ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

https://doi.org/10.59956/escpograpnpv4n2.14

Manejo de la evidencia digital en la investigación del delito de pornografía infantil

Handling digital evidence in the investigation of child pornography crimes.

Recepción del artículo: 22/12/2024 | Aceptación para publicación: 04/03/2025 | Publicación: 17/03/2025

Lelis Ludeña Díaz
43873104@escpograpnp.com

Henry Alexander Diaz Silva
44346846@escpograpnp.com

Djahani Francisco Calixto Velasquez
40067200@escpograpnp.com

Escuela de Posgrado de la Policía Nacional del Perú

Resumen

El estudio analiza el manejo de la evidencia digital en la investigación de delitos de pornografía infantil, destacando su complejidad técnica y jurídica. Se adopta un enfoque cualitativo con diseño hermenéutico, empleando análisis documental como técnica de recolección de datos. La muestra se basa en normativas nacionales, estudios previos y peritajes realizados en escenarios reales y simulados. Se examinan procedimientos clave como la cadena de custodia, la clonación bit a bit y el uso de software forense como EnCase y FTK. Los resultados revelan que la evidencia digital, por la facilidad de ser alterada, requiere protocolos rigurosos para su preservación y autenticación. Se identifican desafíos en la aplicación de normativas y en el combate al uso de cifrado en redes clandestinas. Se concluye que la implementación de estándares internacionales como ISO 27037 e ISO 27042 es indispensable para garantizar la trazabilidad y validez probatoria de la evidencia digital. Además, se resalta la necesidad de fortalecer la capacitación pericial en técnicas forenses avanzadas y el desarrollo de normativas específicas que permitan una respuesta más efectiva en el procesamiento penal de estos delitos.

Palabras clave: Pornografía infantil, evidencia digital, cadena de custodia.

Abstract

The study analyzes the handling of digital evidence in the investigation of child pornography crimes, highlighting its technical and legal complexity. A qualitative approach with a hermeneutic design is adopted, employing documentary analysis as the data collection technique. The sample is based on national regulations, previous studies, and forensic examinations conducted in real and simulated scenarios. Key procedures such as the chain of custody, bit-by-bit cloning, and the use of forensic software like EnCase and FTK are examined. The results reveal that digital evidence, due to its susceptibility to alteration, requires rigorous protocols for its preservation and authentication. Challenges are identified in the application of regulations and in combating the use of encryption in clandestine networks. It is concluded that the implementation of international standards such as ISO 27037 and ISO 27042 is essential to ensure the traceability and probative validity of digital evidence. Additionally, the need to strengthen forensic training in advanced forensic techniques and develop specific regulations to enable a more effective response in the criminal prosecution of these crimes is emphasized.

Keywords: Child pornography, digital evidence, chain of custody.

Para citar:

Ludeña, L., et al. (2025). Manejo de la evidencia digital en la investigación del delito de pornografía infantil. *ESCPOGRA PNP, 4*(2), 205-220. https://doi.org/10.59956/escpograpnpv4n2.14

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

Introducción

La expansión de las tecnologías de la información y comunicación ha transformado la manera en que las personas interactúan, facilitando un acceso inmediato y global a contenidos digitales. Sin embargo, este desarrollo también ha favorecido la proliferación de delitos cibernéticos, entre ellos la producción, distribución y consumo de material de pornografía infantil. La Interpol y el ICMEC han reportado un incremento sostenido en estos delitos, señalando que más del 70 % de los casos documentados utilizan plataformas digitales para su difusión, lo que dificulta la identificación y sanción de los responsables.

En el Perú, esta problemática ha seguido una tendencia similar. Durante el primer semestre de 2023, la Policía Nacional registró más de 120 casos de delitos vinculados a la pornografía infantil, lo que representó un aumento del 30 % en comparación con el mismo período del año anterior. Estos delitos se concentran principalmente en zonas urbanas, donde el acceso a internet es mayor y las redes sociales facilitan la captación y explotación de menores. Lima ha sido escenario de varios casos emblemáticos, como el desmantelamiento de una red que distribuía material ilícito a través de grupos en aplicaciones de mensajería, con más de trescientas víctimas menores de edad.

Las principales causas de esta problemática incluyen la falta de supervisión parental, la disponibilidad de dispositivos electrónicos y la ausencia de políticas eficaces en educación digital. Estas condiciones permiten que los agresores operen con relativo anonimato. Las consecuencias para las víctimas son devastadoras, con secuelas psicológicas y sociales severas, mientras que sus familias enfrentan la impunidad y la dificultad de acceso a justicia.

Esta investigación analiza el manejo de la evidencia digital en los casos de pornografía infantil, centrándose en la recolección y preservación de datos y su impacto en la investigación y resolución de estos delitos. Se busca establecer lineamientos que mejoren los procedimientos actuales y fortalezcan la capacidad operativa de la Policía.

La validez, objetividad y confiabilidad de la evidencia digital son aspectos centrales en este estudio. La validez garantiza que los procedimientos reflejen con precisión los hechos investigados; la objetividad exige que las intervenciones se realicen sin sesgos ni influencias externas; y la confiabilidad asegura que los métodos empleados produzcan resultados consistentes y reproducibles, fundamentales para la admisibilidad de las pruebas en juicio. La integridad y autenticidad de la evidencia digital, ya sea un documento electrónico o un mensaje de datos, son condiciones indispensables para su uso en los procesos penales.

