

Manejo del indicio digital telefónico en la escena del crimen

Handling the digital telephone evidence at the crime scene

- ¹ Marco Antonio Salazar Yépez  <https://orcid.org/0000-0002-5025-0804>
Licenciado Administración Policial, Maestrante en la Universidad Nacional de Chimborazo (UNACH)
antonio.salazar@unach.edu.ec
- ² Verónica Paulina Cáceres Manzano  <https://orcid.org/0000-0001-5710-5661>
Magister en Criminología, Docente Universidad Nacional de Chimborazo (UNACH)
vcaceres@unach.edu.ec



Artículo de Investigación Científica y Tecnológica

Enviado: 10/01/2023

Revisado: 25/02/2023

Aceptado: 27/03/2023

Publicado: 15/05/2023

DOI: <https://doi.org/10.33262/visionariodigital.v7i2.2561>

Cítese:

Salazar Yépez, M. A., & Cáceres Manzano, V. P. (2023). Manejo del indicio digital telefónico en la escena del crimen . Visionario Digital, 7(2), 70-83.
<https://doi.org/10.33262/visionariodigital.v7i2.2561>



VISIONARIO DIGITAL, es una revista científica, **trimestral**, que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. <https://visionariodigital.org>
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec



Esta revista está protegida bajo una licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 International. Copia de la licencia: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

Palabras**claves:**

Evidencia digital, dispositivos móviles, criminalística y forense.

Keywords:

Digital evidence, mobile devices, criminalistics, and forensics.

Resumen

Introducción: La investigación actual se centra en la gestión de pruebas telefónicas digitales en la escena del crimen siendo este, el valor probatorio de la información almacenada o establecida en forma digital que puede ser utilizada en juicio, con el propósito de analizar su control determinando el correcto manejo de la evidencia digital por búsqueda bibliográfica. **Objetivo:** Realizar una búsqueda bibliográfica sobre el manejo adecuado del indicio digital telefónico en la escena del crimen. **Metodología:** La investigación es de tipo documental y bibliográfica, descriptiva, que tiene una secuencia transversal retrospectiva, utilizando información recopilada y actualizada de las distintas bases de datos científicas de donde se obtendrá información referente al tema de investigación y como muestra 6 documentos encontrados en revistas científicas, libros y artículos de revisión. **Resultados:** Se detallarán aspectos importantes a seguir en el tratamiento de indicios digitales como evidencia según varios autores. **Conclusión:** Se determinó que el almacenamiento digital de la información a través de los dispositivos inteligentes móviles es de gran utilidad para descifrar el motivo del delito actualmente. Por ende, la búsqueda bibliográfica de tendencias innovadoras en cuanto a descifrar las evidencias en dispositivos móviles son relevantes a la hora de recopilar información sobre los hechos en criminalística y forenses. **Área de la ciencia:** Criminalística/Forense. **Área de estudio específica:** Derecho-Criminalística.

Abstract

Introduction: The current research focuses on the management of digital telephone evidence at the scene of the crime being this, the probative value of the information stored or established in digital form that can be used in trial, with the purpose of analyzing its control determining the correct handling of digital evidence by bibliographic search. **Objective:** To conduct a bibliographic search on the proper handling of the telephone digital evidence at the crime scene. **Methodology:** The research is documentary and bibliographic, descriptive, which has a retrospective cross-sectional sequence, using information collected and updated from the different scientific databases from where information regarding the research topic will be obtained and as a sample six documents found

in scientific journals, books, and review articles. **Results:** Important aspects to follow in the treatment of digital indications as evidence according to several authors will be detailed. **Conclusion:** It was determined that the digital storage of information through mobile smart devices is especially useful to decipher the motive of the crime today. Therefore, the bibliographic search for innovative trends in terms of deciphering evidence on mobile devices are relevant when collecting information about the facts in criminalistics and forensics. **Science Area:** Laboratory – Criminalistics/Forensics.

Introducción

Actualmente, usar la tecnología para recolectar evidencia ya no es una opción, es una necesidad debido al aumento de participación en el delito, ya que con el desarrollo de las tecnologías informáticas y la globalización mundial, ha permitido que el ser humano utilice sistemas altamente sofisticados para la comunicación como son los medios digitales inalámbricos.

Principalmente los teléfonos celulares se han convertido en parte de nuestra vida cotidiana que no son solamente utilizados para tareas ordinarias como recibir y enviar mensajes o llamadas, sino que algunos de ellos proveen las mismas funcionalidades que brinda una computadora de escritorio. Esto hace que los celulares se conviertan potencialmente en una valiosa fuente de evidencia en un análisis forense.

