuta o realiza diversos actos con una motivación específica.

En relación con los fines del proceso penal, puede afirmarse que las distintas actuaciones que se desarrollan a lo largo del iter procedimental se orientan hacia la consecución de una finalidad propia de dicho proceso. Surge entonces la cuestión central: ¿cuál es ese objetivo? Para responder a esta interrogante, resulta necesario, en primer término, identificar el modelo procesal que sirve de fundamento e inspiración a nuestra normativa adjetiva.

Cabe precisar que, en torno a los fines del proceso penal, la doctrina no presenta una posición unánime. Diversos autores sostienen que dichos fines pueden comprender la "búsqueda de la verdad", la "protección del individuo frente al ius puniendi del Estado", la "solución de controversias", la "protección del inocente, la sanción del culpable y la reparación del daño causado", así como el "mantenimiento de la paz social", entre otros. En nuestro caso, compartimos la postura de quienes consideran que la finalidad esencial del proceso penal radica en la "búsqueda de la verdad" y en la "protección de la persona frente al ius puniendi estatal".

Nuestros legisladores han establecido que la finalidad del proceso penal peruano es la búsqueda de la verdad, ahora, si bien dicha finalidad no se encuentra establecida de manera taxativa en el cuerpo normativo adjetivo, sin embargo al estar regulado la actuación de la prueba de oficio como una facultad del juzgador, entonces ello nos permite señalar que lo que busca el proceso penal es justamente ello, porque de lo contrario no tendría justificación dicha

regulación, ya que el juez previo a emitir un fallo justo puede considerar necesario la actuación excepcionalmente de la prueba de oficio (Salinas, sf).

3.2.2.4. El objeto del Proceso Penal Peruano

Sendra (2003) detalla que el objeto del proceso penal se constituye por el thema decidendi; o sea, por los actos comisivos u omisivos delictivos que se someten a juicio, lo que dicho en otro modo sería, los hechos enjuiciados si constituyen delito y sus derivadas consecuencias penales hacia los sujetos inculpados. De forma simplificada, se puede decir que el hecho penal es el objeto del proceso penal, toda vez que se adviertan que los actos juzgados son los de las personas sometidas a juicio, y que, a su vez, sean concretos y dotados de relevancia antijurídica.

3.2.2.5 fases del proceso penal peruano

El proceso penal en el Perú se encuentra regulado por el Código Procesal Penal (Decreto Legislativo N.º 957), norma que establece un modelo procesal acusatorio, garantista y adversarial. Este modelo se estructura en fases claramente diferenciadas, las cuales buscan asegurar el respeto al debido proceso, la tutela jurisdiccional efectiva y el derecho a un juicio justo. Cada etapa tiene características y finalidades específicas que contribuyen al esclarecimiento de los hechos, la determinación de la responsabilidad penal y la protección de los derechos fundamentales de las partes involucradas.

Según Gonzales (2018), el proceso penal peruano se desarrolla a través de cuatro fases principales: la etapa de investigación preliminar, la etapa de investigación preparatoria, la etapa intermedia y el juicio oral. Cada una de estas cumple una función determinada dentro de la dinámica procesal penal.

Pero nosotros consideramos que solo existen tres fases o etapas principales, es decir etapa de investigación preliminar y dentro de ella se encuentra como una sub etapa la etapa de investigación preparatoria, la etapa intermedia y la etapa de juzgamiento, conforme desarrollaremos a continuación.

a. Etapa de investigación preliminar

Esta fase se activa mediante la notitia criminis o el conocimiento de un posible ilícito, siempre bajo la conducción del Ministerio Público, se busca corroborar el hecho, individualizar a los presuntos autores y recabar los primeros indicios de convicción, en este periodo se ejecutan diligencias preliminares de carácter urgente, las cuales solo requieren autorización judicial si vulneran derechos fundamentales.

a.1. Etapa de investigación preparatoria

Aquí, el Ministerio Público formaliza la investigación con la finalidad de sustentar la acusación futura o, en su caso, archivar el caso. La investigación es más profunda, se realiza con conocimiento del imputado y está sujeta al control judicial. Según López (2020), en esta etapa se produce la mayor recolección de pruebas, y el juez de investigación preparatoria interviene cuando se requiere autorizar medidas coercitivas, como la prisión preventiva o el levantamiento del secreto de las comunicaciones.

b. Etapa intermedia

Concluida la investigación preparatoria, se inicia la etapa intermedia, donde el juez de investigación preparatoria evalúa la suficiencia de los elementos de convicción presentados por el fiscal, en esta fase se depura el proceso: se decide sobre la admisión o exclusión de pruebas, se resuelven cuestiones incidentales, y se determina si corresponde abrir o no juicio oral (García, 2017).

c. Juicio oral

Es la fase central y culminante del proceso penal, el cual se desarrolla bajo los principios de oralidad, inmediación, concentración, contradicción y publicidad, es presidido por un juez o colegiado que valora las pruebas actuadas durante la audiencia, es en esta etapa donde se determina la culpabilidad o inocencia del acusado, y se emite sentencia (Vargas, 2019).

Esta forma por etapas garantiza un proceso penal más ordenado, transparente y respetuoso de los derechos procesales, diferenciándose del modelo inquisitivo anterior. Además, promueve la eficiencia procesal y refuerza la legitimidad del sistema de justicia penal.

3.2.2.6 Sujetos procesales

Se entiende por los sujetos procesales aquellas personas físicas o jurídicas que intervienen de manera activa en el desarrollo del proceso, ya sea en representación del Estado, en defensa de sus derechos o como partes interesadas. El Código Procesal Penal (Decreto Legislativo N.°957) delimita con claridad quiénes conforman este grupo, estableciendo sus roles, derechos y obligaciones procesales.

De acuerdo con Gonzales (2017), los sujetos procesales se dividen en dos grandes categorías: los principales (Ministerio Público, imputado, defensor, agraviado) y los auxiliares o terceros (parte civil, actor civil, terceros civilmente responsables, peritos, testigos, etc.). Cada uno cumple una función específica en la búsqueda de la verdad material y en la garantía de un proceso justo.

a. El Ministerio Público

El fiscal es el titular de la acción penal penal, es quien dirige la investigación preliminar y preparatoria, ejerce la acusación en el juicio oral y tiene el deber de actuar con objetividad, según el artículo 60 de la Constitución Política del Perú y el artículo IV del Título Preliminar

del CPP, su función es proteger los intereses de la sociedad y garantizar la legalidad del proceso penal (Ministerio de Justicia y Derechos Humanos, 2004).

b. El imputado

El imputado es la persona a quien se le atribuye la comisión de un delito, en el marco del Estado constitucional de derecho, goza de una serie de garantías constitucionales, como el derecho a la defensa, a guardar silencio, a ser juzgado en un plazo razonable, entre otros, la presunción de inocencia, reconocida en el artículo 2, inciso 24, de la Constitución, lo protege hasta que exista una sentencia condenatoria firme (López, 2018).

c. La Defensa Técnica

El abogado defensor puede ser designado por el propio imputado de su libre elección o asignado por el Estado, tiene como misión principal salvaguardar los derechos del acusado y asegurar que el proceso penal se desarrolle dentro del marco legal. La defensa técnica es obligatoria en todas las etapas del proceso, garantizando el principio del contradictorio (García, 2020).

d. La víctima o agraviado

Es aquella persona natural o jurídica que ha sufrido un daño como consecuencia del delito. Tiene el derecho de intervenir en el proceso penal, de ser informado sobre el desarrollo del caso y de solicitar la reparación civil. Según la Ley N.º 30364 y el propio CPP, el agraviado puede constituirse como parte civil para exigir una indemnización por los daños sufridos (Castillo, 2019).

e. Otros sujetos procesales

También intervienen otros actores como el juez penal, cuya función es imparcial y garantiza que el proceso se desarrolle conforme a derecho; los terceros civilmente responsables, quienes pueden responder por los daños derivados del delito.

En conjunto, todos estos sujetos participan con roles bien definidos, y su actuación debe respetar los principios del debido proceso, igualdad de armas, legalidad y contradicción, garantizando así la justicia penal en el marco del sistema acusatorio adoptado en el Perú.

3.2.2.7 Los sistemas procesales Penales

El Derecho procesal penal peruano ha experimentado una evolución significativa a lo largo de la historia, dando lugar a distintos sistemas procesales penales, los cuales reflejan la forma en que se organiza el enjuiciamiento penal en un determinado orden jurídico. Estos sistemas no solo representan modelos técnicos, sino también concepciones ideológicas sobre el poder del Estado, los derechos del imputado y el rol de las partes en el proceso.

Según Gómez (2016), existen tres modelos clásicos: el sistema inquisitivo, el sistema acusatorio y el sistema mixto, cada uno con características distintivas en cuanto a la función de los sujetos procesales, la forma de producir la prueba y las garantías procesales.

a. Sistema inquisitivo

El sistema inquisitivo, originado en la Europa medieval, se caracteriza por la concentración de funciones en una sola autoridad, que investiga, acusa y juzga. En este modelo, el proceso se desarrolla de forma escrita, secreta y sin contradicción. El imputado es tratado como objeto del proceso y no como sujeto de derechos. No existe igualdad de armas ni imparcialidad, y la confesión suele ser el medio de prueba central (Pérez, 2018).

Este sistema fue adoptado en diversos países de tradición romano-germánica y se mantuvo en vigencia por siglos, aunque ha sido ampliamente cuestionado por ser contrario a los principios del debido proceso y los derechos humanos.

b. Sistema acusatorio

El sistema acusatorio esta centrado en la separación clara de funciones entre el acusador, el defensor y el juez, quien debe actuar como un tercero imparcial. Este modelo se caracteriza por ser oral, público, contradictorio e inmediato. La carga de la prueba recae en la parte acusadora, y el imputado es considerado inocente hasta que se demuestre lo contrario (García, 2020).

Este sistema reconoce la centralidad del juicio oral como espacio de debate público y garantiza la participación activa de las partes en igualdad de condiciones. Se inspira en los principios liberales y está ampliamente reconocido en los sistemas de corte anglosajón y, en la actualidad, en las reformas procesales penales latinoamericanas.

c. Sistema mixto

El sistema mixto es una combinación de elementos del sistema inquisitivo y del acusatorio. Generalmente, presenta una fase preliminar escrita e inquisitiva (concentrada en el Ministerio Público) y una fase de juicio oral acusatoria, donde se garantiza el contradictorio. Es un modelo de transición que ha sido adoptado por muchos países de tradición civilista, incluido Perú.

En el caso peruano, el Código Procesal Penal (Decreto Legislativo N.º 957) establece un sistema acusatorio con rasgos mixtos, donde el Ministerio Público dirige la investigación y el juez penal actúa con funciones jurisdiccionales limitadas a resolver peticiones de las partes. El juicio oral es público, oral y contradictorio, y el imputado goza de garantías fundamentales

como la presunción de inocencia, el derecho a la defensa y el principio de legalidad (Ministerio de Justicia y Derechos Humanos, 2004).

c. La tendencia hacia el modelo acusatorio en América Latina

En las últimas décadas, diversos países latinoamericanos han reformado sus sistemas procesales penales para adoptar el modelo acusatorio, promoviendo una justicia más transparente, ágil y respetuosa de los derechos fundamentales. Estas reformas responden a estándares internacionales como los establecidos por la Convención Americana sobre Derechos Humanos y la Corte Interamericana de Derechos Humanos (Quintana, 2021).

3.2.2.8 El nuevo código procesal penal

Características del Nuevo Código Procesal Penal peruano.

