REVISTA ARBITRADA DEL CIEG - CENTRO DE INVESTIGACIÓN Y ESTUDIOS GERENCIALES (BARQUISIMETO - VENEZUELA) ISSN: 2244-8330 DEPÓSITO LEGAL: ppi201002LA3492 / ZAPATA GIL, IRENE / LA CRIMINALÍSTICA DIGITAL EN EL ABORDAJE DEL CIBERCRIMEN: CAPACIDADES Y DESAFÍOS DEL CICPC EN VENEZUELA / DIGITAL FORENSICS IN ADDRESSING CYBERCRIME: CAPABILITIES AND CHALLENGES OF THE CICPC IN VENEZUELA / Número 76 noviembre-diciembre 2025 [páginas 254-266] FECHA DE RECEPCIÓN: 10agosto2025/FECHA DE ACEPTACIÓN: 12octubre2025.

LA CRIMINALÍSTICA DIGITAL EN EL ABORDAJE DEL CIBERCRIMEN: CAPACIDADES Y DESAFÍOS DEL CICPC EN VENEZUELA

Zapata Gil, Irene 1

RESUMEN

El presente estudio estuvo enmarcado en el análisis de la criminalística digital en el abordaje del Cibercrimen: Capacidades y desafíos del CICPC en Venezuela, para lo cual se asumió la investigación, lo que evidenció que si bien Venezuela cuenta con un marco legal establecido para el cibercrimen (Ley Especial Contra los Delitos Informáticos de 2001, Código Orgánico Procesal Penal de 2021 y Constitución de 1999), la rápida evolución de las modalidades delictivas; fraudes, ransomware, ciberacoso, genera una tensión significativa debido a la antigüedad de la ley, evidenciando una brecha en la capacidad normativa para abordar las nuevas tipologías y tecnologías. En cuanto a las capacidades del CICPC, se reconoce el desarrollo de divisiones especializadas y la aplicación de las fases esenciales de la investigación forense digital (preservación, adquisición, análisis y presentación); sin embargo, estas se ven constantemente desafiadas por la insuficiente actualización tecnológica y la carencia de formación especializada en herramientas y software forense de última generación.

Palabras Clave: *Criminalística digital, cibercrimen, capacidades operativas, desafíos.*

DIGITAL FORENSICS IN ADDRESSING CYBERCRIME: CAPABILITIES AND CHALLENGES OF THE CICPC IN VENEZUELA

ABSTRACT

The present study was framed within the analysis of digital criminalistics in addressing cybercrime: Capabilities and challenges of the CICPC in Venezuela. The research showed that, although Venezuela has an established legal framework for cybercrime (Special Law Against Computer Crimes of 2001, Organic Criminal Procedure Code of 2021, and the 1999 Constitution), the rapid evolution of criminal modalities—such as fraud, ransomware, and cyberbullying—creates significant tension due to the outdated nature of the law, thus revealing a gap in the normative capacity to address new typologies and technologies. Regarding the capabilities of the CICPC, the development of specialized divisions and the application of the essential phases of digital forensic investigation (preservation, acquisition, analysis, and presentation) are recognized. However, these are constantly challenged by insufficient technological updates and the lack of specialized training in state-of-the-art forensic tools and software, as well as in the handling of both volatile and non-volatile digital evidence.

Keywords*: Digital criminalistics, cybercrime, operational capabilities, challenges.*

[1] https://orcid.org/0009-0004-2742-1419 izapatagil@gmail.com

1. INTRODUCCIÓN

En los últimos años, la era digital ha reconfigurado profundamente la faz de la sociedad, y con ella, la naturaleza y ejecución de los delitos. En Venezuela, al igual que en el panorama global, el cibercrimen ha emergido como una amenaza de creciente sofisticación y alcance, desafiando las metodologías tradicionales de investigación criminal. Desde estratagemas de fraude electrónico y *phishing* hasta sofisticados ataques de *ransomware* y el tráfico ilícito de datos, las modalidades delictivas en el ciberespacio se multiplican y evolucionan a un ritmo vertiginoso. Este escenario exige que los entes de seguridad y justicia, como el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), adapten y perfeccionen sus habilidades para operar eficazmente en un entorno donde las fronteras físicas se desdibujan y la evidencia se presenta en formatos intangibles.