Según un estudio reciente existe, miles de dispositivos digitales que han sido incautados por la policía como evidencia de presuntos delitos, se encuentran almacenados en una acumulación cada vez mayor que los investigadores luchan por abordar (Grupo Forenses Digital, 2023).

Ante la falta de recursos eficientes para analizar la evidencia, la agencia de noticias de Palestina plantea que 12.122 dispositivos incluidos teléfonos, tabletas y computadoras son examinadas, esto puede o no obstaculizar a los fiscales en los casos penales. En otro caso, una investigación del New York Times del año 2021 que se encuentra en el mismo portal digital indica que se encuentra pendientes de examen 12.667 dispositivos de 33 fuerzas policiales.

Las investigaciones pendientes durante mucho tiempo muestran cuán abrumado esta un equipo forense digital debido al gran volumen de evidencia recopilada. En Ecuador la

tecnología *Global System for Mobile Communications* (GSM), está siendo utilizada mayoritariamente por las empresas celulares que operan en el país, abarcando con su cobertura a un importante número de usuarios a nivel nacional (Maleza & Sandoval, 2018).

Según la revista *Líderes*, Ecuador es uno de los países que más usuarios tiene en telefonía móvil a escala mundial. En concreto, posee 12 millones 946 mil usuarios de los 14'306.876 de ecuatorianos. De ellos, 212.842 usuarios tienen contratado el servicio de e-mail para sus teléfonos celulares. La tecnología GSM es el estándar de telefonía celular más utilizado alrededor del mundo; según la firma de industrias móviles *Wireless Intelligence*, en un reporte de Julio del año 2010, se anunció que el número de conexiones móviles globales ha sobrepasado los 5.000 millones en el mercado mundial, después de que a finales del 2008 se registraron 4.000 millones de conexiones (Maleza & Sandoval, 2018).

Debido a que la evidencia digital es volátil y frágil y el manejo inadecuado de esta evidencia puede alterarla, por ello se deben seguir protocolos para garantizar que los datos no se modifiquen durante su manejo, es decir, durante su acceso, recopilación, empaquetado, transferencia y almacenamiento. Según la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2019), “estos protocolos delinean los pasos a seguir cuando se maneja evidencia digital en cuatro fases involucradas en el manejo inicial de la evidencia digital: identificación, recopilación, adquisición y preservación” (p. 2).

Por ende, el presente trabajo se enfoca en realizar una búsqueda bibliográfica sobre el manejo adecuado del indicio digital telefónico en la escena del crimen puesto que, es importante destacar que las investigaciones relacionadas y las perspectivas teóricas, seguidas de una descripción de los métodos aplicados ayudan a esclarecer los procesos correctos de manipulación y procedimientos de traslado de indicios como a su vez, de las fuentes de evidencia digital y parámetros de incautación de indicios. Si bien, proporciona una mirada profunda a los dispositivos móviles y explica las tecnologías involucradas y su relación con los procedimientos forenses, para la validación, preservación, adquisición, examen, análisis y generación de informes de información digital.

Metodología

La presente investigación es de tipo documental y bibliográfica, descriptiva, que tiene una secuencia transversal retrospectiva, utilizando información recopilada y actualizada de las distintas bases de datos científicas como son *Pudmed*, *Elsevier*, *SciELO*, entre otros. Donde se buscó artículos científicos y revistas sobre el manejo del indicio digital telefónico en la escena del crimen. En donde se utilizó como población las diferentes bases de datos científicas de donde se obtendrá información referente al tema de investigación y como muestra 6 documentos encontrados en revistas científicas, libros y

artículos de revisión. También se tomó en cuenta criterios de inclusión que fueron artículos científicos y libros que correspondan a los 10 últimos años y de exclusión los que no corresponden a los 10 últimos años.