El Nuevo Código Procesal Penal del Perú (en adelante, NCPP), aprobado mediante el Decreto Legislativo N.º 957 y vigente de manera progresiva desde 2006, representa una transformación profunda del sistema de enjuiciamiento penal en el país, este código adopta un modelo acusatorio y garantista, orientado a reforzar los principios del debido proceso, la eficiencia judicial y la tutela efectiva de los derechos humanos.

A diferencia del modelo anterior de corte inquisitivo y escrito, el NCPP promueve un proceso oral, público, contradictorio, transparente y con clara separación de funciones entre los sujetos procesales. Estas transformaciones responden tanto a compromisos internacionales como a la necesidad de modernizar el sistema judicial peruano.

Según García (2019), las principales características del Nuevo Código Procesal Penal son las siguientes:

a. Sistema acusatorio y adversarial

El NCPP adopta un modelo acusatorio, en el que las funciones de investigar, acusar y juzgar están claramente diferenciadas. El Ministerio Público dirige la investigación; el juez de garantías controla la legalidad del proceso; y el juez o tribunal de juicio oral emite sentencia. Este modelo fortalece el principio del contradictorio y garantiza un juez imparcial (Gonzales, 2021).

b. Oralidad y publicidad

Uno de los pilares del nuevo sistema es la oralidad en todas las etapas del proceso penal, especialmente en la audiencia de juicio. La oralidad permite un mayor control social y favorece la cercanía entre las partes y el juez en la actuación de los medios probatorios. Además, la publicidad del proceso garantiza transparencia y ayuda a prevenir abusos (Ministerio de Justicia y Derechos Humanos, 2004).

c. Concentración y celeridad procesal

Implica quitar los retrasos que no hacen falta, agilizar los procesos y fijar plazos razonables para cada etapa. De esta manera, el sistema judicial, basado en el principio de tutela judicial efectiva, se vuelve más eficiente y receptivo (López, 2020).

d. Principio de igualdad procesal

Según Pérez (2018), dentro del marco del NCPP, las partes, es decir, la fiscalía y el abogado defensor del acusado, se encuentran en igualdad de condiciones durante todo el proceso. Esto significa reconocer derechos fundamentales del acusado, como contar con representación legal, poder recabar pruebas, interrogar a los testigos y también dar su propio testimonio.

d. Protección de derechos fundamentales

El derecho al debido proceso, a apelar, a no declarar contra uno mismo y el derecho a la presunción de inocencia, entre otros.

e. Juicio oral como etapa central

En el juicio, que constituye el núcleo del proceso penal, la fiscalía y la defensa presentan sus argumentos, exponen sus alegatos y, a continuación, el tribunal dicta su veredicto. Este sistema garantiza que el juez evalúe las pruebas de forma inmediata, basándose en los principios de concentración, publicidad, contradicción e inmediatez (Quintana, 2022).

f. Participación activa de la víctima

Ahora, las víctimas pueden iniciar una acción civil, participar en los procedimientos, recibir información actualizada sobre el caso y reclamar una indemnización por daños y perjuicios en el marco del NCPP, lo que supone un cambio con respecto al sistema anterior. Como resultado, el sistema de justicia penal se vuelve más empático y equitativo (Castillo, 2020).

3.2.2.9 La inteligencia artificial y la valoración de la prueba en el proceso penal peruano

Los jueces están obligados a expresar de manera coherente sus opiniones al evaluar las pruebas, de conformidad con el artículo 158, que exige la aplicación de la lógica, los conocimientos científicos y los principios derivados de la experiencia. Además, la sentencia debe ser detallada e inequívoca, y explicar el razonamiento por el que se acepta o se rechaza un hecho, tal como lo exige el artículo 394.3.

No se puede subestimar la importancia de que el juez realice una evaluación justa y exhaustiva de las pruebas de conformidad con normas probatorias y principios jurídicos bien

establecidos. Este enfoque de evaluación garantiza la búsqueda de la verdad y la toma de decisiones basadas en principios jurídicos. Para una evaluación precisa de las pruebas son necesarios conocimientos especializados en derecho, experiencia laboral relevante y un profundo conocimiento de los hechos y circunstancias del caso.

3.2.2.10 Cadena de Custodia en el derecho Procesal Peruano

Desde la parte conceptual, se entiende que son las actividades y medidas implementadas para asegurar la autenticidad y conservación de las pruebas obtenidas durante una investigación, garantizando así su validez legal en el proceso judicial. Si este procedimiento se ve interrumpido o vulnerado, no se podría asegurar que la evidencia presentada sea la misma que la originalmente recolectada, lo que comprometería su valor probatorio.

En el caso de las evidencias digitales estas están en constante transformación debido al rápido avance de las tecnologías de la información y la comunicación (TIC). Esto obliga a una actualización permanente en los métodos de tratamiento de dichas evidencias.

Las formas más frecuentes de evidencia digital en los procesos penales incluyen:

• Correos electrónicos.

• Mensajes multimedia enviados por redes públicas (como aplicaciones de mensajería).

• Mensajes SMS y MMS transmitidos a través de teléfonos móviles, los cuales pueden contener texto, imágenes, grabaciones de audio o video.

• Interacciones en línea como debates, publicaciones, conversaciones en redes sociales, y espacios de trabajo colaborativo. Estas se desarrollan en el entorno digital, donde las personas comparten opiniones, costumbres o información con una gran cantidad de usuarios en internet.

• También se incluye el documento de identidad electrónico, utilizado para validar la identidad de una persona en medios digitales.

3.3 Definición de términos

Alterabilidad

Su vulnerabilidad a ser modificada o borrada sin dejar un registro evidente de dichas acciones (Portugal et al., 2022).

Cadena de custodia

Protocolo jurídico y técnico que certifica que la prueba digital se mantuvo intacta, auténtica y rastreable desde el hallazgo hasta el debate judicial, descartando cualquier manipulación (Ministerio del Interior, 2019).

Código Hash

La función hash permite “verificar que los datos no hayan sido alterados, asegurando así la autenticidad de la evidencia” (Jones, 2018, p. 45).

Cibercriminalidad

Se refiere a las actividades ilícitas ejecutadas mediante tecnologías de la información o en el ciberespacio, que abarcan desde intrusiones no autorizadas y fraudes electrónicos hasta la propagación de contenidos prohibidos, dejando siempre un rastro de evidencia digital.

Derecho probatorio

Rama del Derecho Procesal que regula los medios, principios y procedimientos mediante los cuales se obtiene, incorpora y valora la prueba en un proceso judicial, incluyendo la prueba digital (García, 2023).

Derecho penal peruano

Como el conjunto de normas establecidas por el Estado que asocian al crimen (delito) la pena como legítima consecuencia (Sánchez et al., 2022).

Duplicidad

La capacidad de realizar copias exactas (imágenes forenses) sin alterar el original ni información que contiene (Chavez et al., 2024).

Evidencia digital

Información de valor probatorio que se encuentra almacenada o transmitida en formato digital, como correos electrónicos, archivos, registros de navegación, mensajes en redes sociales, entre otros (Osco et al., 2025).

Legalidad procesal

Principio fundamental que exige que toda actuación dentro del proceso penal, incluida la obtención y valoración de evidencia digital (Naula et al., 2022).

Peritaje informático

Examen técnico realizado por un especialista en informática forense con el fin de identificar, extraer, preservar y analizar evidencia digital, (Osco et al., 2025).

Volatilidad

La facilidad con la que los datos digitales pueden perderse o alterarse si no se recolectan a tiempo (Sosa et al., 2024).

IV. Metodología

4.1. Tipo y nivel de investigación

Tipo:

El presente estudio es de enfoque cualitativo y de dogmático analítico ya que se enfoca en el análisis crítico de normas jurídicas, doctrina y jurisprudencia aplicables al tratamiento de la evidencia digital en el proceso penal peruano, con el objetivo de identificar vacíos, incoherencias y proponer soluciones desde una perspectiva jurídica. Según Castro-Cuba (2019) los estudios dogmáticos analíticos en derecho son aquellos que se centran en el análisis interno del ordenamiento jurídico, para interpretar las normas y/o instituciones jurídicas con el fin de esclarecer su contenido, estructura y aplicación.

La investigación es de enfoque cualitativo, en tanto se desarrolla a partir del análisis documental de normas, doctrina y jurisprudencia, así como de entrevistas semiestructuradas a operadores del sistema de justicia penal, lo que permite interpretar significados, criterios y experiencias vinculadas al tratamiento de la evidencia digital, sin recurrir a datos cuantificables. Asimismo, es de tipo aplicado, ya que no se limita a la descripción o explicación teórica del fenómeno estudiado, sino que tiene como finalidad identificar vacíos normativos y deficiencias prácticas, con el propósito de contribuir a la mejora del tratamiento jurídico de la evidencia digital en el proceso penal peruano y generar un impacto concreto en la realidad jurídica.

Nivel:

La presente investigación es de nivel básico porque está orientada a ampliar y profundizar el conocimiento jurídico existente sobre el tratamiento de la evidencia digital en el proceso penal peruano, mediante el análisis de normas, doctrina y jurisprudencia. Su propósito principal es generar conocimiento teórico y conceptual respecto de los criterios jurídicos aplicables a la evidencia digital, identificando vacíos normativos, inconsistencias interpretativas y desafíos en su aplicación práctica, sin buscar la implementación inmediata de una intervención específica.

4.2. Ámbito temporal y espacial

El ámbito temporal de la investigación comprende el análisis del marco normativo y jurisprudencial vigente hasta el año 2025, considerando las disposiciones del Código Procesal Penal, así como normas conexas, doctrina reciente y casos judiciales desarrollados en los últimos cinco años, en los que la evidencia digital haya tenido un rol relevante.

El ámbito espacial se circunscribe principalmente a la Corte Superior de Justicia del Cusco, donde se recogió información a través de entrevistas a expertos.

4.3. Población y muestra

En investigación, la población se entiende como el conjunto total de individuos, elementos o unidades que poseen características comunes y que son objeto de estudio. En el ámbito jurídico, la población está conformada por aquellos actores que participan directamente en la aplicación, interpretación o ejecución de normas relacionadas con el fenómeno investigado. Según Hernández-Sampieri (2018), la población constituye el universo de referencia del cual se extrae la muestra, y su adecuada delimitación es fundamental para garantizar la validez y pertinencia de los resultados.

La población de la presente investigación está conformada por operadores del sistema de justicia penal, tales como jueces, fiscales, abogados defensores y efectivos de la Policía Nacional del Perú (PNP), todos ellos con experiencia en el uso de evidencia digital en procesos penales. La muestra seleccionada es no probabilística e intencional, dado que se eligió a participantes que cumplen con criterios específicos de conocimiento y experiencia en el tema. En total, se incluyó aproximadamente a 08 expertos, cuya participación permitió obtener información relevante y especializada para el análisis crítico del tratamiento de la evidencia digital en el proceso penal peruano.

La muestra seleccionada para esta investigación es no probabilística e intencional, conformada por 07 expertos operadores del sistema de justicia penal. Se incluyeron jueces, fiscales, abogados defensores y efectivos de la Policía Nacional del Perú (PNP), todos ellos con experiencia comprobada en el uso y valoración de evidencia digital en procesos penales. La elección de los participantes responde a la necesidad de contar con informantes clave que aporten conocimiento especializado y práctico sobre el tema de estudio.