Por lo que, el problema radica en que los paradigmas investigativos penales convencionales, concebidos para delitos en el plano material, demuestran ser insuficientes o ineficaces ante la especificidad del cibercrimen. La evidencia digital posee características particulares: es volátil, efímera y demanda un manejo altamente especializado para su correcta identificación, preservación, adquisición y análisis. La ausencia de protocolos estandarizados, la escasez de recursos tecnológicos de vanguardia y la falta de personal altamente cualificado en criminalística digital pueden conducir a la pérdida irrecuperable de pruebas, la impunidad de los ciberdelincuentes y la erosión de la confianza pública en el sistema judicial.

En este mismo orden, Casey (2011:3), hace referencia que, "la investigación forense digital no es una simple extensión de la criminalística tradicional, sino una disciplina con metodologías, herramientas y desafíos distintivos para el procesamiento de la evidencia electrónica". Esta afirmación que hace énfasis en la imperiosa necesidad de una especialización profunda por parte de los organismos encargados de la investigación en este ámbito. Considerando que, la criminalística digital se establece como la disciplina fundamental para el abordaje efectivo del cibercrimen. Su aplicación no solo permite a los investigadores rastrear las huellas electrónicas dejadas por los ciberdelincuentes, sino también reconstruir sucesos digitales complejos, identificar a los actores involucrados y presentar pruebas digitalmente válidas en un entorno judicial.

Es así como Nelson, Phillips y Steuart (2015:15), afirman que, "la capacidad de una organización para contrarrestar el cibercrimen está directamente vinculada a su maestría en la criminalística digital, la cual abarca desde la colección adecuada de evidencia hasta el análisis avanzado de redes y dispositivos". Dejando claro que, la integración de esta especialidad es, indispensable para que el CICPC logre desentrañar la complejidad de los delitos en el ciberespacio, asegurando la validez de las pruebas y la efectividad de las acciones judiciales.

De allí que, la trascendencia de analizar las capacidades y desafíos del CICPC en la contención del cibercrimen mediante la criminalística digital es incuestionable. Un examen exhaustivo de esta temática no solo permitirá identificar las fortalezas presentes en el organismo, sino también señalar las brechas y limitaciones que requieren atención prioritaria para optimizar su desempeño. Comprender los avances tecnológicos necesarios, la formación especializada del capital humano y las adaptaciones en el marco legal es crucial para proponer estrategias que fortalezcan la respuesta del Estado venezolano ante esta amenaza creciente. El éxito en la lucha contra el cibercrimen no solo repercutirá en la seguridad de los ciudadanos, sino que también protegerá infraestructuras críticas y contribuirá a la estabilidad económica del país.

Razones por las cuales, el interés del presente estudio de analizar las capacidades y desafíos de la criminalística digital del CICPC en el abordaje del cibercrimen en Venezuela, lo cual ser realizo con la revisión pormenorizada de la literatura especializada, los marcos legales pertinentes y la información disponible sobre las prácticas de la institución. Esta aproximación busca comprender la evolución de sus métodos, las herramientas utilizadas y los obstáculos que restringen su accionar, con el fin de generar un corpus de conocimiento que sirva de base para la formulación de futuras estrategias de fortalecimiento.

1.1 Contexto de la Investigación

El siglo XXI ha marcado una transformación sin precedentes, impulsada por la era digital, que ha redefinido no solo la forma en que interactuamos, sino también la naturaleza misma de la criminalidad. En Venezuela, al igual que en el panorama global, el cibercrimen ha emergido como una amenaza de creciente sofisticación y alcance, desafiando las estructuras tradicionales de investigación criminal. Desde estratagemas de fraude electrónico y *phishing* hasta sofisticados ataques de *ransomware* y el tráfico ilícito de datos, las modalidades delictivas en el ciberespacio se multiplican y evolucionan a un ritmo vertiginoso. Esta realidad exige, de manera perentoria, que los entes de seguridad y justicia, como el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), adapten y perfeccionen sus habilidades para operar eficazmente en un entorno donde las fronteras físicas se desdibujan y la evidencia se presenta en formatos intangibles.

Todo ello, tomando en cuenta que, la problemática central se manifiesta en la profunda disparidad entre los esquemas investigativos convencionales y la inherente especificidad del cibercrimen. Las metodologías forenses desarrolladas para el universo material chocan frontalmente con la naturaleza inmaterial, volátil y a menudo efímera de la evidencia digital. A diferencia de las huellas dactilares o las pruebas balísticas, los datos electrónicos demandan una pericia técnica y herramientas especializadas no solo para su identificación y preservación, sino también para su adquisición, análisis exhaustivo y presentación válida en sede judicial. La ausencia de protocolos estandarizados para esta nueva forma de

evidencia, sumada a la escasez de recursos tecnológicos de vanguardia y la falta de personal altamente cualificado en criminalística digital, puede derivar en la pérdida irrecuperable de elementos probatorios cruciales.