Diversos estudios han señalado la necesidad de implementar estándares internacionales en el manejo de evidencia digital para mejorar la investigación y el procesamiento de delitos cibernéticos. Colmenares et al. (2024) destacan que el sexting constituye un factor de riesgo en la difusión de material ilícito, por lo que recomiendan un mayor control parental sobre el acceso de menores a la tecnología y redes sociales. De la Cruz y Pérez (2023) advierten que el tráfico de

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

pornografía infantil plantea retos tanto legales como tecnológicos, lo que exige una respuesta coordinada en el ámbito legislativo y operativo.

Palmeiro (2022) analizó el impacto de la pandemia de COVID-19 en la seguridad digital de niños y adolescentes, evidenciando que el aislamiento social y el uso intensivo de internet aumentaron la exposición a delitos sexuales en línea. En Brasil, el incremento de casos de pornografía infantil durante este período estuvo respaldado por estadísticas que reflejan un crecimiento en las denuncias. Afirmando Paredes (2024) que la pornografía infantil se ha convertido en una de las expresiones más graves de delincuencia digital, impulsada por la expansión de internet y el acceso a la Dark Web. Más allá de la producción y distribución de material ilícito, la simple tenencia de estos contenidos representa un desafío para las estrategias de control y regulación. Aunque en España se han fortalecido los marcos normativos, las redes de explotación infantil continúan operando mediante técnicas de anonimato y plataformas cifradas, lo que complica la labor de las autoridades.

Por su parte, Portugal (2024) examina cómo los delitos informáticos han transformado el marco jurídico en el Perú, resaltando la relevancia de la evidencia digital en los procesos penales. Su investigación enfatiza que la autenticación y preservación de esta evidencia presentan dificultades que requieren actualizaciones normativas y una capacitación más rigurosa para los operadores de justicia. Asimismo, señala que la carencia de herramientas tecnológicas y personal especializado limita la capacidad investigativa en estos delitos.

Método

Este estudio se fundamentó en un enfoque cualitativo, orientado a comprender de manera profunda y detallada las particularidades del manejo de la evidencia digital en la investigación de delitos de pornografía infantil. Este enfoque se seleccionó debido a su capacidad para captar las dinámicas subjetivas, los procesos técnicos y los marcos legales que influyen en este tipo de investigaciones, en concordancia con lo señalado por Barraza (2023), quien indica que los estudios cualitativos son ideales para explorar fenómenos complejos en contextos específicos.

El diseño metodológico adoptado fue el hermeneútico, que se orienta a la interpretación de textos, considerando el contexto en el que fueron producidos y los significados de su contenido. Este diseño no se limita a la descripción de la información, sino que busca comprender la intencionalidad del discurso, las estructuras y las influencias socioculturales (De la Espriella y Gómez, 2020).

Las técnicas de recolección fueron el análisis documental, que abarcó normativas nacionales sobre delitos de pornografía infantil, trabajos previos, y peritajes realizados a la evidencia en escenarios simulados y reales, con una perspectiva integral y contextualizada. Sosteniendo Hernández y Duana (2020) que esta técnica por su complementariedad en la generación de datos puede compenetrarse a favor de la investigación.

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

Resultados

El artículo 2° del Decreto Legislativo N° 1267 (2016) señala como función de la Policía en su inciso 12) que debe "Obtener, custodiar, asegurar, trasladar y procesar indicios, evidencias y elementos probatorios relacionados con la prevención e investigación del delito, poniéndolos oportunamente a disposición de la autoridad competente".

La evidencia digital es cualquier información almacenada o transmitida en formato electrónico que puede ser utilizada como prueba en investigaciones judiciales o técnicas, siempre que se garantice su integridad, autenticidad y trazabilidad mediante métodos adecuados. Su aplicación abarca delitos contra la vida, el cuerpo y la salud; delitos contra el honor; delitos contra la libertad; delitos contra el patrimonio; delitos contra los derechos intelectuales; delitos contra la administración pública y delitos contra la fe pública. El Manual de Evidencia Digital argentino (2023) señala que la evidencia digital es toda información obtenida de medios tecnológicos, electrónicos o informáticos, como computadoras, teléfonos móviles, dispositivos de video digital o soportes ópticos, tras ser sometida a una intervención humana, electrónica o informática. Desde un punto de vista técnico, corresponde a un tipo de evidencia física compuesta por pulsos electrónicos y campos magnéticos, los cuales pueden ser recolectados y analizados mediante herramientas y métodos especializados. Su utilidad radica en que puede ser presentación como prueba dentro de un proceso judicial.

El manejo de la evidencia digital en los delitos de pornografía infantil enfrenta desafíos vinculados a la correcta preservación y autenticidad de los indicios existentes en la escena del crimen, muchas veces hallados durante el operativo de revelación del delito, habida cuenta del artículo 68° - A, del Código Procesal Penal (2004). Los protocolos establecidos, como el cumplimiento de la cadena de custodia, sumado al uso de softwares especializados, garantizan la integridad de los datos recopilados. Según el manual de análisis de evidencia digital de la PNP, se entiende la importancia de realizar procedimientos rigurosos para prevenir alteraciones, modificaciones o sustracciones durante la recolección y el traslado de dispositivos electrónicos.