Los criterios de inclusión establecidos para la presente investigación comprenden a los operadores del sistema de justicia penal, tales como jueces, fiscales, abogados defensores y efectivos de la Policía Nacional del Perú, que cuenten con experiencia directa en casos donde la evidencia digital haya sido utilizada como medio probatorio, que posean un mínimo de cinco años de ejercicio profesional en el ámbito penal, que hayan participado en procesos judiciales dentro de la Corte Superior de Justicia del Cusco y que, además, acepten voluntariamente formar parte del estudio mediante el otorgamiento del consentimiento informado; por otro lado, los criterios de exclusión consideran a aquellos operadores del sistema de justicia penal que no tengan experiencia en el uso de evidencia digital, a los profesionales que no se encuentren ejerciendo actualmente funciones en el ámbito penal, a quienes no otorguen su consentimiento

informado o decidan retirarse durante el proceso de entrevistas, así como a los funcionarios que desempeñen cargos de carácter administrativo sin intervención directa en procesos penales.

Justificación

La selección de forma intencional de la “muestra” responde a la necesidad de obtener información cualitativa más especializada, y que provenga de actores directamente relacionados con el manejo de la evidencia digital.

4.4. Instrumentos

Considerando el enfoque cualitativo aplicado al derecho, se emplearon dos técnicas de recolección de datos con sus correspondientes los instrumentos así se tiene:

-El análisis documental de normas nacionales e internacionales y doctrina especializada.

-Entrevistas semiestructuradas las cuales se aplicaron a actores clave .

Los instrumentos fueron la guía de análisis documental y la guía de entrevista.

4.5. Procedimientos

Comprendió los siguientes pasos:

1. Revisión bibliográfica y normativa: Para construir un marco conceptual sólido, se realizó una recopilación y organización bastante exhaustiva de la legislación nacional e internacional sobre la gestión de pruebas digitales, junto con la teoría jurídica y la jurisprudencia relacionadas.
2. Diseño y validación de los instrumentos: Especialistas revisaron y aprobaron las versiones finales tanto de la guía de análisis documental como de la guía de entrevistas semiestructuradas.

3. Entrevistas: Un total de siete responsables de la toma de decisiones del sistema de justicia penal del Tribunal Superior de Justicia de Cusco (entre ellos jueces, fiscales, abogados defensores y miembros de la PNP) participaron en entrevistas semiestructuradas.
4. Procesamiento de los datos: utilizando las categorías preestablecidas de la investigación, los datos obtenidos de las entrevistas y del análisis documental se organizaron metódicamente en tablas y matrices.
5. Análisis: para determinar qué puede hacer el sistema de justicia penal peruano para manejar mejor las pruebas digitales, qué es lo que la normativa no puede hacer y qué deficiencias prácticas existen, se realizó un análisis temático de contenido.
6. Elaboración de resultados y conclusiones: con base en el análisis realizado, se presentaron los hallazgos principales, formulando lineamientos que contribuyen a fortalecer la legitimidad, confiabilidad y eficacia de la prueba digital en concordancia con estándares internacionales y principios del derecho procesal penal.

4.6. Análisis de datos

A partir de las taxonomías del estudio, los datos recopilados se organizaron mediante un análisis de contenido temático. Con el fin de identificar patrones, lagunas normativas y recomendaciones pertinentes, los datos se presentarán de forma descriptiva utilizando resúmenes, citas directas y matrices.

4.7. Consideraciones éticas

En el estudio se consideró el respeto por las normas éticas y de uso de información proporcionada por los participantes, quienes fueron informados de los objetivos de la

investigación; asimismo los datos recopilados han sido utilizados únicamente con fines académicos. El análisis de la legislación, las doctrinas y la jurisprudencia se llevó a cabo de manera imparcial, y con rigor académico, transparencia y objetividad.

V. Resultados y discusión

5.1 Resultados

Análisis de los antecedentes

Tabla 1

Análisis de los antecedentes de investigación.

Título de la investigación	**Autor (es)**	**Año**	**Ubicación**	**Método**	**Resultados Principales (síntesis de las conclusiones)**	**Relevancia para la investigación Actual (según el objetivo general).**
El tratamiento de la evidencia digital en el proceso penal y la motivación de las decisiones judiciales de acuerdo con la ley y el derecho a la defensa	Layana OñateTatiana Elizabeth	2023	Ecuador	Enfoque Cualitativo	La presente investigación demuestra que, mientras el mundo ha sido revolucionado por las TICs, el Derecho Penal ecuatoriano y sus operadores aún se encuentran en un estado de rezago que pone en riesgo la eficacia de la justicia frente a las nuevas formas de criminalidad digital.	La relevancia radica en el análisis jurídico exhaustivo de la normativa y la praxis procesal actual, con el fin de identificar las limitaciones en la aplicación y valoración de la evidencia digital dentro del proceso penal peruano, proponiendo directrices para fortalecer su validez probatoria.
La incorporación de las pruebas digitales en el proceso penal acusatorio tesis	Omar Garcia Rodriguez	2023	Ecuador	Enfoque cualitativo	El principal hallazgo de la investigación es la ampliación del concepto de prueba digital dentro del proceso penal.	Se enfoca en cerrar la brecha digital en el derecho penal peruano, pasando de un sistema analógico a uno apto para la era digital, garantizando así una justicia más eficaz y respetuosa de los derechos.
La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia.	Bujosa, L., Bustamante, M., & Toro, L.	2021	Brasil	Investigación documental.	La prueba digital, especialmente la obtenida mediante vigilancia secreta, requiere urgentemente la adecuación del sistema normativo y procesal penal para garantizar su lícita obtención, autenticidad, integridad y valoración, equilibrando la eficacia investigativa con la protección de los derechos fundamentales.	Los principios de la evidencia digital son que se deben de obtener de manera licita, autenticidad, integridad y luego sea valorado en el proceso penal.
El impacto de la tecnología en el derecho a la prueba en el proceso penal: desafíos y perspectivas en la era digital.	Elizabeth Quispe Palma	2024	A nivel Nacional	Investigación cualitativa y jurídica.	La digitalización del proceso penal agiliza la justicia, pero plantea desafíos críticos de autenticidad y fiabilidad de la evidencia digital y material, exigiendo protocolos rigurosos, capacitación legal y medidas de equidad e inclusión para proteger el derecho a la prueba y los derechos fundamentales.	Mediante la utilización correcta de la recolección de la evidencias digitales se garantiza la autenticidad y fiabilidad de la evidencia digital frente al riesgo de manipulación, asegurando una cadena de custodia efectiva y respetando los derechos.
La prueba digital y la validez probatoria en el proceso penal peruano	Ever Gabriel Chavez Alva	2024	A nivel Nacional	La investigación cualitativa	En la tensión entre la realidad tecnológica y el vacío legal peruano sobre la evidencia digital, y la necesidad urgente de una solución normativa.	El tratamiento actual de la evidencia digital en el proceso penal peruano está comprometido por un vacío normativo que amenaza su autenticidad y validez probatoria, siendo imperativo proponer un marco legal que garantice el debido proceso.

5.1 Resultados de las entrevistas

Tabla 2.

En su experiencia, ¿existen elementos que hacen que la evidencia digital requiera un tratamiento distinto al de la evidencia física? ¿Cuáles son esos elementos?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Bien, entiendo que la evidencia digital es la de recabar los medios de prueba para acreditar un hecho, para las evidencias físicas o comunes se deben de hacer la cadena de custodia para garantizar la autenticidad, pero las evidencias digitales se tiene que hacer una cadena de custodia digital, ahí surge la complicación ya que no existe una regulación de cómo hacer una autenticidad de esa evidencia, quizá mediante el sistema Hash pero con la participación de un perito que garantice la autenticidad la no manipulación más aun en estos tiempos de la inteligencia artificial.
Dr. Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de WaNCHAQ	En mi consideración si considero que existen elementos o características, en vista de que al evidencia física o tradicional es única, es la oportunidad para poder obtener en cambio la evidencia digital es volátil, fácilmente duplicable, puede ser ocultable o descifrar esas serían las diferencias por ello la urgencia de abordar urgente de manera adecuada básicamente por los efectivos policiales quienes son los que tienen directamente contacto con los elementos digitales.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	En efecto existen elementos que diferencia la evidencia digital de la evidencia física, la evidencia física es algo que podamos percibir a simple vista, pero la evidencia digital necesita un tratamiento especial, ya que pueden ser borrados, alterados o suprimidos de manera digital
Ronald Henry MOTTA GONZA S1 PNP Perito Informatico de la PNP.	Que, si existen elementos en la evidencia digital que hacen diferencia a la evidencia física, son la autenticidad, la integridad, pueden ser reproducidos en un archivo la muestra generando el código Hash podemos generar copias, otro también es la trazabilidad.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	Bueno, desde mi punto de vista si existen elementos que hacen que el tratamiento de la evidencia digital sea distinto a la evidencia física, los cuales son volátil, cambiante, dependiendo en el dispositivo electrónico en la que se encuentre la evidencia digital, este tratamiento debe de realizarse de acuerdo a los procedimientos y protocolos establecidos en los manuales de la Evidencia digital.
Wilfredo FARFAN QUISPE abogado co ICAL N°93408	Es un tipo de prueba documental que se encuentra en soporte electrónico. Debe cumplir con los principios de legalidad autenticidad, integridad y pertinencia para que pueda ser admitida en juicio. Los mismos que se encuentran señalados en los artículos 158-A, 158-B, 172, 178-A, 185 Y 187, excepcionalmente, pueden utilizarse otros distintos, siempre que no vulneren los derechos y garantías de la persona, como son: mensajes de correo, historial de navegación de Internet, Chat de Internet, listas de registros, fotografías en distintos formatos de archivos (JPG, PNG, GIF, BMP, TIF), archivos de imágenes, documentos, archivos de texto, metadatos de archivos, claves en memoria, claves de encriptación, etc.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	Si considero que la evidencia digital tiene que tener un tratamiento estrictamente distinta a la evidencia física, en vista que la evidencia digital es muy volátil y corre el riesgo de desaparecer sino se obtiene de manera oportuna, puede ser modificable fácilmente si no se recaba de la manera adecuada y con la seguridad del caso y otro aspecto importante es que se puede ver a simple vista su contenido como sucede con las evidencias físicas.

Si hacemos un análisis crítico, a las respuestas de cada uno de los entrevistados es que estas son pertinentes y abordan correctamente el núcleo de la pregunta. Todos los participantes coinciden en que existe una diferencia en el tratamiento de la evidencia digital y la evidencia física o la clásica, y además mencionan los elementos claves como son la (volatilidad, duplicidad, autenticidad y generación del código Hash o la cadena de custodia digital).

Tabla 3.

¿Considera que el sistema de justicia peruano reconoce adecuadamente estas diferencias en la práctica judicial?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	No hemos vistos casos, son recientes lo poco que se tiene son imágenes, grabaciones, audios y no hay la cantidad de peritos o la especialización que se pueda hacer una diferenciación, muchas veces el Ministerio Público considera que descargando la información en un dispositivo y hacer una cadena de custodia en el dispositivo es suficiente.
Dr.Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Yo que creo que sí, existen pronunciamiento de las cortes supremas donde cuentan sobre esta diferencia entre la evidencia física y la evidencia digital, creo que el problema radica ente los operadores digitales quienes no tenemos claro de cómo trabajar con estas evidencias digitales, existen protocolos donde establecen el recojo de la evidencia digital pero los operadores de justicia no lo ponen en práctica por desconocimiento.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	Considero que no, ya que para poder recabar cierta información sobre evidencia digital se debe de seguir ciertos protocolos y procedimientos en la obtención de la evidencia digital, y en las evidencias comunes físicos es únicamente el paso común.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Que he notado que al ser una rama nueva para nosotros aquí en Perú en los casos que tengo, sabiéndole explicar al juez o a los operadores de justicia lo entienden, pero en otras ocasiones en su mayoría los abogados defensores no lo entienden.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	Estos temas son nuevos, en el área de investigaciones de Alta Tecnología de la Policía en la que trabajamos son de reciente conocimiento, y progresivamente estamos aprendiendo a preservar u conservar adecuadamente las evidencias digitales, para que estos sean valorados adecuadamente como medios de prueba en un proceso judicial y que sirvan para determinar al responsabilidad de un presunto imputado, pero lamentablemente muchos operadores de justicia fiscales, jueces policial desconocen el correcto tratamiento de estas evidencias digitales .
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	No.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	Considero que el sistema judicial peruano NO reconoce adecuadamente esta diferencia, en vista que en la práctica la evidencia digital para ser aplicada pasa por reglas generales establecidas para la evidencia.