Este escenario no solo fomenta la impunidad de los ciberdelincuentes, sino que también socava la confianza pública en la capacidad del sistema de justicia para garantizar la seguridad en el ámbito digital. Casey (2011:3)**,** al diferenciar el campo, subraya que "la investigación forense digital no es una simple extensión de la criminalística tradicional, sino una disciplina con metodologías, herramientas y desafíos distintivos para el procesamiento de la evidencia electrónica". Esto enfatiza la necesidad de una especialización profunda y autónoma.

Como se puede apreciar, en la realidad actual la criminalística digital se ha convertido en lo que podría llamarse una disciplina fundamental para el abordaje efectivo del cibercrimen. Teniendo en cuenta que, su aplicación no solo permite a los investigadores rastrear las huellas electrónicas dejadas por los ciberdelincuentes, sino también reconstruir sucesos digitales complejos, identificar a los actores involucrados y presentar pruebas digitalmente válidas en un entorno judicial. Según Nelson, Phillips y Steuart (2015:15), la capacidad de una organización "para contrarrestar el cibercrimen está directamente vinculada a su destreza y conocimiento en la criminalística digital, la cual abarca desde la recolección adecuada de evidencia hasta el análisis avanzado de redes y dispositivos". La integración de esta especialidad es, por lo tanto, indispensable para que el CICPC logre desentrañar la complejidad de los delitos en el ciberespacio, asegurando la validez de las pruebas y la efectividad de las acciones judiciales.

De allí, el interés por analizar las capacidades y desafíos del CICPC en la contención del cibercrimen mediante la criminalística digital es incuestionable. Un examen exhaustivo de esta temática no solo permitirá identificar las fortalezas presentes en el organismo, sino también señalar las brechas y limitaciones que requieren atención prioritaria para optimizar su desempeño. Comprender los avances tecnológicos necesarios, la formación especializada del capital humano y las adaptaciones en el marco legal es crucial para proponer estrategias que fortalezcan la respuesta del Estado venezolano ante esta amenaza creciente. El éxito en la lucha contra el cibercrimen no solo repercutirá en la seguridad de los ciudadanos, sino que también protegerá infraestructuras críticas y contribuirá a la estabilidad económica del país.

1.2 Antecedentes

La dinámica del cibercrimen que se vive en estos tiempos exige una constante actualización de las estrategias de investigación criminal, y la criminalística digital como la vanguardia en este campo. Un antecedente contemporáneo es el artículo escrito por Molina Brizuela (2024), titulado **"**La Informática Forense como

Herramienta Esencial en la Lucha contra el Cibercrimen Venezolano", el cual proporciona un marco conceptual y metodológico indispensable para entender la criminalística digital en el contexto actual del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) en Venezuela**.** La autora, al exhibir una teoría dogmática de la criminalística y analiza la informática forense como herramienta esencial, subraya la importancia crítica de esta disciplina para enfrentar la creciente sofisticación de los delitos digitales.

La autora estaca la identificación, preservación y presentación de evidencia digital como procesos centrales para la resolución de casos y la determinación de responsabilidades. Para el CICPC, esto implica que las capacidades no solo se limitan a la pericia técnica en el análisis de datos, sino también a la necesidad de una comprensión profunda de los desafíos que enfrenta Venezuela debido a la rápida evolución tecnológica, la complejidad inherente de los ciberdelitos y las particularidades del sistema jurídico nacional. Estos retos persisten y se magnifican en el panorama actual, exigiendo al CICPC una inversión continua en capacitación especializada, una actualización legislativa constante que se adapte a las nuevas tipologías delictivas, una colaboración interinstitucional más estrecha tanto a nivel nacional como internacional, y una investigación continua que permita anticipar y responder a las amenazas emergentes.

En este mismo orden y en la vanguardia de la discusión sobre la criminalística digital y el abordaje del cibercrimen en Venezuela, destaco el artículo escrito por Rodríguez (2025), titulado Delitos Informáticos: Análisis Forense de la Ciberseguridad en Venezuela**.** Este artículo es particularmente relevante para el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), ya que analiza los riesgos legales de la ciberseguridad en el país, el marco normativo de los delitos informáticos y, fundamentalmente, la eficacia de la criminalística forense para investigar y analizar incidentes que atentan contra la seguridad informática.