El Código Penal (1991) tipifica el delito de pornografía infantil como:

Artículo 129-M.- Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa, publicita, publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad (...).

Cuyos agravantes son:

La víctima tenga menos de catorce años de edad.

El material se difunda a través de cualquier tecnología de la información o de la comunicación o cualquier otro medio que genere difusión masiva.

El agente actúe como miembro o integrante de una banda u organización criminal.

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

La recopilación de información digital incluye dispositivos como teléfonos móviles, memorias USB, servidores remotos, entre otros dispositivos con la capacidad de almacenar información. El manejo de estos elementos demanda la utilización de técnicas avanzadas, como la clonación bit a bit con el uso de duplicadores forenses, cuyo propósito es crear copias exactas sin alterar la información original. Con el fin de mantener la trazabilidad de la evidencia, siendo este aspecto establecido por estándares internacionales como las normativas ISO 27037 e ISO 27042 sobre identificación y análisis forense digital conforme a lo absorbido a través de la investigación, los peritajes que se realiza el personal especializado lo hace en las copias espejo (duplicados del original), puesto que la evidencia original debe mantenerse intacta hasta la presentación en el juicio oral.

El uso creciente de herramientas de cifrado por parte de los delincuentes (pedófilos o consumidores de pornografía), complica el acceso a la información. En respuesta, los peritos emplean técnicas de extracción lógica y física para descifrar datos cifrados. También se encontró discrepancias en la aplicación de normativas relacionadas con delitos cibernéticos; si bien la normativa nacional aborda aspectos generales, los casos de pornografía infantil exigen medidas específicas que garantizan la admisibilidad de la evidencia en juicio; teniendo en cuenta que tenemos una norma procesal en extremo garantista, y que es señalada como un obstáculo recurrente durante el proceso investigativo; ello conlleva a que la labor del personal pesquisa sea más profesionalizada y perspicaz.

Se han identificado patrones delictivos que involucran el uso de redes sociales y plataformas de mensajería para la distribución de material ilícito. Estas actividades han sido rastreadas mediante técnicas de monitoreo en línea, lo que ha permitido a los investigadores recopilar pruebas sin vulnerar derechos fundamentales, en concordancia con las modificaciones introducidas por el Decreto Legislativo N° 1611 (2023) en la normativa procesal. En este contexto, los agentes virtuales desempeñan un rol esencial en las operaciones de vigilancia e infiltración en foros digitales, donde identifican redes de distribución de contenido ilegal, analizan los métodos empleados, perfilan a los involucrados, detectan patrones de consumo y ubican a los responsables. Asimismo, su labor permite obtener información en tiempo real sobre posibles atentados contra las víctimas, contribuyendo a la prevención y persecución de estos delitos.

La investigación de delitos vinculados a la pornografía infantil enfrenta desafíos tecnológicos significativos, entre ellos el uso de herramientas de encriptación y técnicas de anonimato por parte de los infractores, quienes operan en redes como la Dark Web. Estas barreras han requerido la aplicación de análisis forenses avanzados y la cooperación internacional para superar las restricciones jurisdiccionales en la persecución de estos delitos (Igarza et al., 2024). Las metodologías empleadas en el peritaje digital integran criterios científicos y precisión técnica. El uso de herramientas forenses especializadas permite recuperar

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

datos eliminados, reconstruir patrones digitales y analizar redes de explotación infantil a partir de evidencia rastreable y verificable (Krebbekx, 2024).

Paredes (2024) menciona que la pornografía infantil incluye la representación de menores en actos explícitos sexuales con fines de lucro o explotación, desde la tenencia hasta la distribución del material. Este fenómeno viola derechos fundamentales de los menores y permite la exposición de imágenes en redes globales. Ello conlleva a pensar en actualizar el marco normativo frente a las nuevas modalidades delictivas, donde se adapte la legislación a los avances tecnológicos que abren las puertas a nuevas modalidades delictivas.

La transmisión de pornografía infantil se facilita por el acceso a tecnologías que complican la trazabilidad de los responsables. La Convención sobre los Derechos del Niño (1989) y normativas nacionales insertaron medidas legislativas estrictas para prevenir y sancionar estos delitos, enfrentando barreras técnicas y jurisdiccionales, sin embargo y pese a la labor ardua de la Policía, los ciberdelincuentes continúan propalando imágenes pornográficas donde participan menores. Por ello, el manejo de evidencia digital exige protocolos rigurosos que aseguren su integridad y autenticidad. Dispositivos como servidores y teléfonos móviles almacenan información, y deben aplicarse estándares internacionales como las normas ISO 27042 e ISO 27037 para preservar la admisibilidad de las pruebas, al ser recogida la información que contienen. Los delitos informáticos adoptan diversas formas que comprometen la seguridad de la información, se logra descubrir intrusiones en sistemas protegidos hasta alteraciones de datos complejos y con cifrado extremo. La aplicación de protocolos como la ISO 27042 garantiza el análisis y la presentación de evidencia admisible en los tribunales.

El Grooming, representa un proceso pérfido mediante el cual un adulto utiliza estrategias de manipulación emocional y psicológica para acercarse a menores de edad a través de plataformas digitales, con el propósito ulterior de obtener imágenes o videos de carácter sexual. o generar encuentros presenciales a través del chantaje. Este fenómeno, profundamente vinculado a la vulnerabilidad de los menores en entornos virtuales, constituye una forma agravada de explotación, dado que la confianza construida mediante falsedades y engaños se convierte en la herramienta de control utilizada por el agresor para conducir a actos de connotación sexual. (Eltobgy et al., 2024).

