REVISTA DE CIENCIAS JURÍDICAS Y POLÍTICAS
UNELLEZ JURIS

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

INFORMÁTICA FORENSE EN VENEZUELA: GARANTÍAS TECNOLÓGICAS PARA LA INVESTIGACIÓN DE DELITOS EN REDES SOCIALES DESDE UNA MIRADA TÉCNICO-JURÍDICA

COMPUTER FORENSICS IN VENEZUELA: TECHNOLOGICAL GUARANTEES FOR SOCIAL MEDIA CRIME INVESTIGATION FROM A TECHNICAL-LEGAL PERSPECTIVE

Jackson Daniel Florez. Ingeniero de Sistemas (IUPSM), Abogado (UNELLEZ). Magíster en Gerencia Empresarial (UFT). Doctorante en Ciencias Forenses (UNELLEZ-VPDS). Correo electrónico: jacksonflorez6@gmail.com

---

Recibido: Septiembre 2025 **Aceptado: Diciembre 2025**

RESUMEN

La investigación se centró en un estudio sobre la Informática Forense en Venezuela y su contribución a la mejora de las investigaciones en los delitos informáticos cometidos en redes sociales, especialmente en la ciudad de Barinas. Por lo dinámico y actual de la temática, se busca establecer la eficacia de esta disciplina como auxiliar de la justicia moderna para detectar pistas sobre delitos en plataformas digitales. El propósito general es determinar cómo la informática forense aporta significativamente a los investigadores competentes en la materia para detectar robo de información, suplantación de identidad y divulgación de información personal. La metodología utilizada se fundamenta en un enfoque cualitativo de tipo documental y descriptivo. Se realiza una revisión del ordenamiento jurídico respectivo (Constitución, Ley Especial contra Delitos Informáticos, Ley de Infogobierno) empleando la hermenéutica jurídica para la interpretación de los textos legales. Se concluye que la informática forense aporta jurisprudencia al sistema jurídico venezolano, garantizando la integridad de la evidencia digital, la cual es sumamente frágil.

Palabras clave: Informática Forense, Delitos Informáticos, Investigación, Redes Sociales.

ABSTRACT

The research focused on a study regarding Computer Forensics in Venezuela and its contribution to improving investigations of cybercrimes committed on social networks, specifically in the city of Barinas. Due to the dynamic and contemporary nature of the subject, it seeks to establish the effectiveness of this discipline as an auxiliary to modern justice for detecting clues about crimes on digital platforms. The general purpose is to determine how computer forensics significantly assists competent investigators in detecting information theft, identity theft, and the disclosure of personal information. The methodology used is based on a qualitative, documentary, and descriptive

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

approach. A review of the respective legal system is carried out (Constitution, Special Law against Computer Crimes, Infogovernment Law) using legal hermeneutics for the interpretation of legal texts. It is concluded that computer forensics provides jurisprudence to the Venezuelan legal system, guaranteeing the integrity of digital evidence, which is highly fragile.

Keywords: Computer Forensics, Cybercrimes, Investigation, Social Networks.

CONTEXTUALIZACIÓN DEL OBJETO DE ESTUDIO

El avance de la informática y las nuevas tecnologías ha influenciado profundamente la calidad de vida, facilitando tareas cotidianas mediante dispositivos remotos, la automatización del hogar y el apoyo emergente de la Inteligencia Artificial. No obstante, este escenario de hiperconectividad es aprovechado por ciberdelincuentes que buscan vulnerabilidades en los sistemas para comprometer la seguridad de los ciudadanos. En este ecosistema, las Tecnologías Informáticas se definen no solo como el estudio y diseño de sistemas, sino como estructuras que requieren una simbiosis entre *software* y *hardware* para garantizar procesos de comodidad, ahorro y, fundamentalmente, seguridad.

En este contexto, las redes sociales, especialmente Facebook, WhatsApp, Instagram y TikTok, han generado una revolución en la interacción humana. Para Cadena y Romero (2012), estas plataformas son espacios que permiten conectar individuos y crear comunidades sobre intereses similares como el trabajo, la lectura o las relaciones interpersonales. Sin embargo, esta vertiginosa integración social ha transformado cada perfil de usuario en una base de datos personales expuesta, situación que los perpetradores aprovechan para ejecutar delitos como el *doxing*, la extorsión, el robo de identidad y el fraude económico.

Esta problemática se agudiza al considerar que la exposición a contenidos inapropiados y el ciberacoso afectan con mayor severidad a grupos vulnerables, como niños y jóvenes, quienes a menudo carecen de la experiencia necesaria

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

para discernir entre interacciones seguras y peligrosas. Ante esta realidad, surge la necesidad de tipificar el delito informático. Según la legislación venezolana vigente, estos se comprenden como actividades ilícitas donde la informática es el medio o el fin para causar daños, provocar pérdidas o impedir el uso legítimo de sistemas, acciones que se encuentran sancionadas por la Ley Especial contra los Delitos Informáticos.