Consideramos que el sistema de justicia peruano SÍ reconoce las diferencias a nivel normativo y jurisprudencial, pero NO lo hace de manera adecuada en la práctica judicial cotidiana empleado por los operadores de justicia.

Tabla 4.

¿Qué consecuencias ha observado cuando no se garantiza adecuadamente la cadena de custodia en pruebas digitales?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Las consecuencias serían que pueda llegar material manipulado, alterado se presente medios de pruebas no auténticos o deteriorados, llegamos a juicio con CDS, DVDS, que luego no corren en la computadora no es porque no tenga cadena de custodia, sino que al haberse anexado sin la mínima condición a la carpeta se deterioran.
Dr.Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Hasta el momento yo no he visto mayor problema, pero entiendo que esto es por el desconocimiento de los operadores, vamos aponer un ejemplo, la policía ellos se satisfacen con capturas de pantallas, este tipo de evidencias puede ser hasta manipulable, puede duplicar o generar capturas falsas, ellos tienen a la mano los dispositivos que se les pone a la mano al momento de recepcionar las denuncias, desde ahí radica la importancia que nadie se está percatando de la fiabilidad de la autenticidad de las evidencias digitales, tampoco los ficales y jueces están haciendo mayor atingencia y con este tipo de evidencias están condenando, pero lo correcto sería que haga un abordaje adecuado, un a extracción adecuada con una cadena de custodia como el código Hash, pero nadie cumple eso y nadie tampoco ha observado, pero entiendo que prontamente ya los abogados empezaran a cuestionar este tipo de evidencia herrada que se está obteniendo.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	Las consecuencias serían que puedan ser eliminados, suprimidos y alterados la evidencia digital que se encuentra en un dispositivo.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Lo que he observado en los casos es que los casos se caen, pierden solidez, por ejemplo en los casos que estoy recibiendo se extraen los videos de un DVR no se generan adecuadamente el código Hash y con ello se interrumpe el debido proceso de la obtención de evidencia digital, y al final ya no se admite como prueba para un proceso penal.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	Referente a la pregunta, en la práctica se ve que estamos trabajando de manera empírica y por ello se invalida o se caen los casos en sus diferentes modalidades, dejando impune a los presuntos autores de delitos muy graves como por ejemplo pornografía infantil, ya que no se hace el manejo correspondiente.
Wilfredo FARFAN QUISPE abogado co ICAL N°93408	Favorece la absolución de Cibercriminales y otros delincuentes que dejan pruebas en los dispositivos electrónicos.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	Teniendo en consideración de que la cadena de custodia da fe de la autenticidad y originalidad de la prueba, al no realizarse de manera adecuada genera inadmisibilidad probatoria y nulidad del proceso.

Opinión crítica del investigador: Mi aporte crítico se centrar en categorizar cómo estas respuestas confirman la impunidad y la invalidez procesal como las principales consecuencias, destacando los puntos de falla específicos.

Tabla 5.

¿Cómo influye la falta de normas específicas sobre autenticidad digital en las decisiones judiciales sobre admisibilidad probatoria?

Nombre de Entrevistado	**Respuestas**
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Bueno, en este caso es a favor de la otra parte, al no tener la regulación quien presenta los controles de legalidad, conducencia pertenencia y utilidad casi todos se admiten ya será en la actuación si todos son auténticos.
Dr. Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Yo creo que no existe falta de pruebas sino el desconocimiento de los operadores de justicia, ya hay manuales donde establece la correcta extracción de las evidencias digitales, también ISOS internacionales donde se establece sobre la evidencia digital.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	Influye enormemente toda vez que las normas ayudarían a que se puedan recabar las evidencias digitales de manera oportuna y rápida en cualquier tipo de delitos.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Autenticidad viene a ser si el archivo digital es auténtico y si ha sido generado por un dispositivo, la pericia que se me solicita es auténtico generado por un dispositivo, sino ha sido manipulado, para ello se debe de acceder al metadato para poder determinar sobre la autenticidad y al no tener las herramientas y normas específicas dificultan el correcto y adecuado preservación de las evidencias digitales.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	La falta de una regulación específica y actualizada sobre la autenticidad y el tratamiento de la evidencia digital influye significativamente en las decisiones judiciales, variedad de criterios de los juzgadores el cual afecta la seguridad jurídica de un proceso penal.
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	Ya existen normas lo único que falta es la aplicación de las mismas.
Franco QUISPE abogada con ICAC N°	La falta de normas específicas sobre la autenticidad digital, durante los diferentes procesos crea un ambiente de incertidumbre, porque no existe un criterio técnico vinculante para evaluar la autenticidad de las pruebas digitales, por la evaluación de su autenticidad queda a discrecionalidad de los jueces y ello dificulta la admisibilidad probatoria.

Opinión crítica del investigador: Mi aporte crítico se centrará en la confusión que existe entre la existencia de manuales técnicos (ISOs/protocolos) y la ausencia de una norma legal vinculante, confirmando que esta confusión es la principal causa de la inseguridad jurídica.

Tabla 6.

¿Qué vacíos identifica usted en la legislación procesal penal peruana respecto a la incorporación de evidencia digital?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Bueno existe un vacío, no se ha regulado es un tema nuevo, pese que ya años venimos trabajando con tecnología no todos los delitos ser prueban con evidencia digital, no hay la cantidad suficiente de peritos para este tipo de evidencias digitales, no está en todo regulado.
Dr.Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	De algún modo talvez si, con los protocolos con los ISOS internacionales ya se puede completar, porque de exigir que exista en el código penal, en la Constitución, sería una legislación sobreabundante, creo que debe de haber actualizaciones para los operadores de justicia en esos temas de evidencia digital.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	Los vacíos serian que no es rápido y oportuna la obtención de las evidencias digitales por falta conocimiento y capacitación de los operadores de justicia, segundo que estos puedan ser homologadas en su oportunidad, y también los requerimientos que se hace ante el órgano judicial demanda mucho tiempo y hasta entonces la evidencia digital se pierde.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	La designación en las evidencias digitales del código hash que no son generados por los operadores de justicia como la Policía, La Fiscalía y los jueces, asimismo MD5, pero este programa tiene algunas dificultades y se recomienda el uso del código Hash.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	En si hay vacíos legales, ya que no existe una norma específica que indique que software o procedimientos establecidos se deberían de aplicar para la extracción y análisis de la evidencia digital y estos sirvan a los operadores de justicia incluido los abogados defensores.
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	Si bien es cierto los tribunales de justicia han realizado esfuerzos de interpretación en materia de prueba digital, lo cierto es que en el camino han desarrollado criterios con enfoques y sentidos distintos, circunstancia que colisiona frontalmente con el principio de seguridad jurídica. Por otro lado, en este último tiempo, observamos que la inteligencia artificial, sin dificultad, permite clonar, crear y recrear voces, imágenes y videos que tornan casi imposible distinguir una prueba real de una prueba editada con inteligencia artificial.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	La falta de normas que regulen de manera sistemática la obtención y preservación de las evidencias digitales y la inexistencia de normas que establezca la cadena de custodia para el tratamiento de las evidencias digitales.

Opinión crítica del investigador: La confusión entre la norma y el protocolo y cómo esta confusión perpetúa la inseguridad jurídica y la obsolescencia del sistema ante la Inteligencia Artificial (IA).

Tabla 7.

¿Considera que estos vacíos legales afectan la valoración y eficacia de la prueba digital en los procesos penales?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Si, afectan, pero es suplida de alguna forma con que nadie cuestione la evidencia digital, y de hacerlo tendría que probarlo que no es auténtico o ha sido manipulado.
Dr. Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Si podría en algún momento, pero en la actualidad no veo mayor problema con alguno de los operadores, actualmente se está gestionando mayor capacidad operativo respecto a dispositivos que ayuden a la obtención de estas evidencias digitales.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	Por supuesto, justamente con que no haya normas que aceleren o existan normas específicas sobre la materia de evidencia digital, hacen que acarree que estas sean borradas o eliminadas y con ello no puede a determinarse la responsabilidad penal o la inocencia de un procesado.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Si, considero que esos vacos legales afectan enormemente la valoración de las pruebas digitales dentro de un proceso penal.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	Claro, la falta de elaboración de la extracción y conservación de las evidencias digitales, conllevan a la dificultad de los operadores de justicia.
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	Claro que sí.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	Si, toda vez que estos vacíos legales son el principal obstáculo para la correcta valoración de la evidencia digital por los jueces, que no se ven obligados a seguir estándares técnicos para su valoración quedando a discrecionalidad de los mismos generando con ello una inseguridad jurídica.

Opinión crítica del investigador: Nuestra opinión en base a las respuestas de los entrevistados es que, la peligrosa complacencia revelada en algunas respuestas y la confirmación de que la impunidad por caducidad de la prueba es la consecuencia más grave y reconocida.

Tabla 8.

¿Considera usted que los operadores del sistema penal cuentan con suficiente capacitación técnica sobre evidencia digital?

Nombre de Entrevistado	Respuestas
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	No, se tiene esta capacitación, muchas veces no hay cursos respecto a estas materias, hace dos años se ha creado fiscalías especializadas sobre delitos informáticos, pero solamente en Lima, entonces muchos fiscales viajan a capacitarse hacer pasantías, pero no los abogados, no los policías no los jueces.
Dr. Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Creo que no, creo que nos fala a todos los operadores, como es la policía, Ministerio Publico, jueces, abogados, defensores públicos para que de esta manera se pueda dar cumplimiento a la norma sobre la evidencia digital.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	No, porque es un tema nuevo en nuestro sistema, considero yo que debe haber una mayor capacitación para los operadores de justicia para los temas de evidencia digital.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Yo considero que estamos en camino, la Policía y el Ministerio público recibimos algunos cursos de capacitación, pero no lo penen en práctica.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	La Policía Nacional De Perú, en el campo de la investigación criminal está siendo capacitado respecto a la evidencia digital, pero en una minoría ya que es un tema nueva y reciente y la Policía no destina los recursos para capacitar a todo el personal policial del campo de la investigación criminal, ya que es importante que todo efectivo policial conozca sobre esos temas de evidencia digital.
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	No.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	NO, en vista que los operadores del sistema penal (jueces, fiscales, abogados y personal policial), no reciben una capacitación de manera conjunta y de haberla recibido lo han realizado de manera individual y con ello se genera una capacitación desigual y heterogenia, sin unidad de criterio.

Opinión crítica del investigador: La insuficiencia de capacitación técnica en el sistema penal peruano es generalizada, geográficamente sesgada e ineficaz en su aplicación práctica. Las respuestas confirman que, a pesar de la existencia de algunos esfuerzos puntuales (R4, R5), el sistema carece de la infraestructura y el compromiso de recursos necesarios para abordar este problema de manera integral. La consecuencia directa de esta insuficiencia es la consolidación de los vacíos legales en la práctica: si la ley no exige el rigor (vacío normativo) y el operador no sabe cómo aplicarlo (vacío de capacitación), la impunidad técnica está garantizada.

Tabla 9.