Fundamentación teórica

El análisis y presentación de las evidencias digitales son métodos muy eficaces para la obtención de información de un hecho de carácter delictivo, debido a que esta forma parte de uno de los procesos más importantes dentro de una investigación criminal, la cual pone en manifiesto la originalidad e integridad de las evidencias encontradas, con el fin recuperar los registros y mensajes de datos existentes dentro de un indicio digital ya que según Maleza & Sandoval (2018):

Se confirmará la existencia de la infracción y la culpabilidad de quienes se encuentran formando parte de un inicio como presuntos responsables, ya que toda esta información encontrada servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva dicho asunto de manera que toda la información recabada que puedan ser utilizada posteriormente como prueba ante un tribunal. (p. 21)

En sí, la evidencia digital, es la encontrada en las memorias del Equipo Móvil, ya que muchos fabricantes de teléfonos celulares usan la memoria interna del equipo, para implementar nuevas funciones y almacenar cierta información que no puede ser almacenada en la tarjeta SIM, debido a que tienen especificaciones que permiten el almacenamiento de cierto tipo de información (Maleza & Sandoval, 2018). En general para Acurio (2019) las fuentes de evidencia digital lo constituyen:

IMEI (*International Mobile Equipment Identity*), directorio telefónico, historial de llamadas, mensajes cortos, mensajes multimedia, buscadores, web y correos electrónicos, calendario, números marcados, números personales de Identificación (PIN), números de llamadas hechas con tarjeta, se puede encontrar valiosa información en la pantalla del aparato, imágenes, fotos, grabaciones de voz, información guardada en las tarjetas de expansión de memoria. (p. 12)

Discusión

A continuación en la tabla 1, se detallarán aspectos importantes a seguir en el tratamiento de indicios digitales como evidencia según varios autores.

Tabla 1

Análisis de procedimientos de traslado correcto de indicios, fuentes de evidencia digital y parámetros de incautación de indicios

Autor/es	Año	Título	Procedimiento correcto de traslado	Fuentes de evidencia	Parámetros de Incautación
Loarte et al.	2017	Marco de trabajo estandarizado para el análisis forense de la evidencia digital	La cadena de custodia se debe seguir bajo estándares RFC 3227, ISO 27370 y se debe contar con la presencia de la autoridad competente	Smartphone, tarjetas SIM, tarjetas microSD, computador, memoria RAM, <i>memory stick</i> , tarjetas xD	Según los establecidos en el COIP*
Bujosa et al.	2021	La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia.	Referirse a la prueba digital es abrirse a un universo de alternativas conceptuales desde el ámbito de la prueba, pues esta expresión está íntimamente ligada a los conceptos de prueba informática o electrónica y prueba tecnológica	Chats, fotografías, videos, correos electrónicos, etc.	Resulta cada vez más frecuente la incautación de equipos informáticos o de dispositivos de almacenamiento de datos o el registro y la vigilancia secreta a través de estos medios, y es realmente relevante el contenido de estos que llega al proceso penal a través del reconocimiento del investigado
Unidad de investigaciones cibernéticas y operaciones tecnológicas	2018	Guía técnica de cadena de custodia de evidencia digital	El servidor público que lleve a cabo el traslado tiene como encomienda, transportar los indicios probatorios digitales, debidamente embalados, sellados, etiquetados, firmados y con el registro de Cadena de Custodia Digital, del lugar de intervención, hacia el lugar determinado por parte del Ministerio Público	Flash, computadoras, celulares, fuentes de almacenamiento digital, correos	Todo indicio o material probatorio digital deberá ser descrito a través de la percepción de los sentidos del interviniente, dando a notar las características específicas de cada uno, además de poder apoyarse de fichas técnicas, etiquetas o textos

Tabla 1

Análisis de procedimientos de traslado correcto de indicios, fuentes de evidencia digital y parámetros de incautación de indicios (continuación)

Autor/es	Año	Título	Procedimiento correcto de traslado	Fuentes de evidencia	Parámetros de Incautación
Pinto	2021	Metodología de análisis forense orientada a incidentes en dispositivos móviles	Cuando un dispositivo móvil está involucrado en un delito o en un incidente se debe analizar y tomar en cuenta que el dispositivo contiene información personal, laboral, e incluso puede reflejar costumbres o hábitos de la persona, convirtiéndose así en información muy sensible para ser tomada para una investigación.	La agenda de contactos. Blogs de llamadas realizadas y recibidas SMS, MMS Datos que permitan conocer la ubicación física en la que se encontraba el móvil al momento de su obtención (si el mismo se encontraba apagado) a partir del registro de la celda de comunicación empleada	Es una herramienta de apoyo y ayuda en la obtención de pruebas para esclarecer diferentes tipos de ilícitos; si se lo hace de manera adecuada, y manteniendo el respectivo asesoramiento jurídico, para no tener problemas legales o ser considerado violación de la privacidad.
Bautista & Smith	2018	La informática forense en dispositivos Android	Un informe de Symantec sobre plataformas móviles y su seguridad, describe algunos problemas relacionados con el sistema operativo Android: Google no tiene un modelo de certificación riguroso de aplicaciones, lo que permitió el creciente volumen de software malicioso.	la potencial evidencia que se puede encontrar en un dispositivo móvil es: el historial de llamadas, la lista de contactos, mensajes de texto y correos electrónicos, multimedia (imágenes, videos, audio), historial de navegación, registro de chat, cuentas de redes sociales, notas y calendarios, las conexiones (red móvil, Wi-Fi, Bluetooth), la información con respecto a la localización	También la IOCE menciona una lista de cualidades que se debe tener en práctica en el peritaje