El sexting se transformó en una fuente inadvertida de pornografía infantil, pues el contenido generado y prohibido, una vez apropiado por terceros, se distribuye en redes clandestinas (Dark Web o Deep Web), por ello se requiere de un adecuado manejo de la evidencia digital y se requiere técnicas avanzadas de preservación; el sexting consiste en el intercambio de mensajes o imágenes íntimas y específicas mediante dispositivos electrónicos, frecuentemente en contextos juveniles, generando riesgos de exposición indebida y efectos psicosociales complejos (Colqui y Vergaray, 2023). La legislación internacional y nacional establece medidas para combatir la pornografía infantil, criminalizando su producción y

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

distribución. En Perú, el Código Penal sanciona estos actos bajo figuras específicas, actualizando continuamente sus disposiciones frente a las tecnologías emergentes.

El modus operandi de los agresores digitales combina anonimato y manipulación emocional para explotar a menores. Estas funestas personas operan en redes encriptadas y utilizan herramientas avanzadas para ocultar sus rastros, dificultando la acción de las autoridades. La evidencia digital en casos de pornografía infantil, al ser efímera y volátil, exige técnicas avanzadas de preservación y análisis.

Los peritos utilizan el software EnCase y FTK que son herramientas de alta especialización en el ámbito del análisis forense digital, orientadas a la investigación de dispositivos electrónicos mediante la extracción y procesamiento de datos electrónicos, magnéticos u ópticos. EnCase, desarrollado por OpenText, permite la recopilación de información digital en un entorno controlado, conservando la integridad de las evidencias mediante la creación de imágenes forenses. Esta herramienta es reconocida por su capacidad de identificar archivos ocultos, recuperarlos y analizar metadatos, configuraciones de sistemas operativos y registros de actividad, lo cual resulta fundamental en investigaciones de naturaleza penal. Además, EnCase dispone de funcionalidades avanzadas para realizar búsquedas detalladas con palabras clave, lo que facilita identificar elementos probatorios específicos dentro de un gran volumen de datos.

Por otro lado, FTK, producto de AccessData, ofrece una solución integral para el análisis de evidencia digital, enfocándose en la eficiencia en el manejo de grandes volúmenes de información. Esta herramienta incluye un motor de indexación previo al análisis, lo que permite acceder a los datos de manera ágil y realizar búsquedas precisas. Su capacidad para analizar correos electrónicos, registros de sistema y bases de datos la hace particularmente adecuada en investigaciones relacionadas con delitos económicos o cibernéticos. FTK permite la recuperación de información eliminada y el acceso a datos cifrados, proporcionando una ventaja técnica considerable al investigador.

Ambas herramientas aseguran la confiabilidad del proceso investigativo, pues trabajan como duplicadores forenses de los dispositivos originales, lo que evita la alteración de las evidencias y un adecuado manejo de la información existente, con la garantía de que no será alterada. Estos programas garantizan la trazabilidad de la información, ayudan a la producción de informes técnicos que cumplen con los estándares requeridos para su presentación en procesos judiciales. Son una solución eficaz para el análisis minucioso de dispositivos digitales; pues, proporcionarán informes detallados que respaldan la presentación de pruebas en los tribunales, garantizando la confiabilidad de los resultados obtenidos, previa redacción de actas de los archivos hallados y la participación del representante del Ministerio Público, le da un soporte legal al trabajo de los peritos.

La era digital ha transformado profundamente el manejo de la evidencia en delitos de pornografía infantil, donde los procedimientos que requieren una rigurosa observancia de

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

principios técnicos y legales son necesarios para tal fin. Este tipo de crimen, marcado por la producción y distribución de material que explota a menores de edad, encuentra en las tecnologías actuales una herramienta de perpetuación y ocultamiento. Las legislaciones internacionales, como el Convenio de Budapest, junto con normativas nacionales, han establecido estándares estrictos para combatir este flagelo, enfatizando la importancia de garantizar la inalterabilidad y autenticidad de las evidencias digitales obtenidas en estos casos (Paredes, 2024).

La evidencia digital, caracterizada por su volatilidad y naturaleza efímera, exige técnicas meticulosas de recolección y preservación. Los dispositivos electrónicos y redes sociales se han convertido en elementos fundamentales para la obtención de pruebas, desde comunicaciones encriptadas hasta material audiovisual almacenado en servidores remotos. El manejo correcto de estos elementos, enmarcado bajo protocolos internacionales como los establecidos por las normas ISO 27037, asegura su admisibilidad en juicio y protege la integridad del proceso investigativo (Simio, 2023).

El proceso de preservación de la evidencia digital involucra herramientas avanzadas como duplicadores forenses, que permiten la creación de copias exactas de discos duros y otros dispositivos sin alterar su contenido original. A este procedimiento se suman técnicas como la recuperación de datos eliminados o encriptados mediante software especializado, cuyo objetivo es reconstruir el flujo de actividades digitales vinculadas al delito investigado. Estas prácticas fortalecen la trazabilidad de la evidencia y su validez jurídica en escenarios judiciales (Aiquipa, 2024).