*¿Qué impacto cree que tiene esta falta de formación especializada en la eficiencia del proceso penal y en la valoración de las pruebas digitales***?**

Nombre de Entrevistado	**Respuestas**
Dr. Miguel Wesly ASTETE REYES Juez Superior Provisional de Cusco.	Por el momento no hay un impacto evidente o notorio debido a que no se utiliza mucho, se sigue trabajando a la antigua para la conservación de las pruebas digitales y quien lo cuestiona tendría que demostrar que ese esta manipulado, editado mediante un perito, el problema es que al no cuestionar las partes muchas veces se están pasando hasta pantallazos de WhatsApp, impresiones de chat comunicaciones o algunas grabaciones sin autorización que podrían incluso considerarse como prueba fidedigna y sirvan para un futuro sentencia condenatoria.
Dr. Alain Alberto MIRANDA SOLIS Fiscal Provincial penal de Wanchaq	Prácticamente lo que está pasando, se puede condenar a un inocente con una prueba de evidencia digital creada, alterada, modificada, se puede condenar o procesar a una persona que no estaba en un lugar con una captura de pantalla creada, modificada, y esto es una aberración al no tener los adecuados protocolos y si no se tienen a la vanguardia estos protocolos actualizados se va a tener sentencias injustas inocentes sentenciados injustamente.
Dr. Álvaro Justo CCASANI TUNQUIPA Fiscal Adjunto Provincial Penal de Wanchaq.	El impacto que va a acarrear es que en un caso no tenga pronóstico favorable o no se llegue a recabar la información sobre la evidencia digital y posiblemente se llegue a archivar.
Ronald Henry MOTTA GONZA S1 PNP Perito Informático de la PNP.	Defectivamente negativo, por ejemplo, si me traen un celular con evidencia digital y este no ha sido recogido debidamente un culpable podría ser puesto en libertar o un inocente sentenciado de manera injusta.
Jaime MAMANI APAZA S2 PNP Policía de Investigaciones de Delitos de Alta Tecnología DEPINCRI PNP CUSCO	El impacto es negativo, toda vez que la falta de capacitación del personal policial y demás operadores de justicia no permite que estas evidencias digitales sean valoradas y sirvan para determinar la responsabilidad do inocencia de un imputado, pese que hay peritos informáticos expertos sin embargo no contamos con herramientas o softwares.
Wilfredo FARFAN QUISPE abogado con ICAL N°93408	La mala interpretación de la normal y la errada dilucidación en procesos penales.
Yanet Valeria FRANCO QUISPE abogada con ICAC N°9099	Considero que un impacto negativo en vista que la falta de especialización de los operadores de justicia, es el tratamiento de la evidencia digital hace que no se valoren de manera objetiva las pruebas digitales y con ello se genera la ineficacia del proceso penal.

Opinión crítica del investigador: La falta de formación prolonga los procesos y disminuye la confiabilidad de la evidencia digital, haciendo al sistema penal ineficiente y vulnerable a los desafíos de la delincuencia moderna.

5.2. Discusión

Discusión de resultados por objetivos

Teniendo en cuenta el enfoque de investigación cualitativo aplicado al derecho, este apartado se desarrollará por objetivos, considerando las bases teóricas, los antecedentes, las entrevistas y la propia opinión del investigador.

Objetivo general:

Analizar de qué manera el inadecuado tratamiento práctico de la evidencia digital genera dificultades en su obtención, conservación, análisis y admisibilidad dentro del proceso penal.

Las bases teóricas desarrolladas desde el plano conceptual señalan que la evidencia digital se define como información intangible, volátil y susceptible de alteración, almacenada o transmitida mediante sistemas informáticos. Según la teoría jurídica especializada, el carácter único de las pruebas implica que su obtención indebida, su contaminación o su destrucción durante los procesos iniciales de recopilación afectan directamente a su correcta obtención y posterior evaluación en los juicios penales.

Los problemas relacionados con la conservación de las pruebas digitales se derivan de sus características inherentes, entre las que se incluyen su capacidad de duplicación, su sensibilidad a la manipulación y su volatilidad, así como la falta de normas técnicas suficientes y el incumplimiento de la cadena de custodia. Debido a esto, la gente comienza a dudar de su fiabilidad y validez, lo que reduce su valor probatorio e impide un análisis forense más profundo.

Igualmente importantes para la evaluación de las pruebas digitales son sus principios rectores: relevancia, fiabilidad y suficiencia. La verificación de la integridad de los datos se ve

obstaculizada por el uso inadecuado o inexistente de estos principios en conjunción con herramientas tecnológicas como los códigos hash, lo que pone en duda la fiabilidad del análisis de los expertos y la validez de los resultados.

Además, de acuerdo con las normas que rigen la admisión de pruebas y los fundamentos teóricos del sistema de justicia penal del Perú, las pruebas digitales deben ser técnicamente sólidas y haberse obtenido y conservado legalmente, de conformidad con las normas del debido proceso. En este contexto, las pruebas digitales pueden ser excluidas del expediente del caso como consecuencia de una gestión ilegal, del derecho a la defensa o de consideraciones legales relacionadas con la cadena de custodia.

Debido al rápido avance tecnológico, la formación inadecuada de los funcionarios judiciales y la falta de leyes claramente definidas, han persistido los problemas con la recolección, el almacenamiento, el análisis y la admisibilidad de las pruebas digitales. En teoría, esto significa que es necesario mejorar los estándares técnicos y legales para garantizar que el sistema de justicia penal del Perú administre la justicia de manera efectiva, lo cual es el objetivo principal.

El objetivo principal del estudio fue determinar cómo las pruebas digitales pueden verse alteradas para dificultar su recopilación, almacenamiento, análisis y admisión en los procesos penales. Los ejemplos que se han estudiado, tanto a nivel nacional como internacional, respaldan este objetivo.

Layana (2023), García (2023) y Bujosa, Bustamante y Toro (2021) coinciden en que el rápido avance tecnológico ha convertido a las pruebas digitales en un elemento esencial de la demostración, y que las deficiencias normativas, las sentencias judiciales contradictorias y las violaciones de los derechos fundamentales son consecuencia de una regulación y una gestión técnica insuficientes. Las pruebas aquí presentadas muestran que las pruebas digitales a

menudo se recogen y evalúan de forma deficiente debido a la falta de criterios técnicos especializados, a la formación inadecuada de los empleados del sistema judicial y a la ausencia de protocolos claros. También confirman que las pruebas digitales requieren un enfoque diferente al de las pruebas tradicionales debido a sus características técnicas.

Además, Quispe (2024) y Chávez (2024) constataron en su investigación nacional que Perú aún tiene un largo camino por recorrer, tanto en materia de legislación como de tecnología, para gestionar correctamente las pruebas digitales. La inestabilidad de los datos, la cadena de custodia inadecuada y la vulnerabilidad a la manipulación hacen que su validez e integridad sean inciertas. Esto significa que no se utilizarán en casos penales como prueba y no serán admisibles.

Los resultados muestran que las pruebas digitales representan un problema común en muchos sistemas jurídicos, sobre todo en lo que tiene que ver con su recopilación, almacenamiento, evaluación y admisión como prueba. Este estudio de caso respalda la tesis principal del artículo: el manejo poco eficaz de las pruebas digitales se debe a fallas institucionales, jurídicas y técnicas que terminan obstaculizando la administración efectiva de la justicia penal.

En un intento por cubrir un vacío en la literatura existente, este estudio ofrece un análisis jurídico bastante completo que ayuda a entender el problema en el contexto peruano y propone marcos teóricos sólidos para mejorar el manejo de las pruebas digitales en los juicios penales.

El objetivo de la investigación es entender cómo el sistema de justicia penal en Perú maneja las pruebas digitales y cómo su administración deficiente afecta su recopilación, almacenamiento, análisis y admisibilidad. Las conversaciones con abogados, jueces, fiscales, expertos en informática y autoridades policiales han dado resultados que respaldan y refuerzan este objetivo.

Según todos los entrevistados, las pruebas digitales son muy distintas a las pruebas físicas. Son más fáciles de manipular, se pueden copiar sin problema, necesitan verificación con tecnología y además pueden ser modificadas. Esto refuerza la idea de que los métodos tradicionales usados para manejar pruebas físicas resultan insuficientes e incluso riesgosos cuando se trata de datos digitales, ya que estas afirmaciones muestran que las pruebas digitales requieren un manejo especial y más especializado.

En segundo lugar, respecto al reconocimiento de estas diferencias por parte del sistema judicial peruano, existe una gran brecha entre lo que reconoce el poder legislativo y lo que en realidad hacen los jueces. Se mencionan decisiones legales y manuales técnicos, pero la mayoría piensa que no sirven de mucho, porque les falta información, experiencia o incluso conciencia sobre el tema. Como resultado, aparecen problemas serios relacionados con la recolección y el almacenamiento desordenado de las pruebas digitales.

Además, los hallazgos sobre la cadena de custodia digital muestran que el incumplimiento trae consecuencias graves, como la nulidad procesal de las pruebas, la reducción de los casos, la destrucción de evidencias y hasta la posibilidad de impunidad en delitos graves. Los procedimientos técnicos mal hechos afectan la credibilidad y la validez de las pruebas, lo que también repercute en su admisión y evaluación en los tribunales. Entre estos procedimientos se incluyen la generación incorrecta de códigos hash, la extracción forense y la documentación especializada.

Según los encuestados, las sentencias judiciales se ven afectadas de manera negativa por la falta de regulaciones legislativas claras sobre la autenticidad digital, lo que genera normas contradictorias y disminuye la seguridad jurídica. Además, se nota una confusión constante entre la existencia de manuales técnicos y los estándares internacionales (ISOs) y la

ausencia de una norma legal vinculante, lo cual provoca inseguridad jurídica y debilita el control de legalidad en la admisión de la prueba digital.

Los resultados muestran que la normativa sobre el proceso penal en Perú no define con claridad los procedimientos, el software, las normas ni los plazos para obtener pruebas digitales. La falta de supervisión, sumada al aumento de riesgos de manipulación, falsificación y fabricación de pruebas que traen los avances tecnológicos, como la inteligencia artificial, hace que el sistema de justicia penal quede seriamente comprometido.

Teniendo en cuenta que las pruebas digitales se pierden, borran o eliminan con mucha más facilidad del expediente, los entrevistados sostienen que estas deficiencias legales dificultan su evaluación y uso para determinar la culpabilidad o inocencia. El sistema acusatorio y el debido proceso se ven amenazados por una tendencia preocupante hacia la normalización del examen inadecuado de las pruebas.

Según los resultados, existe un problema sistemático con la capacitación técnica de quienes operan el sistema de justicia penal. El sistema de justicia penal es ineficiente debido a la capacitación actual, que es limitada, centralizada y rara vez se utiliza en la práctica. La fiabilidad de las pruebas digitales se ve disminuida, aumenta la posibilidad de veredictos incorrectos y se prolonga la duración de los procedimientos legales debido a esta deficiencia en la capacitación.

En conjunto, los resultados de las entrevistas confirman que el inadecuado tratamiento de la evidencia digital en el sistema penal peruano responde a una combinación de vacíos normativos, deficiencias técnicas y falta de capacitación especializada, lo cual impacta negativamente en su obtención, conservación, análisis y admisibilidad, afectando la eficacia del proceso penal y la tutela de los derechos fundamentales.

a. Naturaleza jurídica diferenciada de la evidencia digital frente a la evidencia física

Debido a su naturaleza intangible, volátil y fácilmente alterable, las pruebas digitales se distinguen de las pruebas físicas o escritas tradicionales a los ojos de la ley. Las pruebas digitales requieren medidas técnicas adicionales para garantizar su integridad, autenticidad e inmutabilidad, a diferencia de las pruebas tangibles, que pueden verse y cuya validez queda garantizada en gran medida por la cadena de custodia tradicional.