Tabla 1

Análisis de procedimientos de traslado correcto de indicios, fuentes de evidencia digital y parámetros de incautación de indicios (continuación)

Autor/es	Año	Título	Procedimiento correcto de traslado	Fuentes de evidencia	Parámetros de Incautación
Maleza & Sandoval	2018	Estudio y análisis de evidencia digital en teléfonos celulares con tecnología GSM para procesos judiciales	El análisis físico implica una copia bit a bit de una entrada física de almacenamiento (chip de memoria); mientras que el análisis lógico implica una copia bit a bit de los objetos lógicos (archivos) que residen sobre un almacenamiento lógico	La evidencia digital potencial, es la encontrada en las memorias del Equipo Móvil, ya que muchos fabricantes de teléfonos celulares usan la memoria interna del equipo móvil, para implementar nuevas funciones y almacenar cierta información que no puede ser almacenada en la tarjeta SIM	Determinar si la herramienta puede recuperar del usuario: IMSI, ICCID, SPN, ADN, LND y mensajes SMS relacionados en la tarjeta SIM, incluidas las entradas borradas

A partir de lo expuesto en la tabla 1, Maleza & Sandoval (2018), propone y redacta:

Un procedimiento de tecnología GSM que es un estándar mundial para teléfonos celulares, diseñado para utilizar señales digitales, así como también, canales de voz y canales de control digitales desde el punto de vista técnico y legal, que servirá como guía para realizar un adecuado manejo de la evidencia electrónica y digital en la investigación judicial bajo la cual esté involucrado el teléfono celular. (p.14)

Mientras que Loarte et al. (2017) redacta:

Un procedimiento interno llamado SOPs este otorga trazabilidad en la actividad pericial desarrollada, de forma tal que si los resultados de una pericia informática son cuestionados siempre es posible repetir la experticia. Los SOPs se establecen para demostrar que los pasos propios del trabajo metodológico siempre son más valiosos que el hardware o software que se utilice para una pericia informática. (p. 8)

Si bien, el manejo de evidencia digital es necesario tener presente 4 principios establecidos como: el personal no debe cambiar ningún tipo de dato, ser capaz de presentar la evidencia y explicar la relevancia de esta, crear un registro de toda la evidencia digital y por último asegurar el respeto a las normas y cumplir estos principios.

Maleza & Sandoval (2018), menciona que “elementos de prueba o evidencias dentro de un proceso judicial son de vital importancia, ya que mediante su investigación se puede llegar a determinar la confirmación o desvirtuación de una hipótesis o afirmación precedente de lo que corresponde a la verdad” (p. 10).

Por consiguiente, las técnicas de extracción de la información como: Evidencia Potencial en la Arquitectura GSM, Evidencia Digital Potencial en el Equipo Móvil, Evidencia Digital Potencial en la Tarjeta SIM, Técnicas de Análisis Físico y Lógico para la Extracción de Evidencia Digital de Teléfonos Celulares y Protección de la Información.

Según Maleza & Sandoval (2018):

La evidencia digital, es una herramienta de especial cuidado, para el proceso de investigación de delitos tecnológicos; debe ser tratada por parte de especialistas que conserven todas las medidas de precaución necesarias para no contaminarla y/o alterarla, para que ésta no sea objeto de desestimación ante un proceso legal. Por consiguiente, la evidencia digital no solo está limitada a lo que se encuentra en las computadoras, también se puede extender a los dispositivos electrónicos tales como MP3, memorias flash, iPod, teléfonos celulares, entre otros aparatos de telecomunicaciones y multimedia. (p. 2)

Como se mencionó anteriormente la evidencia digital es una herramienta la cual debe ser manejada con cautela para que de esta manera no sean alteradas y no sean un motivo de rechazo en un proceso legal y tienen un valor probativo (Arévalo, 2018):

La evidencia digital es cualquier información con valor probativo que es almacenada o transmitida en forma digital. La evidencia digital la podemos clasificar en dos tipos: La volátil: hace referencia a información temporal, como la que reside en la memoria principal (RAM) y la no volátil: hace referencia a memoria permanente tales como discos duros, usb's, cd's, etc.; esta información se mantiene cuando se apaga el equipo. (p. 17)

La evidencia digital es de suma importancia en el ámbito de las ciencias forenses ya que, abarca la información que se puede encontrar en los dispositivos tecnológicos de manera volátil o no volátil y tienen un valor probativo.