La evidencia digital en la escena del crimen debe ser recolectada bajo estrictos procedimientos técnicos para garantizar su integridad y autenticidad. Esto implica aislar la escena y proteger los dispositivos tecnológicos identificados, evitando cualquier tipo de manipulación que pueda alterar los datos almacenados. La Policía Nacional del Perú, conforme a lo estipulado en el manual, debe identificar los dispositivos de almacenamiento (unidades de almacenamiento), para luego proceder con su procesamiento.

Antes de proceder al traslado de la evidencia, se debe documentar cada dispositivo mediante registros visuales y escritos, detallando sus características como marca, modelo, número de serie y estado físico. Estos detalles se consignan en actas formales que forman parte de la cadena de custodia. Es imperativo que los puertos de entrada y salida de los dispositivos sean protegidos con cintas de seguridad, y que el embalaje se realice de manera individual para evitar contaminación cruzada.

En casos donde los dispositivos se encuentren encendidos, no deben ser apagados sin antes documentar cualquier actividad visible en pantalla, como ventanas activadas de redes sociales o correos electrónicos. En situaciones donde los dispositivos estén apagados, se prohíbe encenderlos, ya que esto podría alterar la información importante almacenada en su memoria

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

RAM. La manipulación debe limitarse a lo estrictamente necesario para asegurar su preservación, siempre siguiendo los procedimientos establecidos.

Una vez recolectada, la evidencia digital debe ser lacrada y etiquetada en presencia de los intervinientes, quienes deberán firmar las actas correspondientes para asegurar la trazabilidad de los dispositivos. El traslado a las unidades especializadas para su análisis informático forense debe realizarse con el máximo cuidado, empleando vehículos seguros y en cumplimiento de las normativas vigentes. Cualquier irregularidad en este proceso podría comprometer la legitimidad de los hallazgos durante el análisis posterior.

El tratamiento de la evidencia digital no solo implica la aplicación de procedimientos técnicos, sino también el cumplimiento de las disposiciones legales que garantizan el respeto a los derechos fundamentales de los involucrados. La normativa peruana establece parámetros claros para la recopilación, traslado y análisis de esta evidencia.

Los dispositivos que podrían contener información digital son los siguientes: memorias Usb; memoria externa (Sd, Microsd); lector de banda magnética (Skimmer); tarjeta electrónica; sistema de videovigilancia (Dvr, Nvr, Ndvr); computadora personal (Pc); computadora portátil (laptop, notebook); servidor; disco duro interno; disco duro externo; equipo de comunicación (Router, Switch); impresora multifuncional; dispositivos multimedia; tarjeta sim (chip); módem usb (internet móvil); sistema de posicionamiento global (Gps); dispositivos tipo Palm; tabletas; vehículo aéreo no tripulado (Drone); reloj inteligente (Smartwatch); terminal de punto de venta (Pos); cámara espía; caja de liberación y desbloqueo; cámaras filmadoras; cámaras fotográficas; equipo terminal móvil (teléfono celular).

La información electrónica, magnética u óptica, requieren ser embalada utilizando guantes antiestáticos y en materiales con características particulares como: bolsas antiestáticas, sobres con protección de aire encapsulado, bolsas Faraday o papel Kraft, con la finalidad de evitar que sean controlados los equipos de manera remota y que se borre la información contenida en ellos.

El embalado, sellado y etiquetado, deberá contener fecha, hora, lugar, nombre y firma. Se debe documentar cualquier cambio o alteración en el embalaje o en su contenido; el embalaje es sellado con cinta de seguridad con la leyenda “evidencia”, la cual lleva nombre, fecha y firma del personal que embaló. El rotulo que se añade al embalaje para identificarlo. Para una mayor constancia, se elabora un acta de inventario de bienes, después de que sean examinados, fotografiados o video grabados, perennizados; este inventario se incluye en el acta de intervención. El manejo de la evidencia digital debe ser elaborado de forma profesional y por peritos, cuyo resultado final se exprese conforme a la siguiente imagen, la cual es la forma adecuada de preservar la evidencia.

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

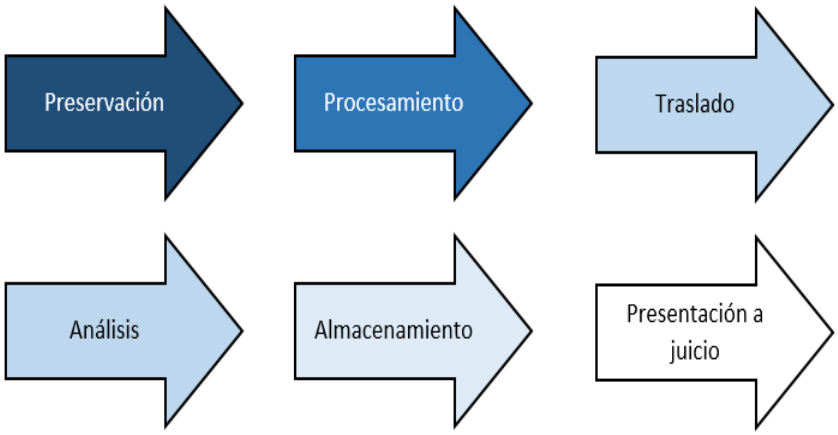
La cadena de custodia es un pilar fundamental en el manejo de la evidencia digital, pues a través de este proceso se asegura que cada elemento probatorio se mantenga íntegro desde su recolección, su análisis, hasta su presentación en juicio. Este proceso implica un registro minucioso de cada intervención sobre los dispositivos, donde la utilización de herramientas como la inserción de códigos hash garantiza la inalterabilidad de los datos. El código hash es un identificador único derivado de un algoritmo matemático que transforma datos de cualquier tamaño en una secuencia alfanumérica fija. Esta representación es ampliamente utilizada en el ámbito forense digital debido a su capacidad para verificar la integridad de la información analizada. En términos técnicos, el hash opera como una "huella digital" de un archivo, ya que cualquier modificación, incluso mínima, en el contenido original genera un cambio completo en el código generado. El incumplimiento de estos estándares podría derivar en la exclusión de pruebas esenciales, debilitando las estrategias de acusación en juicios relacionados con delitos de pornografía infantil, ante la alteración del contenido de las muestras (Paredes, 2024).