Según el derecho penal contemporáneo, las pruebas digitales necesitan un tratamiento probatorio especializado, ya que no son objetos tangibles, sino información guardada en soportes electrónicos. La aplicación indiscriminada de leyes pensadas para pruebas físicas ignora las complejidades técnicas de la información digital y termina violando conceptos de fiabilidad y legalidad probatoria. Por eso, la legislación procesal penal debería reconocer un marco probatorio específico basado en criterios tecnológicos, como la creación de códigos hash, la trazabilidad y la preservación forense.

b. Cadena de custodia digital, autenticidad y debido proceso penal

La cadena de custodia digital, como una estructura jurídica y procesal clave, asegura que los datos digitales se mantengan intactos para fines probatorios. Su objetivo principal es proteger las pruebas digitales contra la manipulación, la pérdida o la alteración, y garantizar que las pruebas presentadas en los tribunales sean coherentes con las que se obtuvieron durante la investigación.

Dado que surgen dudas sobre la fiabilidad de las pruebas cuando la cadena de custodia digital no se aplica o se aplica mal, los conceptos de validez probatoria y debido proceso se ven debilitados. Una decisión judicial válida no puede basarse en pruebas que no tengan verificación técnica de validez, según una visión jurídica más proteccionista. En el tribunal, las pruebas que no son tan relevantes, como ciertos datos obtenidos de experimentos, un código

hash incorrecto o la falta de interpretación por parte de un experto, pueden ser ignoradas o recibir menos peso.

Además de debilitar la capacidad de la parte contraria para presentar un contraargumento técnico sólido, aceptar pruebas digitales sin una verificación completa va en contra del principio acusatorio. Según la teoría del proceso penal, la cadena de custodia digital funciona más como una garantía para asegurar un juicio penal imparcial que como una simple formalidad.

c. Vacíos normativos, capacitación insuficiente y seguridad jurídica en el proceso penal

La seguridad jurídica se ve debilitada por la falta de normas claras para la recopilación, el almacenamiento y la evaluación de las pruebas digitales, lo que constituye una deficiencia normativa importante. Desde una perspectiva jurídico-teórica, esto genera una dificultad, ya que los procesos institucionales, las normas internacionales y las guías técnicas existentes no tienen fuerza jurídica vinculante. Como consecuencia, aparecen distintas interpretaciones y sentencias judiciales contradictorias.

La brecha normativa se agrava y la aplicación coherente y estricta de los requisitos probatorios se ve obstaculizada por la falta de formación técnica adecuada entre el personal del sistema de justicia penal. Dado que la evaluación de las pruebas digitales en este caso depende de la competencia tecnológica del operador más que de normas claramente definidas, la equidad procesal se ve comprometida.

Además, las nuevas preocupaciones sobre la manipulación, falsificación y fabricación de pruebas digitales provocadas por la IA y otros avances tecnológicos exigen un enfoque diferente por parte de las comunidades regulatoria y jurídica. La falta de una legislación clara y de capacitación especializada crea un entorno de incertidumbre jurídica, lo que socava la

eficacia de los procesos penales y pone en peligro la protección de los derechos fundamentales del acusado.

Las pruebas digitales deben reconocerse como un tipo de evidencia distinto, que necesita mayores garantías jurídicas y técnicas, según el análisis de estas tres áreas fundamentales del derecho. La falta de un marco normativo bien definido, la aplicación deficiente de la cadena de custodia digital y la formación insuficiente del personal del sistema generan un problema sistémico en la justicia penal peruana, que termina debilitando la legitimidad, la certeza y la justicia sustantiva.

Según los hallazgos y la investigación, las pruebas digitales necesitan una supervisión regulatoria y técnica especializada por su naturaleza jurídica particular. Lamentablemente, la falta de requisitos legales claros, la aplicación incorrecta de la cadena de custodia digital y la formación insuficiente del personal judicial hacen que el sistema de justicia penal en Perú no maneje bien las pruebas digitales. Esto genera dudas sobre su fiabilidad, validez y aceptación, lo que termina provocando inseguridad jurídica y la posibilidad de injusticias y violaciones del debido proceso.

En consecuencia, se sostiene que se ha cumplido con el logro del objetivo general.

Objetivo específico 1:- Precisar cuáles son las características particulares de la evidencia digital que exigen un tratamiento diferenciado respecto a la evidencia física en el proceso penal.

Partiendo de los conceptos teóricos ya mencionados, se colige que las pruebas digitales difieren fundamentalmente de las pruebas físicas tradicionales, por lo que requieren un marco probatorio específico.

En efecto desde una perspectiva teórica, las pruebas digitales no pueden existir como objetos físicos, ya que se trata de información almacenada de forma electrónica. Si bien es posible determinar rápidamente la existencia y el estado de las pruebas físicas, esta característica hace que las pruebas digitales no puedan percibirse con los sentidos y exige el uso de herramientas tecnológicas para su detección, recuperación y análisis.

Dado que los datos pueden modificarse, borrarse o incluso reconstruirse de manera instantánea, sin importar la intención del usuario, las pruebas digitales son por naturaleza inestables. Por eso es clave actuar con rapidez y con competencia técnica durante la recolección, ya que cualquier manejo incorrecto o retraso puede terminar en la pérdida irrecuperable de la información probatoria.

La capacidad de generar muchas réplicas exactas del original es posible gracias al cumplimiento de normas forenses adecuadas, que son atributos clave. Sin embargo, esta misma característica hace que la manipulación o el cambio sean más probables cuando no existen procedimientos de verificación, como pasa con las pruebas físicas tradicionales que no generan códigos hash.

Debido al predominio de la tecnología avanzada y la inteligencia artificial en el entorno actual, las pruebas digitales son especialmente vulnerables a ser alteradas y manipuladas. Esta característica resalta la necesidad de verificar su autenticidad, integridad y trazabilidad, a diferencia de las pruebas físicas, donde suele ser más sencillo detectar modificaciones.

Al manejar pruebas digitales, es fundamental contar con expertos en informática forense, seguir los procesos adecuados, mantener las evidencias dentro de una cadena de custodia digital y asegurarse de cumplir ciertos estándares tecnológicos. En los procesos judiciales, las pruebas digitales resultan vulnerables, poco confiables y muchas veces terminan siendo rechazadas porque no se aplican estos estándares.

Como resultado, el sistema de justicia penal debe adoptar un enfoque especializado para garantizar la recopilación, conservación y evaluación adecuadas de las pruebas digitales debido a sus características únicas, que incluyen ser intangibles, volátiles, duplicables, susceptibles de manipulación y requerir verificación técnica.

El Objetivo Específico 1 estuvo orientado a precisar las características propias de la evidencia digital que exigen un tratamiento distinto al de la evidencia física en el proceso penal. Esto se ve ampliamente respaldado por los antecedentes de investigación revisados tanto a nivel internacional como nacional. En conjunto, dichos estudios coinciden en que la evidencia digital presenta rasgos técnicos y jurídicos particulares que no pueden ser abordados con las reglas tradicionales aplicables a la evidencia material.

Según la investigación de Layana (2023), el rápido avance de las tecnologías de la información ha superado la capacidad de adaptación del derecho penal y de sus profesionales. Esto ha generado un vacío jurídico y práctico que dificulta la evaluación adecuada de las pruebas digitales. En este contexto, dichas pruebas se caracterizan por su complejidad técnica y por el hecho de que los entornos digitales están en constante evolución. Como resultado, requieren una gestión especializada que se diferencia de los estándares más estables y tradicionales aplicados a las pruebas físicas.

El entorno tecnológico actual exige una ampliación del concepto de prueba digital, según García (2023). Esto demuestra que las pruebas digitales incluyen todo tipo de información y van más allá del mero material físico. Este hallazgo pone de relieve la necesidad de adoptar una técnica probatoria específica que garantice una autenticación y evaluación suficientes en los procesos penales, teniendo en cuenta la intangibilidad y la diversidad de las formas de pruebas digitales.

Bujosa et al. (2021) señalan que las pruebas digitales, especialmente aquellas obtenidas mediante tácticas de vigilancia encubierta, necesitan reformas legislativas inmediatas para garantizar su legitimidad, autenticidad e integridad. En este sentido, se pueden identificar características propias de las pruebas digitales, como su alta susceptibilidad a la manipulación y la necesidad de contar con protecciones técnicas reforzadas. Estas particularidades no están presentes en las pruebas físicas y exigen procedimientos probatorios distintos. Según Quispe (2024), aunque la digitalización de los procesos penales en el ámbito nacional mejora la eficiencia procesal, también genera serias preocupaciones sobre la fiabilidad y la validez de las pruebas digitales. Debido a su carácter volátil y manipulable, los datos digitales requieren regulaciones estrictas y una cadena de custodia específica. El ensayo defiende el uso de las pruebas digitales y explica en qué se diferencian de las pruebas físicas tradicionales.

Por su parte Chávez (2024), las leyes de gestión de datos de Perú adolecen de una falta de regulación, lo que reduce la utilidad de los datos digitales como prueba. La dependencia de criterios tecnológicos para evaluar la validez y la fiabilidad de las pruebas digitales subraya sus atributos únicos y requiere un marco regulatorio independiente, diferente al que rige las pruebas físicas, como ilustra esta conclusión.

Debido a su intangibilidad, volatilidad, susceptibilidad a la manipulación, diversidad de formas y dependencia de procedimientos tecnológicos especializados, las pruebas digitales en los casos penales requieren un tratamiento distinto al de las pruebas físicas. Así lo demuestra el caso que se analiza. Las conclusiones resaltan la importancia del Objetivo Específico 1, que impulsa al sistema de justicia penal a reconocer las pruebas digitales como un tipo independiente. Todos los entrevistados coincidieron en que las características técnicas y jurídicas únicas de las pruebas digitales dificultan su incorporación a las normas estándar que rigen las pruebas físicas.

Los participantes entrevistados señalaron que, a diferencia de las pruebas tangibles, las pruebas digitales no existen en forma física, sino como información almacenada o transmitida a través de sistemas informáticos. Al ser datos intangibles, su identificación, incautación y conservación requieren métodos tecnológicos más sofisticados y un análisis profesional especializado.

Según las personas con las que hablamos, los datos digitales son intrínsecamente inestables, lo cual es una de las principales razones por las que necesitan un cuidado especial. Los participantes sostienen que el riesgo de pérdida de pruebas se ve agravado porque el material digital puede modificarse, eliminarse o sobrescribirse fácilmente, a menudo sin intervención humana. En este caso se requieren procesos rápidos y protocolos técnicos específicos, que son superfluos cuando se trata de pruebas físicas comunes. La mayor vulnerabilidad de las pruebas digitales frente a la manipulación y la réplica fue una de las principales preocupaciones de los participantes. Para asegurar la autenticidad e integridad de los activos digitales, los expertos jurídicos subrayan la necesidad de contar con métodos de verificación técnica, como sistemas de autenticación y herramientas forenses. Por ello, la información digital resulta más expuesta a la corrupción o duplicación que las pruebas físicas, las cuales suelen estar sujetas a normas estrictas.

Una característica clave de las pruebas digitales, según los encuestados, es la necesidad de contar con conocimientos técnicos específicos. A diferencia de las pruebas tangibles, las digitales no pueden observarse a simple vista. Su fiabilidad dentro de los procedimientos judiciales depende en gran medida de la experiencia de los especialistas en informática, quienes son responsables de su extracción, almacenamiento y análisis. Esto subraya la importancia de una gestión experta de las pruebas digitales.