Pues bien, la aplicación informática forense para el análisis de dispositivos tecnológicos donde se almacena multitud de información que puede resultar determinante a la hora de

resolver un caso pues es primordial identificar el dispositivo a analizar y poder garantizar que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis. Para ello Villacreses et al. (2021), da a conocer la importancia del uso correcto de software que se utilizan para el análisis y extracción de la información existente en los dispositivos tecnológicos, mediante aplicaciones que se emplean en la informática forense y así mismo hacer el uso correcto de las mismas.

Bujosa et al. (2021), menciona que “la evidencia digital constituye un pilar fundamental en la investigación forense; razón por la cual, se analizan los principales marcos de mejores prácticas existentes y su aplicación a un proceso de investigación digital” (p. 6).

Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados

Por otra parte Gómez (2015), menciona “la informática forense es una disciplina técnico-legal. Es una especialidad con base en las ciencias informáticas que se nutre de otros conocimientos propios del derecho y la criminalística” (p. 19).

Independientemente del carácter fungible del perito, éste debe tener mínimamente un título universitario habilitante en la materia pertinente respecto de la cual ha de expedirse. La correcta aplicación de los pasos en la telefonía celular permite que se desarrolle la actividad pericial sobre dispositivos sin perder de vista el marco metodológico requerido para el manejo de evidencia digital, pudiendo hacer uso de las técnicas y herramientas de informática forense que estén disponibles (Gómez, 2015).

Los procedimientos operativos estandarizados contribuyen a mantener la calidad del servicio y llevan al siguiente nivel a las guías básicas de buenas prácticas. Esta propuesta es considerada como impulsora y sirve como modelo de referencia para el desarrollo de otros procedimientos operativos estandarizados que conformen los futuros manuales de operaciones de otras unidades periciales la Justicia nacional y provincial.

Previamente recolectada con éxito, es decir efectuar la recolección de evidencias bajo parámetros legales así como en la forma de proceder para su recolección, lo que garantiza la integridad de las evidencias; teniendo como principal inconveniente la inexistencia de un estándar mundial que rija este tipo de tareas. Que sirve como un complemento en la búsqueda de la verdad. Por esta razón nos menciona Salas (2018):

Es importante entender que la diferencia entre investigación y examinación denota dos áreas que trabajan coordinadamente, la primera para establecer la metodología y el diseño del plan de investigación científica; y el segundo el análisis de indicios de evidencia; convergiendo en descubrir la verdad como mutua objetivo. (p. 2)

La objetividad en los delitos cibernéticos va de la mano con la metodología a utilizar siendo esta la pieza clave y el punto de partida para conocer la verdad mediante los medios digitales que son utilizados diariamente.

Por otra parte el mismo Salas (2018) menciona:

La evidencia electrónica es frágil, se puede alterar o destruir, por el mal manejo o la mala práctica en la identificación, recolección y extracción; por esta razón, para desarrollar un correcto procedimiento de identificación, etiquetación, validación y preservación de la evidencia es lo primordial. (p. 5)

Empleando herramientas como:

- Computadora Portátil o Tablet con la respectiva plataforma forense
- Software Forense de validación y seguridad de evidencia
- Guantes
- Cámara Fotográfica Digital con GPS
- Registro inventario de evidencia
- Etiquetas para evidencia
- Fundas antiestáticas para hardware
- Fundas de Papel con burbujas para evidencia
- Tape para cercar o clausurar la ubicación de la escena del crimen
- Tape para sellar evidencia y otros que eviten la destrucción o contaminación de los indicios/evidencias

Que son complementadas con plataformas basadas en la nube, las cuales permiten una sincronización entre la recolección In Situ y el laboratorio de análisis forense, permitiendo transferencias seguras de información para cumplir así con el requisito de integridad y validación.