La cadena de custodia de la evidencia digital, en su carácter técnico-legal, representa un conjunto de procedimientos rigurosamente diseñados para asegurar la integridad, mismidad, autenticidad y trazabilidad de los indicios recolectados en el marco de una investigación. Cada paso dentro de este proceso, desde la identificación inicial del material en la escena del crimen, hasta su presentación en el juicio, debe estar documentado de forma precisa, garantizando que la información contenida en los dispositivos electrónicos no haya sido alterada o comprometida en ningún momento. La mínima duda en este proceso podría anular la validez probatoria de la evidencia, tornando ineficaz su utilización en el proceso judicial.

Cada intervención en la cadena de custodia, desde el traslado físico de los dispositivos hasta su análisis en laboratorios forenses, requiere de un escrutinio constante, donde cada actor involucrado, ya sea personal policial, peritos forenses o autoridades judiciales, asuma la responsabilidad de la integridad. del material. Esto incluye la implementación de protocolos

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

estrictos de seguridad, tanto en el manejo físico como en el acceso digital a la información, previniendo cualquier tipo de intromisión no autorizada que pudiera poner en riesgo la pureza del proceso investigativo. Los pasos de la cadena de custodia son:



Cualquier fallo en la custodia podría permitir que los responsables evadan la justicia, amparados en la contaminación o pérdida de pruebas objetivas. La recolección, embalaje, sellado y etiquetado de los indicios digitales, se realizará de acuerdo con su tipo, con el propósito de garantizar su integridad, autenticidad, mismidad e identidad, Posteriormente, se embalarán en contenedores o recipientes nuevos, de forma individual, finalizando con el sellado, etiquetado y firma del responsable del procesamiento y demás participantes de la diligencia.

Una vez finalizado las etapas anteriores, los dispositivos electrónicos y/u ópticos se entregarán con su respectivo formato de cadena de custodia a la autoridad competente. Una vez llevadas a cabo estas actividades, el perito, en el laboratorio, debe llevar a cabo las siguientes acciones de verificación y control de la Cadena de Custodia:

Verificar que el embalaje de los indicios o elementos digitales probatorios se encuentre debidamente sellado, etiquetado y firmado, sin que exista roturas en los soportes, cajas o contenedores.

Cotejar la información del rotulo del embalaje, con la información del registro en el acta correspondiente, para constatar que los datos asentados correspondan entre sí.

Revisar que se cuente con la documentación de los indicios o elementos digitales probatorios (escritos y fotografías).

Llenar el registro de Cadena de Custodia por indicio, el cual, lo acompañará en todo momento, debiendo contener los siguientes datos:

Identificación.

Documento.

Recolección y traslado.

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

Servidores públicos que intervinieron en el recojo/procesamiento.

Tipo de traslado.

Continuidad y trazabilidad.

Cuando un indicio o elemento digital probatorio, se pierda, altere, destruya o contamine, el interviniente anotará dicha circunstancia en el apartado de observaciones del registro de cadena de custodia, e informará de manera inmediata, al Ministerio Público.

Se deberá adoptar las medidas de seguridad para mantener intangible e inalterable la cadena de custodia hasta su disposición o resolución final en el proceso de modificación. Los elementos materiales probatorios y la evidencia física son auténticos y permanecen intangibles, mientras hayan sido asegurados, fijados, recogidos y embalados técnicamente, y sometidos a la regla de cadena de custodia (MININTER, 2020).

Discusión

Los hallazgos reflejan la complejidad inherente al manejo de evidencia digital en este tipo de delitos, por ser un delito novedoso que utiliza las tecnologías de la comunicación e información para producir sus efectos, a su vez, los procedimientos técnicos y legales son fundamentales para garantizar la validez y admisibilidad de las pruebas.

A través del análisis de los documentos, procesamiento de evidencia, la cadena de custodia y el uso de herramientas forenses especializadas, como “EnCase” y “FTK”, se ha demostrado que es necesario preservar la autenticidad de la evidencia digital. A su vez, estos resultados son consistentes con los planteamientos de Colmenares et al. (2024), quienes exaltan la importancia de herramientas tecnológicas en el tratamiento de la evidencia digital, especialmente en casos donde se enfrentan barreras técnicas como el cifrado de datos. Además, los patrones de conducta delictiva identificados en redes sociales y plataformas encriptadas confirman los desafíos que plantea la expansión de la Dark Web (Paredes, 2024).