Según los resultados de las entrevistas, existen procedimientos inconsistentes en cuanto al manejo de las pruebas digitales en todo el sistema judicial debido a la falta de procedimientos regulados y de leyes claras. Los encuestados coinciden en que debería haber normas claras para diferenciar entre las pruebas digitales y las físicas en los juicios penales, ya que la ausencia de estandarización aumenta el riesgo de violaciones del debido proceso y del derecho a la defensa.

Según los participantes entrevistados, las pruebas digitales se diferencian de las pruebas físicas por ser etéreas, volátiles, fácilmente manipulables y requerir conocimientos tecnológicos especializados. Estos hallazgos empíricos respaldan el Objetivo Específico 1, que establece que las pruebas digitales deben ser controladas mediante un procedimiento probatorio imparcial y especializado en los procesos penales.

Las pruebas digitales, según la teoría del proceso penal, posee una esencia jurídica propia y única debido a ciertas características técnicas y funcionales. Su carácter intangible requiere una mediación tecnológica para su adopción y evaluación por parte de los tribunales. La idea de autenticidad se ve afectada por su volatilidad y mutabilidad, lo que exige una cadena de custodia digital más estricta y técnicas de conservación específicas.

Asimismo, la duplicación ilimitada de datos pone en duda la idea convencional del original probatorio y desplaza la atención hacia la credibilidad del contenido informativo. Se requiere un examen exhaustivo de la proporcionalidad y la legalidad, ya que la recopilación de datos tiene un impacto sustancial en derechos fundamentales, como la privacidad y la protección de datos. Se requiere un nuevo enfoque de la legislación y la doctrina para abordar el uso de la prueba digital en los casos penales.

La evidencia digital presenta características propias como su intangibilidad, volatilidad, facilidad de manipulación y dependencia de conocimientos técnicos especializados, que la diferencian sustancialmente de la evidencia física. Todo esto exige un tratamiento probatorio

específico y adaptado a su naturaleza diferenciado en el proceso penal. Estas particularidades poseen incidencia directamente en su obtención, preservación, autenticación y valoración judicial, y evidencian que la aplicación de criterios tradicionales resulta insuficiente para garantizar su fiabilidad y el respeto al debido proceso, por lo que se justifica la necesidad de reglas y protocolos específicos para su adecuada incorporación como medio de prueba.

Objetivo específico 2: Examinar cómo afecta la falta de capacitación de jueces, fiscales y policías en el tratamiento de evidencia digital al desarrollo eficaz del proceso penal.

Los fundamentos teóricos analizados respaldan la idea de que la eficacia de los procesos penales se ve afectada negativamente por la falta de formación especializada de jueces, fiscales y policías en el manejo de pruebas digitales. En cuanto al debido proceso, una capacitación técnica insuficiente pone en riesgo la supervisión legal de los procedimientos probatorios y, aun cuando existen normas procesales, su aplicación deficiente termina debilitando la protección efectiva de los derechos fundamentales y el equilibrio de poderes entre las partes.

Se necesitan especialistas en informática forense, conservación y verificación de la autenticidad para descifrar las pruebas digitales de manera que se cumplan las normas legales vigentes, debido a su complejidad. Sin estos conocimientos, es mucho más probable que se cometan errores durante la recopilación, la conservación y la presentación. Debido a problemas de admisibilidad y a la disminución del valor probatorio, una formación insuficiente socava la eficacia de los procesos penales.

Una capacitación inadecuada obstaculiza la búsqueda de la verdad material al prolongar el proceso, introducir nulidades innecesarias y rechazar pruebas, todo lo cual es perjudicial para la eficiencia procesal. La emisión de sentencias por parte de los jueces es susceptible de estar

sujeta a sus evaluaciones subjetivas o empíricas de los hechos debido a la falta de conocimientos especializados, lo que podría dar lugar a sentencias arbitrarias.

Según los modelos teóricos, sin una formación especializada, el sistema de justicia penal pierde fiabilidad en un mundo digital en constante evolución. Tanto los casos concretos como el sistema en su conjunto muestran este comportamiento. Cuando los funcionarios encargados de hacer cumplir la ley no son capaces de manejar las pruebas digitales, el público pierde la confianza en la capacidad del sistema para abordar los delitos que implican el uso de la tecnología.

Según Layana (2023), la formación insuficiente del personal del sistema judicial es un problema importante en los procesos penales ecuatorianos en lo que respecta a la gestión de las pruebas digitales. Esto tiene un impacto negativo en la fundamentación de las sentencias judiciales y en la garantía del derecho a la defensa. Un aspecto importante para comprender el efecto de la formación en el debido proceso penal es la afirmación del autor de que una formación técnica inadecuada limita la comprensión de las pruebas digitales, lo que a su vez compromete la supervisión judicial y conduce a veredictos inconsistentes.

En la misma línea, García (2023) llegó a la conclusión de que la capacitación especializada de peritos, jueces y fiscales, así como las reformas normativas, son necesarias para la incorporación efectiva de las pruebas digitales en el sistema de justicia penal acusatorio. Esto se debe a que los errores en la recopilación y evaluación de pruebas digitales pueden deberse a la falta de conocimientos técnicos. Este antecedente es pertinente para el presente estudio al demostrar que la ausencia de capacitación afecta la eficacia probatoria y la correcta aplicación de los principios procesales.

Por su parte, Bujosa, et al. (2021) señalaron que el tratamiento de la prueba digital, especialmente aquella obtenida mediante vigilancia secreta, requiere operadores capacitados

en criterios técnicos y jurídicos para evitar vulneraciones a los derechos fundamentales. Los autores advierten que la falta de especialización incrementa la discrecionalidad judicial y compromete la sana crítica, reforzando la idea de que la capacitación es un elemento estructural para la legitimidad del proceso penal.

En el ámbito nacional, Quispe (2024) identificó que la insuficiente capacitación tecnológica de los operadores de justicia peruanos constituye uno de los principales factores que afectan el derecho a la prueba en la era digital. La autora concluye que esta carencia genera deficiencias en la cadena de custodia, problemas de autenticidad y retrasos procesales, impactando negativamente en la eficiencia del proceso penal y en la igualdad de armas.

De manera complementaria, Chávez (2024) sostuvo que la falta de formación especializada en evidencia digital impide una valoración probatoria adecuada, pues los operadores recurren a criterios empíricos o tradicionales que no responden a la complejidad técnica de los datos digitales. Este antecedente resulta relevante al evidenciar que el déficit de capacitación debilita la fuerza probatoria de la evidencia digital y afecta la calidad de las decisiones judiciales.

Según los encuestados, una de las principales deficiencias en la respuesta del sistema de justicia penal ante los delitos cibernéticos es la falta de capacitación especializada en materia de pruebas digitales para jueces, fiscales y agentes de policía. Según estudios empíricos, las pruebas digitales pueden recopilarse, conservarse y presentarse de manera incorrecta cuando los profesionales se basan en los estándares tradicionales aplicables a las pruebas físicas. Esto, a su vez, afecta la admisibilidad de las pruebas y la forma en que el tribunal las evalúa.

Los participantes también mencionaron el hecho de que, especialmente en las primeras etapas de una investigación, cuando las acciones de la policía son cruciales, la falta de conocimientos técnicos limita la capacidad de regular la legitimidad de los procedimientos

probatorios. Las ineficiencias procesales, la cadena de custodia digital defectuosa y la exclusión de pruebas contribuyen a esta situación, lo que a su vez alarga los procesos penales y pone en duda la idea de la eficiencia procesal.

Según las entrevistas, el hecho de que los jueces se basen en evaluaciones subjetivas o empíricas de los datos digitales, en lugar de utilizar un juicio racional sólido, es consecuencia de su falta de conocimientos técnicos y de que no cuentan con la formación adecuada para hacerlo. Finalmente, los entrevistados señalaron que esta carencia formativa impacta negativamente en la legitimidad del sistema penal, ya que la ciudadanía percibe una justicia desfasada frente al avance tecnológico, lo que reduce la confianza en las decisiones judiciales y en la eficacia del proceso penal.

Se vulneran el debido proceso, la legalidad probatoria y el buen juicio cuando los jueces, fiscales y agentes de policía no reciben formación especializada en la gestión de pruebas digitales. Esto se debe a que no es posible examinar adecuadamente la legalidad, autenticidad e integridad de las pruebas digitales. La discrecionalidad judicial se ve acentuada y el proceso penal se ve socavado debido a la falta de formación, lo que a su vez afecta a la equidad de las posiciones contradictorias y a la credibilidad de las decisiones judiciales adoptadas en respuesta a las dificultades tecnológicas que plantea la ciberdelincuencia. Los procedimientos penales ineficaces se deben a que los jueces, fiscales y agentes de policía carecen de capacitación específica en la gestión de pruebas digitales, lo que conduce a errores en la recopilación, el almacenamiento y la evaluación de las pruebas. Para administrar eficazmente la justicia en la era digital, se requiere la capacitación técnica de los trabajadores del sistema judicial; esta deficiencia pone en peligro el debido proceso, aumenta la discrecionalidad judicial y disminuye la legitimidad y la eficiencia del sistema.

VI. Conclusiones

PRIMERA.

El tratamiento inadecuado de la evidencia digital dentro del proceso penal ocasiona dificultades relevantes en todas las fases de su gestión, desde la obtención hasta la valoración judicial, y la falta de protocolos uniformes junto con las deficiencias en la preservación de la cadena de custodia digital y la limitada capacitación de los operadores de justicia afectan la integridad, autenticidad y fiabilidad de los elementos probatorios digitales, lo que repercute negativamente en su admisibilidad y valoración en el proceso penal y, en consecuencia, estas deficiencias comprometen la eficacia de la actividad probatoria y pueden incidir en la correcta administración de justicia.

SEGUNDA.

La evidencia digital posee características singulares como su naturaleza intangible, volatilidad, facilidad de alteración y capacidad de reproducción exacta sin pérdida de contenido, lo que la diferencia sustancialmente de la evidencia física y justifica un tratamiento especializado dentro del proceso penal, y estas particularidades generan riesgos específicos para la preservación de su integridad, autenticidad y fiabilidad, por lo que requieren la aplicación de procedimientos técnicos y jurídicos adecuados durante su obtención, conservación, análisis y valoración probatoria, y en consecuencia, la utilización de criterios diseñados para la evidencia material resulta insuficiente para garantizar su correcta incorporación y eficacia probatoria, pudiendo comprometer la validez jurídica de la prueba y la adecuada determinación de los hechos materia del proceso penal.

TERCERA

La falta de capacitación especializada de jueces, fiscales y efectivos policiales en el tratamiento de la evidencia digital repercute de manera negativa en el desarrollo eficaz del proceso penal al propiciar errores en su obtención, preservación, análisis y valoración probatoria y esta deficiencia limita la adecuada comprensión de los aspectos técnicos vinculados a la prueba digital, favorece decisiones discrecionales y aumenta el riesgo de nulidades o exclusiones probatorias y como consecuencia se debilita la aplicación correcta de los principios probatorios, se afecta el debido proceso y se reduce la eficacia de la respuesta del sistema de justicia penal frente a los desafíos propios del entorno digital.

VII. Recomendaciones

PRIMERA

Se recomienda al Ministerio de Justicia y Derechos Humanos promover la elaboración e implementación de lineamientos técnicos y jurídicos especializados para el tratamiento de la evidencia digital en el proceso penal, con el fin de uniformizar los procedimientos de obtención, conservación, análisis y valoración de este tipo de evidencia, garantizando su autenticidad, integridad y fiabilidad probatoria, así como fortaleciendo la seguridad jurídica y la eficacia de la administración de justicia frente a los desafíos derivados del entorno digital.