Como respuesta técnico-jurídica, la informática forense se erige como una disciplina especializada que amalgama la tecnología y la justicia. Matthews (2010) la define como un método probatorio consistente en la revisión científica, tecnológica y técnica, con fines periciales, de una colección de evidencias digitalizadas para fines legales. Su propósito fundamental es ejecutar experticias de alta precisión en casos de intercepción de comunicaciones, difusión de información privada y delitos económicos, garantizando que la investigación soporte el escrutinio legal y se mantenga a la vanguardia de las ciencias forenses contemporáneas.

RECORRIDO TEÓRICO

El sustento epistemológico de la informática forense en la actualidad no puede desligarse de la evolución vertiginosa de las Tecnologías de la Información y Comunicación (TIC). En este sentido, Melgar (2020) sostiene que estamos ante una metamorfosis de la interacción social, donde las plataformas de mensajería instantánea y las redes sociales han desplazado los canales tradicionales, convirtiéndose en el repositorio primordial de la actividad humana y, por ende, en la principal fuente de indicios probatorios. Esta transición exige que el investigador no solo posea habilidades técnicas, sino que comprenda la dicotomía entre lo cuantitativo y lo cualitativo; tal como señala Chavarría (2011), la investigación social y por extensión la forense no debe quedar atrapada en dilemas

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

metodológicos, sino adaptarse a la complejidad de los fenómenos humanos que ahora ocurren en entornos digitales.

Desde esta perspectiva, la informática forense se erige como una disciplina científica que, en palabras de Gallardo, Fuentes y Fuentes (2016), trasciende la mera recuperación de datos. Se define como el conjunto de técnicas de carácter técnico-jurídico destinadas a la extracción de evidencia digital bajo protocolos estrictos que garanticen su integridad. Al respecto, Tamayo y Tamayo (2012) subrayan que el proceso de la investigación científica debe ser riguroso y sistemático; aplicado a lo forense, esto implica que la "escena del crimen" digital desmaterializada y extendida a la nube debe ser tratada bajo una metodología que soporte el escrutinio legal más exigente, asegurando que la recolección de evidencias no sea fruto del azar, sino de un procedimiento científico validado.

En el ámbito de la lucha contra el fraude, Díaz (2021) enfatiza que la auditoría forense es una herramienta incuestionable de transparencia. No se trata solo de hallar un archivo, sino de aplicar procesos lógicos para demostrar que dicho elemento no ha sido manipulado. En Venezuela, este respaldo institucional se materializa a través del Centro Nacional de Informática Forense (CENIF, 2014), el cual funciona como el laboratorio de vanguardia del Estado para garantizar que las experticias en dispositivos móviles y redes sociales cumplan con los estándares de seguridad y autenticidad necesarios para la administración de justicia.

Finalmente, la fundamentación teórica encuentra su asidero legal en la Ley Especial contra los Delitos Informáticos (2001), la cual proporciona la base dogmática para entender el delito no como un acto aislado, sino como una vulneración a sistemas protegidos. Para Matthews (2010), este marco permite que la informática forense actúe como un método probatorio que conjuga la ciencia con el derecho. En consecuencia, la convergencia entre el derecho y la ingeniería

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

de sistemas crea un nuevo paradigma de investigación criminal en Venezuela, donde la integridad de la prueba digital es el pilar fundamental para la tutela judicial efectiva y la protección de los derechos ciudadanos en el ciberespacio.

FUNDAMENTACIÓN NORMATIVA Y MARCO JURÍDICO

El andamiaje legal que sostiene la informática forense en Venezuela no se limita a un conjunto de reglas técnicas, sino que constituye un sistema de garantías constitucionales que protegen los derechos humanos en el entorno digital. Este marco se articula desde la cúspide de la pirámide de Kelsen hasta normativas técnicas especializadas, permitiendo que la evidencia digital adquiera valor probatorio pleno en el proceso penal.

1. La Constitución de la República Bolivariana de Venezuela (1999) como Eje Axiológico:

La norma suprema establece los principios de inviolabilidad de las comunicaciones privadas (Art. 48) y el derecho al debido proceso (Art. 49). En este sentido, la informática forense actúa como el instrumento técnico que garantiza que cualquier intervención en sistemas informáticos se realice bajo tutela judicial, respetando la dignidad humana y el derecho a la defensa. La labor pericial debe, por tanto, ceñirse a estos límites constitucionales para evitar la obtención de pruebas ilícitas que viciarían el proceso.