Una categoría emergente significativa en este estudio es la utilización del Grooming como estrategia tomada por los agresores para explotar emocionalmente a las víctimas y obtener material ilícito. Este hallazgo amplía el marco teórico existente, pues conecta las prácticas delictivas con la vulnerabilidad psicosocial de los menores, lo cual había sido previamente abordado por Eltobgy et al. (2024) en el contexto de la manipulación emocional. Asimismo, la inclusión de protocolos específicos para el manejo de dispositivos de almacenamiento en la escena del crimen, documentada en el Manual de Evidencia Digital (2020), refuerza la necesidad de estándares internacionales como las normas ISO 27037 e ISO 27042 para garantizar la integridad de los datos recolectados, vinculados a la pornografía infantil.

En cuanto a la validez de los resultados, el estudio demuestra consistencia interna y coherencia metodológica, sustentándose en un diseño de teoría fundamentada que permite generar explicaciones contextuales aplicables al sistema judicial peruano. La triangulación de datos entre análisis documental y peritajes fortalece la confiabilidad de las conclusiones,

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

mostrando cómo las técnicas de preservación digital inciden en la resolución efectiva de casos de pornografía infantil.

A través de la triangulación se pudo articular diversas fuentes y enfoques metodológicos para obtener una comprensión más integral del fenómeno investigado. Los datos recopilados a partir de documentos y normativas vigentes se complementan al revelar las dificultades técnicas y legales para preservar la integridad de las pruebas, por ser un área nueva para la PNP. Por ejemplo, se evidencian que el uso de herramientas forenses como “EnCase” y “FTK” son indispensables para el análisis de dispositivos electrónicos, mientras que los documentos revisados destacan cómo las normas ISO 27037 e ISO 27042 aportan directrices necesarias para garantizar la autenticidad de la información almacenada. en estos dispositivos. Este entrelazamiento de fuentes confirma la dependencia del proceso judicial en estándares técnicos rigurosos.

El análisis documental reafirma la existencia de un protocolo establecido para el manejo de evidencia digital, como la cadena de custodia y la clonación bit a bit, siendo esenciales para evitar alteraciones en la información recolectada. Esta convergencia se refleja en normativas nacionales como el artículo 68°-A del Código Procesal Penal y las observaciones recogidas en el Manual de Evidencia Digital de 2020, donde se especifica que cualquier omisión en estos procedimientos podría anular la admisibilidad de la prueba en juicio. Asimismo, los peritajes analizados evidencian cómo estas herramientas permiten reconstruir actividades delictivas realizadas en entornos digitales y pueden ser insertadas al proceso penal.

La integración de fuentes primarias y secundarias también resalta cómo las dinámicas delictivas evolucionan con el avance tecnológico, siendo el Grooming y el sexting dos categorías emergentes identificadas tanto en las entrevistas como en los documentos revisados. El primero se establece como una estrategia de manipulación psicológica que facilita la explotación de menores, mientras que el segundo se posiciona como una práctica que alimenta las redes de distribución de material ilícito. Estas interacciones son detectadas y documentadas mediante técnicas de monitoreo en línea y herramientas avanzadas de análisis forense, cuyas metodologías han sido validadas por estudios previos y normativas internacionales. La triangulación confirma así que la adecuada preservación y análisis de evidencia digital no solo depende de herramientas tecnológicas, sino también de un marco normativo y ético que asegure su utilización legítima en el ámbito judicial.

Conclusiones

El manejo de la evidencia digital en delitos de pornografía infantil exige la aplicación rigurosa de protocolos técnicos y el respeto por el marco jurídico, para garantizar la integridad y autenticidad de los datos. Sin estos procedimientos, la admisibilidad de las pruebas en juicio queda comprometida y puede generar la exclusión de los medios de prueba del proceso judicial.

Las técnicas de análisis forense, como la clonación bit a bit y la utilización de software especializado como EnCase y FTK, han demostrado ser esenciales para preservar la información

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

almacenada en dispositivos electrónicos, permitiendo la reconstrucción de actividades delictivas y fortaleciendo el proceso probatorio en casos de pornografía infantil, puesto que la labor pericial se realiza en las copias espejo que han sido generadas de los datos originales y con ello se garantiza que los medios de prueba originales lleguen intactos a la etapa probatoria del juicio.

Las dinámicas delictivas como el Grooming y el sexting surgen como prácticas asociadas a la explotación infantil en entornos digitales, a través de estos medios los agresores/vendedores/consumidores adquieren parte del material, para luego ser distribuido a través de plataformas y entornos virtuales, llámese Deep Web o Dark Web, es por ello que existe la necesidad de capacitar a los operadores de justicia para abordar estas modalidades de manera efectiva y prevenir su continuidad en las redes clandestinas.

La normativa internacional, como las normas ISO 27037 e ISO 27042, establecen estándares esenciales para el manejo de evidencia digital, los cuales deben ser integrados en el marco legal peruano para armonizar las prácticas locales con los criterios globales de preservación y análisis forense; en la Policía existe el manual de recojo de evidencia digital que facilita la labor pericial del personal forense.

Este estudio confirma que la adecuada gestión de la evidencia digital es un pilar fundamental para garantizar la eficacia del sistema judicial en la lucha contra la pornografía infantil. Solo mediante un enfoque integral, que combina tecnología, normativas sólidas y formación especializada, se podrán enfrentar los desafíos técnicos y jurídicos que plantea este delito.