SEGUNDA

Se recomienda al Poder Judicial promover la elaboración e implementación de protocolos especializados para el tratamiento de la evidencia digital, con el fin de garantizar que su obtención, conservación, análisis y valoración probatoria se realicen conforme a sus características particulares de intangibilidad, volatilidad, facilidad de alteración y capacidad de reproducción, asegurando así la integridad, autenticidad, fiabilidad y eficacia jurídica de este tipo de prueba dentro del proceso penal.

TERCERA

Se recomienda al Ministerio Público implementar programas permanentes y especializados de capacitación en evidencia digital e informática forense para los fiscales, con el fin de fortalecer sus competencias en la obtención, conservación, análisis y utilización de la prueba digital, reduciendo errores que puedan comprometer su autenticidad, integridad y admisibilidad. Asimismo, ello contribuirá a evitar nulidades y exclusiones probatorias,

garantizar el respeto del debido proceso y fortalecer la eficacia de la investigación penal frente a los desafíos que plantea el entorno digital.

VIII. Referencias

Bujosa, L., Bustamante, M., y Toro, L. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal, 7(2), 1347*. https://doi.org/10.22197/rbdpp.v7i2.482

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). *Academic Press*.

Castañeda, C. (2021). Valoración de las pruebas bajo la teoría indiciaria en medios electrónicos. *Revista de Investigación Jurídica*.

Castillo, J. (2015). *Delitos informáticos y prueba digital en el proceso penal*. Fondo Editorial Jurídico.

Castillo, J. (2018). *La prueba digital en el proceso penal: Desafíos normativos y tecnológicos*. Fondo Editorial Jurídico.

Castillo, J. (2019). *La víctima en el proceso penal peruano*. Editorial Jurídica Grijley.

Castillo, J. (2020). *La víctima en el proceso penal acusatorio peruano*. Lima: Fondo Editorial Jurídico.

Castillo, J. (2021). *Presunción de inocencia y debido proceso en el sistema penal peruano*. Lima: Gaceta Jurídica.

Castro – Cuba, Y. E. (2019). *Investigar en Derecho. Texto de apoyo a la docencia universitaria*. Universidad Andina del Cusco.

Céspedes, M. (2018). *Teoría general de la prueba en el proceso penal*. Editorial Jurídica Peruana.

Chávez E. (2024). *La prueba digital y la validez probatoria en el proceso penal peruano*. (Tesis para optar por el título profesional de abogado, Universidad Nacional Santiago Antúnez de Mayolo). https://repositorio.unasam.edu.pe/backend/api/core/bitstreams/be30afa9-af13-49d7-a9ce-51c9d812d58d/content

Congreso de la República del Perú. (2013). Ley N.º 30096 - Ley de delitos informáticos. Diario Oficial El Peruano https://busquedas.elperuano.pe

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185)

Eusebio, A. (2020). *La evidencia digital en el proceso penal de la provincia de Buenos Aires.* (Tesis de licenciatura, Universidad Abierta Interamericana). https://dspaceapi.uai.edu.ar/server/api/core/bitstreams/c00e61ee-b2f6-4b82-ac9b-be3cec775de8/content

Farfán, J. E. (2024). *ISO 27037:2012 para mejorar el análisis informático forense en la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú*. (Tesis de Maestría, Universidad Nacional Federico Villarreal). https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/9138/UNFV_EUPG_Farfan_Chiun_Julio_Enrique_Maestria_2024.pdf?sequence=1&isAllowed=y

Fernández M. Urteaga P., Verona A. (2015). *Guía de Investigación en Derecho, Vicerrectorado de Investigación*. PUCP

García, M. (2017). *Etapas del proceso penal: análisis práctico del CPP peruano*. Editorial Jurídica Continental.

García, M. (2019) *Manual de Derecho Procesal Penal*. Lima: Gaceta Jurídica.

García, M. (2020). *Derecho procesal penal: Principios, estructura y garantías*. Editorial Jurídica Continental.

García, M. (2020). *Manual práctico del proceso penal peruano.* Lima: Gaceta Jurídica.

García, M. (2020). *Sistemas procesales penales: Teoría y práctica en América Latina.* Lima: Editorial Jurídica Continental.

García, O. (2023). *La incorporación de las pruebas digitales en el proceso penal acusatorio*. (Tesis para obtener el grado de Magister, Universidad Autónoma de Guerrero). http://200.4.142.40:8080/bitstream/handle/uagro/4208/TM_%20%2007134884_23.pdf?sequence=1&isAllowed=y

Gómez, R. (2016). Evolución histórica del proceso penal: del sistema inquisitivo al acusatorio. *Revista de Derecho Penal Comparado, 4(1), 55–78*.

Gonzales, P. (2017). *Derecho procesal penal: Parte general*. Fondo Editorial de la Universidad Nacional Mayor de San Marcos.

Gonzales, P. (2018). *Proceso penal y garantías constitucionales en el nuevo sistema procesal penal*. Fondo Editorial de la Universidad Nacional Mayor de San Marcos.

Gonzales, R. (2018). Imparcialidad y debido proceso en el juicio penal. *Revista Peruana de Derecho Penal, 5(2), 45–60.*

Gonzales, R. (2021). Características del nuevo proceso penal en el Perú. *Revista Peruana de Derecho Procesal, 12(2), 85–101.*

Hernández-Sampieri, R. (2018). *Metodología de la investigación*. McGraw-Hill Interamericana.

Herrera, J. (2023). *El papel de la prueba digital en los procedimientos penales en Ecuador* (Tesis de maestría, Universidad Andina Simón Bolívar). https://repositorio.uasb.edu.ec/bitstream/10644/10524/1/T4605-MDPE-Herrera-El%20papel.pdf

Julca, I., Segura, M. & Ordeano, D. (2025). *El reto de la ciberjusticia: criterios de valoración de la prueba digital en el Perú*. Llalliq**,** 5(2), 287–300. https://revistas.unasam.edu.pe/index.php/llalliq/article/view/1306/1412

Landáez, L. (2007). La equivalencia funcional, la neutralidad tecnológica y la libertad informática. *Revista de Derecho, Universidad de Carabobo*.

Layana, T. (2023). El tratamiento de la evidencia digital en el proceso penal y la motivación de las decisiones judiciales de acuerdo con la ley y el derecho a la defensa. (Tesis para obtener el grado de Magister, Universidad Central del Ecuador). https://www.dspace.uce.edu.ec/server/api/core/bitstreams/16a6d3b2-cf22-4ff7-ba01-40d2a3775225/content

López, F. (2019). *Manual práctico del proceso penal peruano*. Fondo Editorial Jurídico.

López, R. (2018). *Garantías del imputado en el proceso penal*. Editorial Jurídica Continental.

López, R. (2020). *Manual de derecho procesal penal*. Gaceta Jurídica.

López, R. (2021). Evidencia digital y cadena de custodia: Retos para su valoración probatoria en el Perú. *Revista Peruana de Derecho Procesal, 12(1), 45–60*.

Martínez, A., y Ríos, F. (2022). Aplicaciones de inteligencia artificial en la investigación penal: Retos y oportunidades. *Revista Iberoamericana de Ciencia Forense, 14(2), 88–105.*

Ministerio de Justicia y Derechos Humanos. (2004). Decreto Legislativo N.º 957 - Código Procesal Penal del Perú. Diario Oficial El Peruano.

Ministerio de Justicia y Derechos Humanos. (2004). Decreto Legislativo N.º 957 - Código Procesal Penal. Diario Oficial El Peruano (https://busquedas.elperuano.pe).

Ministerio del Interior. (2019). Manual para el recojo de la evidencia digital. https://cdn.www.gob.pe/uploads/document/file/1303962/DWP-ManualParaRecojo-EVIDENCIA.DIGITAL.pdf

Molina, A. (2020). Importancia de la evidencia digital en el proceso penal. *Revista Jurídica de Ciencias Forenses, 12(2), 45–58.*

Montece, F. (2020). Preservación de la evidencia digital en el procedimiento de cadena de custodia. *Revista RACI, 5(3), 1104.*

Naula, D. E., Quevedo, R., y Zamora, M. (2022). El protocolo de reconocimiento de medios digitales frente a la inobservancia del debido proceso penal. *Revista Arbitrada Interdiciplinarias KOINONIA*. https://dialnet.unirioja.es/descarga/articulo/8480994.pdf

Nessi, S. (2017). *Evidencia digital: Fundamentos técnicos y jurídicos*. Lima: Editorial Jurídica Continental.

Olivares, B., y Ceras, M. (2021). *Delitos informáticos y la evidencia digital en el proceso peruano del Distrito Judicial de Junín, 2020* (Tesis de licenciatura, Universidad Peruana Los Andes). https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2690/TESIS%20en%20formato%20PDF.pdf?sequence=1&isAllowed=y

Osco, M. (2021). La evidencia digital como medio de prueba en el proceso penal. Universidad César Vallejo.

Osco, M. A., Chipana, Y. M. M., García, G. B., Díaz-Pérez, J. J., y Calvo de Oliveira, D. G. (2025). La evidencia digital como medio de prueba en el proceso penal. Procuraduría General del Estado.

https://aulavirtualcfc.pge.gob.pe/pluginfile.php/40969/mod_resource/content/1/LA%20EVIDENCIA%20DIGITAL%20COMO%20MEDIO%20DE%20PRUEBA%20EN%20EL%20PROCESO%20PENAL.pdf

Pérez, A. (2018). El principio de contradicción en el modelo penal acusatorio peruano. *Revista Ius et Praxis, 10(1), 55–72.*

Pérez, J. (2018). *Modelos procesales penales y sus implicancias en el debido proceso*. Fondo Editorial Jurídico.

Piccirilli, M. (2019). Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos: legislación vigente, anteproyectos y Convenio de Budapest. P.G.E. https://repositoriouba.sisbi.uba.ar/greenstone/collect/adrespe/index/assoc/HWA_6501.dir/6501.PDF

Quintana, F. (2021). La justicia penal acusatoria en América Latina: Avances y desafíos. *Revista Latinoamericana de Derecho Procesal, 9(2), 33–50.*

Quintana, L. (2022). Juicio oral y principios procesales en el nuevo modelo penal. Revista Latinoamericana de Derecho Penal, 9(1), 44–61.

Quintana, M. (2020). *Los vacíos normativos en la regulación de la prueba digital en el sistema procesal penal peruano*. Editorial Jurídica Continental.

Quispe, E. (2024). *El impacto de la tecnología en el derecho a la prueba en el proceso penal: desafíos y perspectivas en la era digital*. (Tesis para optar por el título de Segunda Especialidad en Derecho Procesal, Pontificia Universidad Católica del Perú). https://tesis.pucp.edu.pe/server/api/core/bitstreams/7d8435b7-c162-4357-9964-5cc98d01865b/content

Reyes, M. (2024). La prueba digital en los procesos civiles y su prohibición. LATAM Revista Latinoamericana de Ciencias Sociales.

Schirakian, N. (2021). *Evidencia informática: ¿Un nuevo paradigma para el derecho procesal penal? Estudio básico y de enfoque cualitativo*. (Tesis para optar al grado de Maestro, Universidad de San Andrés). https://repositorio.udesa.edu.ar/items/6b0f7ca7-09f6-400b-92e6-8786d874ddc8

Solis, A. (2021). Metodología de la Investigación Jurídico Social. *San Bernardo Libros Jurídicos.*

UNCITRAL. (2017). Ley Modelo sobre documentos transmisibles electrónicos. Naciones Unidas.

Vargas, L. (2019). Capacitación de operadores jurídicos en evidencia digital: Una deuda pendiente. *Revista de Derecho y Tecnología, 8(2), 89–102*.

Los anexos, panel fotográfico y otros documentos están resguardados en la oficina de repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica de los Andes