De acuerdo con Bautista & Smith (2018), “las escenas criminales no solo se limitan a pruebas balísticas, muestras de sangre, sino que también, los elementos electrónicos podrían brindar pistas, ayudar a formalizar una hipótesis y llevar a resolver un caso judicial” (p. 23). De acuerdo con esto, se puede mencionar que los teléfonos inteligentes (Smartphones) a más de ser una herramienta tecnológica de comunicación permite la recopilación de información dentro de un hecho delictivo como lo cita Maleza & Sandoval (2018):

Los dispositivos móviles celulares no son solamente utilizados para tareas ordinarias como recibir y enviar mensajes o llamadas, sino que algunos de ellos proveen las mismas funcionalidades que brinda una computadora de escritorio. Esto hace que los celulares se conviertan potencialmente en una valiosa fuente de evidencia en un análisis forense. (p. 1)

Esto indica que el alcance tecnológico facilita la interconexión entre personas lo que hace más fácil y rápido la comunicación entre personas. También es un instrumento potencial para cometer delitos que a su vez, se convierte en un indicio sujeto a análisis dentro de la investigación de hechos dentro de un caso criminalístico.

Conclusión

- El manejo de la evidencia digital en los últimos tiempos se ha convertido en una fuente de búsqueda de información relevante, que sirve para determinar o mostrar algunos de los indicios y evidencias que suceden en la escena del crimen estos nos brindan información actual de lo que ha transcurrido en un período determinado antes de que suceda el crimen o a su vez nos manifiesta todo lo que ha transcurrido hasta el fallecimiento de la víctima, es por ello que se deben realizar investigaciones telefónicas donde vamos a recopilar información relevante, podemos decir que las bases científicas como *PubMed*, *Scopus* y *SciELO* contribuyen en este tema de investigación aportándonos datos reales, biografías que nos ayudarán a esclarecer pistas en una escena del crimen aplicando una cadena de custodia que nos permita obtener información real.

Referencias Bibliográficas

- Acurio, S. (2019) *Manual de manejo de evidencias digitales y entornos informáticos versión 2.0*. https://www.oas.org/juridico/english/cyb_pan_manual.pdf
- Arévalo, P. O. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista de Economía y Política*, 3(7). 1-14.
- Bautista Dewar, R. & Smith Johan, R. (2018). La informática en dispositivos Android. *Revista Ingenio UFPSO*, 09(1).21-31.
- Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (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).482-490.
- Grupo Forenses Digital. (2023). *Análisis forense digital*. Ec-Council. <https://www.eccouncil.org/what-is-digital-forensics/>
- Gómez Leopoldo, Sebastián M. (2015). Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados. Simposio Argentino de Informática y Derecho (SID 2015) - JAIIO 44 (Rosario, 2015). Sociedad Argentina de Informática e Investigación Operativa (SADIO). ISSN: 2451-7526. pp. 16-25. sedici.unlp.edu.ar/handle/10915/55345

- Loarte Cajamarca, B. G., & Grijalva Lima, J. S. (2017). Marco de trabajo estandarizado para el análisis forense de la evidencia digital. *Revista Publicando*, 4 (11), 42-78. ISSN 1390-9304
- Maleza Peñaherrera, J. A., & Sandoval, Duque. (2018). *Estudio y análisis de evidencia digital en teléfonos celulares con tecnología GSM para procesos judiciales*. <https://bibdigital.epn.edu.ec/bitstream/15000/4903/1/Estudio%20y%20an%C3%A1lisis%20de%20evidencia.pdf>
- Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2019). *Manejo de evidencia digital*. <https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html>
- Pinto, D. (2021). Metodología de análisis forense orientada a incidentes en dispositivos móviles. *Revista Maskana*. 02 (3).1-11
- Salas, P. (2018). Guía técnica de cadena de custodia de evidencia digital. *Revista de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de México*.7 (1). 1-24.
- Unidad de investigaciones cibernéticas y operaciones tecnológicas. (2018, junio). Guía técnica de cadena de custodia de evidencia digital. Studylib. <https://studylib.es/doc/9049294/gui%C3%A1-t%C3%A9cnica-de-cadena-de-custodia-de-evidencia-digital>
- Villacreses, C., Chóez, J., Figueroa, V., & Barreto, J. (2021). Aplicación informática forense para el análisis de dispositivos tecnológicos. *Revista Científica Multidisciplinaria*, 5(4). 9-15.

Conflicto de intereses

Los autores declararan libremente que no existen conflictos de interés en la realización del trabajo.

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Visionario Digital**.



El artículo queda en propiedad de la revista y, por tanto, su publicación parcial y/o total en otro medio tiene que ser autorizado por el director de la **Revista Visionario Digital**.



Indexaciones