2. Ley Especial contra los Delitos Informáticos (2001) y la Tipificación del Delito:

Esta ley representa el hito legislativo más relevante en la materia, al tipificar conductas que vulneran la integridad de los sistemas y la privacidad de los datos. Más allá de las sanciones, la ley establece en su articulado la importancia de la preservación de los sistemas como "objetos de prueba". La informática forense es

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

la disciplina que materializa el cumplimiento de esta ley, permitiendo que los tipos penales allí descritos (acceso indebido, sabotaje, estafa, entre otros) puedan ser demostrados técnica y científicamente ante los tribunales.

3. Ley de Infogobierno (2013) y la Institucionalización de la Computación Forense:

Un aporte fundamental de este texto legal es el reconocimiento explícito de la computación forense. La ley establece las directrices para el uso de tecnologías de información en el Poder Público, dictaminando que la identificación y presentación de datos electrónicos deben seguir protocolos que aseguren su inalterabilidad. Esto obliga a los órganos del Estado a adoptar estándares internacionales en la cadena de custodia de la evidencia digital.

4. El Rol Técnico del Centro Nacional de Informática Forense (CENIF):

Como brazo ejecutor del Ministerio del Poder Popular para la Ciencia y Tecnología, el CENIF (2014) se constituye como el órgano técnico de referencia en el país. Su función trasciende el peritaje; se encarga de estandarizar los procesos de recolección y análisis de datos. Su apoyo técnico a los órganos de investigación penal (como el CICPC) es vital para garantizar que las experticias en dispositivos móviles y redes sociales cuenten con el rigor científico necesario para resistir el escrutinio de las partes en un juicio oral y público.

5. Código Orgánico Procesal Penal (COPP) y la Cadena de Custodia:

Aunque es una norma adjetiva general, el COPP fundamenta la validez de la informática forense al regular la libertad probatoria y la cadena de custodia (Art. 187). La informática forense aporta los protocolos necesarios para cumplir con el registro de continuidad de la evidencia digital, asegurando que desde la incautación del dispositivo (en un procedimiento en Barinas o cualquier parte del país) hasta su análisis en el laboratorio, no exista duda sobre su integridad.

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

RECORRIDO METODOLÓGICO

La arquitectura de la presente investigación se adscribe al paradigma interpretativo con un enfoque cualitativo, el cual, según Chavarría (2011), permite superar la rigidez del empirismo lógico de las ciencias exactas para abordar fenómenos socioculturales complejos que no pueden ser explicados únicamente mediante la acumulación de datos cuantitativos. En este sentido, el estudio se define como una investigación de tipo documental y descriptiva, orientada a puntualizar las características de la informática forense en el contexto venezolano.

Para consolidar el marco estratégico, se asume el concepto de Arias (2012), quien define el marco metodológico como el conjunto de pasos, técnicas y procedimientos empleados para formular y resolver problemas. Bajo esta premisa, el proceso se sistematizó siguiendo las etapas del método científico para, como señalan Tamayo y Tamayo (2012), obtener información relevante que permita entender, verificar y aplicar el conocimiento en el área de las ciencias forenses.

El diseño de la investigación se fundamenta en el análisis de contenido de diversas fuentes primarias y secundarias, incluyendo doctrina, artículos científicos, tesis y un riguroso examen del ordenamiento jurídico nacional. De acuerdo con Martínez (2018), este nivel descriptivo permite enfocar las conclusiones sobre cómo funciona la informática forense en el presente, identificando las brechas entre la normativa legal y la praxis técnica. La metodología cualitativa se presenta, por tanto, como la más apropiada para avanzar en la formación de una teoría en fase de desarrollo (Flick, 2009, citado en Miquel et al., 1997), permitiendo una comprensión hermenéutica de la fragilidad de la evidencia digital y su tratamiento procesal.

ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

El análisis de la información recolectada permite determinar que la informática forense en Venezuela ha dejado de ser una disciplina opcional para convertirse en una necesidad imperativa del sistema de justicia moderno. La principal alternativa hallada para mitigar el impacto de los delitos en plataformas digitales reside en la aplicación de protocolos científicos que permitan la detección de pistas tales como registros de conversaciones, metadatos de correos electrónicos y trazas en chats, garantizando la integridad de la evidencia. Dado que la prueba electrónica es sumamente frágil, su tratamiento técnico especializado es lo que permite que esta aporte jurisprudencia sólida al sistema jurídico.

En este orden de ideas, se observa un robusto asidero legal que tiene su génesis en la Constitución de la República Bolivariana de Venezuela y se ramifica en leyes transversales como la Ley Especial contra los Delitos Informáticos (2001) y la Ley de Infogobierno (2013). Estos instrumentos no solo tipifican las conductas punibles, sino que consagran principios de investigación científica y tecnológica. Es relevante destacar la importancia estratégica del Centro Nacional de Informática Forense (CENIF), cuya creación en el marco del Plan de Desarrollo Económico y Social de la Nación, fortalece la capacidad del Estado para procesar datos almacenados en soportes físicos (discos duros, dispositivos móviles, unidades flash) y entornos virtuales.