Referencias

Aiquipa, F. (2024). Buenas prácticas desde el enfoque criminalístico en el manejo de indicios y cadena de custodia, Huancayo 2021 [Tesis de maestría, Universidad Continental]. https://hdl.handle.net/20.500.12394/15796

Barraza, A. (2023). Metodología de la investigación cualitativa: Una perspectiva interpretativa. Benessère. Centro de Intervención para el Bienestar Físico y Mental AC ISBN: 978-607-99980-4-2. https://biblioteca.enc.edu.pe/bib/4731

Código Penal Peruano [COD]. Artículo 129-M (1991) https://lpderecho.pe/codigo-penal-peruano-actualizado/

Colmenares, L. Barrera, R., y Cerón, C. (2024). Análisis del sexting como factor de riesgo en la difusión de pornografía infantil. CienciaAmérica, 13 (1). https://cienciamerica.edu.ec/index.php/uti/article/view/456/979

Colqui, N. y Vergaray, S. (2023). El control parental y el delito de pornografía infantil de niños, niñas y adolescentes, San Juan de Lurigancho, 2022 [Tesis de pregrado, Universidad Peruana Los Andes]. https://hdl.handle.net/20.500.12848/7258

Constitución Política del Perú [Const.]. Art. 118, inciso 2. (29 de diciembre de 1993).

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

http://www.pcm.gob.pe/wp-content/uploads/2013/09/Constitucion-Pol%C3%ADtica-del-Peru-1993.pdf

De la Cruz, L. y Pérez, L. (2023). La pornografía infantil por redes y su aplicación en el nuevo Código Penal, 2022 [Tesis de pregrado, Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/134578

De la Espriella, R., y Gómez, C. (2020). Teoría fundamentada. Revista Colombiana de Psiquiatría, 49 (2), 127–133. https://doi.org/10.1016/j.rcp.2018.08.002

Eltobgy, A., Aljabali, A., Farag, A., Elshorbgy, M., Hamed, M., Hamouda, E., Hamouda, H., Refaey, N., Kabeel, M., Amro, S., Abouheseba, T., y Tarek, M. (2024). Effects of pubic hair grooming on women's sexual health: a systematic review and meta-analysis. BMC Women's Health. https://bmcwomenshealth.biomedcentral.com/articles/10.1186/s12905-024-02951-1

Hernández, S. y Duana, D. (2020). Técnicas e instrumentos de recolección de datos. Boletín Científico de las Ciencias Económicas Administrativas del ICEA, 9 (17), 51–53. https://repositorio.uaeh.edu.mx/revistas/index.php/icea/issue/archive

Igarza, A. Gioia, C. Eterovic, J. Ureta, W. Krajnik, M. González, J. Conde S. (2024) Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital. Secretaría de Ciencia y Tecnología de la UNLaM. http://repositoriocyt.unlam.edu.ar/handle/123456789/1938

Krebbekx, W. (2024). ¿Una historia de una chica que envía desnudos a un chico? Sexting sin guiones en una escuela holandesa . Journal of Gender Studies , 33 (4), 375-385. https://doi.org/10.1080/09589236.2023.2242288

MININTER. (2020). *Manual para el recojo de la evidencia digital*. Ministerio del Interior. https://www.gob.pe/institucion/mininter/informes-publicaciones/1199631-manual-para-el-recojo-de-la-evidencia-digital

Ministerio Público Fiscal de la República Argentina. (2019). Manual de Evidencia Digital: Fundamentos aplicables para el abordaje de la examinación forense. https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf

Palmeiro, I. (2022). A pornografia infantil à luz da proteção integral: Riscos no ciberespaço durante una pandemia de COVID-19 [Monografía de grado, Universidade Federal de Santa Maria]. http://repositorio.ufsm.br/handle/1/31542

Paredes, G. (2024). Análisis del delito de pornografía infantil [Trabajo fin de grado, Universidad Rey Juan Carlos]. Móstoles, España. https://hdl.handle.net/10115/31044

ESCPOGRAPNP
Revista Académica de la Escuela de Posgrado
de la Policía Nacional del Perú
Vol. 4 N° 2, pp. 205-220, enero-junio, 2025
ISSN: 2961-2527

Paredes, G. (2024). Análisis del delito de pornografía infantil. Trabajo de fin de grado en Derecho. Universidad Rey Juan Carlos. https://hdl.handle.net/10115/31044

Portugal, J. (2024). Delitos informáticos y la evidencia digital en el proceso penal peruano 2023 [Tesis de pregrado, Universidad Privada San Carlos]. http://repositorio.upsc.edu.pe/handle/UPSC/775

Resolución 44/25, Texto de la Convención sobre los Derechos del Niño (20 de noviembre de 1989). https://www.unicef.org/es/convencion-derechos-nino/texto-convencion

Simio, M. (2023). Investigación del crimen organizada mediante acceso remoto: La problemática en la obtención de evidencia digital a distancia desde la perspectiva de las garantías constitucionales en la investigación penal. Buenos Aires. https://biblioteca.csjn.gov.ar/cgi-bin/koha/opac-retrieve-file.pl?id=8506d5f861551afd57eb9965c6bcec73