Los hallazgos indican que la eficacia de la informática forense radica en su capacidad para proporcionar una identificación técnica detallada. Cada elemento recibido debe ser descrito y personalizado según sus características físicas y lógicas, permitiendo que la auditoría de redes de telecomunicación y contenidos multimedia se transforme en pruebas admisibles ante los órganos jurisdiccionales. El Estado, por tanto, posee el andamiaje legal necesario; no obstante, el desafío

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

actual reside en la actualización constante de las herramientas de *software* y *hardware* frente a la sofisticación de los métodos de ataque.

CONCLUSIONES Y CONSIDERACIONES FINALES

La investigación permite concluir que la informática forense representa el eslabón fundamental para el esclarecimiento de hechos punibles en la era de la hiperconectividad. El uso de herramientas forenses especializadas no solo busca la recuperación de datos, sino la documentación rigurosa de cada paso procesal para que la evidencia soporte el escrutinio en juicio, garantizando el respeto al debido proceso y a la tutela judicial efectiva.

Se evidencia una necesidad crítica de adaptar las ciencias forenses a la dinámica de las redes sociales, donde los ciberdelincuentes perfeccionan constantemente sus estrategias de vulneración. Por ello, el perito informático actual debe poseer un perfil multidisciplinario que combine habilidades técnicas avanzadas con una profunda comprensión del comportamiento humano y las motivaciones delictivas. La informática forense, aunque es una disciplina relativamente joven en el país, requiere una expansión académica y profesional urgente para asistir de manera eficiente a los tribunales.

De esta manera, se destaca que la mitigación del daño causado por los delitos informáticos no depende exclusivamente del brazo sancionador del Estado, sino de un enfoque preventivo integral. Es imperativo capacitar a la sociedad civil con especial énfasis en adolescentes y adultos mayores sobre los riesgos de la exposición de datos en un mundo globalizado. La prevención debe institucionalizarse desde las bases comunitarias y los centros educativos (escuelas, liceos y universidades), promoviendo una cultura de seguridad digital que reduzca la vulnerabilidad sistémica de la sociedad venezolana ante las amenazas emergentes del ciberespacio.

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2006). El proyecto de investigación: Introducción a la metodología científica. Episteme.

Arias, F. (2012). El proyecto de investigación: Introducción a la metodología científica (6ta ed.). Episteme.

Cadena Pompa, J. y Romero Herrera, L. (2012). Las redes sociales: ¿privacidad al descubierto? Contribuciones a las Ciencias Sociales. http://www.eumed.net/rev/cccss/21/

Chavarría, M. (2011). La dicotomía cuantitativa / cualitativo: falsos dilemas en investigación social. Actualidades en Psicología, 25, 1-35.

Díaz Varela, G. A. (2021). La auditoría forense como fundamento metodológico en la detección de casos de fraudes informáticos. Innovación tecnológica como proceso.

Flick, U. (2009). An introduction to qualitative research (4ta ed.). SAGE Publications.

Fuentes, T., Mazún, R. y Cancino, G. (2018). Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. Revista Avance en Ingeniería e Innovación [AEI], 2(4), 1-8.

Gallardo, R., Fuentes, A. y Fuentes, R. (2016). Un enfoque básico sobre informática forense. ResearchGate. https://www.researchgate.net/publication/311581737_Un_enfoque_basico_sobre_Informatica_Forense

Ley de Infogobierno. (2013). Gaceta Oficial de la República Bolivariana de Venezuela, 40.274, 17 de octubre de 2013.

Ley Especial contra los Delitos Informáticos. (2001). Gaceta Oficial de la República Bolivariana de Venezuela, 37.313, 30 de octubre de 2001.

Martínez, C. (2018, 24 de enero). Investigación descriptiva: Definición, tipos y características. Lifeder. https://www.lifeder.com/investigacion-descriptiva

Matthews, D. (2010). eDiscovery versus informática forense. Revista de seguridad de la información: Una perspectiva global, 118-123.

UNELLEZ JURIS Depósito Legal: BA2019000001. ISSN: 2739-0365
(2023). Vol. 4 Barinas-Venezuela

Miquel, S., Bigné, E., Lévy, J. P., Cuenca, A. C. y Miquel, M. J. (1997). Investigación de mercados. McGraw-Hill.

Tamayo y Tamayo, M. (2012). El proceso de la investigación científica (4ta ed.). Limusa Noriega Editores.