El autor hace énfasis en que, la criminalística forense desempeña un papel crucial no solo en la colección y manejo de evidencias cibernéticas, sino también en su función preventiva, al permitir la identificación de patrones delictivos y la anticipación de posibles ataques. Este estudio, con su metodología documental y análisis crítico-interpretativo, provee una visión actualizada sobre los desafíos y la importancia estratégica de la informática forense para el CICPC, en su rol de proteger la sociedad venezolana frente a un panorama cibernético en constante evolución.

Como se puede apreciar estos antecedentes son fundamentales para este estudio, ya que establecen un marco temporal y conceptual sólido para entender la criminalística digital en Venezuela. Uno resalta la informática forense como herramienta esencial, señalando sus desafíos epistemológicos y legales, mientras que el otro ofrece una visión actual, analizando su eficacia en el contexto

específico de la ciberseguridad y los riesgos legales. Ambos convergen en la crítica necesidad de fortalecer las capacidades del CICPC en protocolos de investigación, tecnología y formación, delineando los retos y la relevancia de la criminalística digital para la justicia y la seguridad en el país.

2. METODOLOGÍA

El estudio sobre la Criminalística Digital en el Abordaje del Cibercrimen: Capacidades y Desafíos del CICPC en Venezuela adopta un enfoque metodológico de investigación documental bibliográfica. Este método, en línea con los planteamientos de Flick (2018), quien refiere que la importancia de una revisión exhaustiva y sistemática de la literatura existente. Esto incluye la consulta de artículos científicos, tesis doctorales, informes especializados de organismos de ciberseguridad, y la legislación pertinente, tanto a nivel nacional como internacional. Esta selección meticulosa de fuentes permite establecer el marco teórico y práctico que sustenta la criminalística digital, así como identificar con precisión los desafíos y oportunidades que el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) enfrenta en su lucha contra el cibercrimen en el contexto venezolano.

Asimismo, para el proceso investigativo se consideró el planteamiento de Hernández, Fernández & Baptista (2018), realizado este por fases que aseguraran la profundidad y fiabilidad del análisis. Primero, se realizó una búsqueda sistemática de información en bases de datos académicas reconocidas y repositorios especializados, utilizando palabras clave que garanticen la relevancia de los resultados. Posteriormente, se aplicarán técnicas de análisis de contenido y fichaje a la documentación recopilada, extrayendo datos clave, conceptos, metodologías forenses y las perspectivas de distintos autores sobre la temática. Finalmente, se procedió a la síntesis integradora de todos los hallazgos para construir un conocimiento coherente que no solo describa el estado actual de la criminalística digital en el CICPC, sino que también proponga líneas de acción y recomendaciones concretas para el fortalecimiento de sus capacidades operativas y estratégicas.

3. FUNDAMENTACIÓN TEORICA

La comprensión de la criminalística digital en el contexto del cibercrimen y los desafíos del CICPC en Venezuela se fundamenta en diversas teorías que aportan solidez conceptual a su abordaje. Una de las bases teóricas más relevantes es la Teoría de la Prueba Digital, que establece los principios para la admisibilidad y validez de la evidencia electrónica en un proceso judicial. Según Casey (2011), la volatilidad, la invisibilidad y la facilidad de modificación de los datos digitales requieren de protocolos forenses específicos y rigurosos para garantizar su autenticidad e integridad. Esta teoría es fundamental pues, no basta con colectar datos; es imperativo seguir una cadena de custodia inquebrantable y aplicar

técnicas de análisis forense que validen la evidencia ante los tribunales venezolanos, asegurando así que los hallazgos digitales puedan sostener una acusación y contribuir a la determinación de responsabilidades en delitos cibernéticos.

De igual manera, se hace referencia a la Teoría de la Actividad Rutinaria, adaptada al entorno digital por criminólogos como Cohen y Felson (1979), esta teoría postula que un delito ocurre cuando convergen un agresor motivado, un objetivo atractivo o vulnerable (sistemas informáticos, datos, infraestructuras críticas) y la ausencia de guardianes capaces (controles de seguridad, software antivirus, marcos legales o capacidades de investigación). Esta teoría no solo ayuda a identificar a los ciberdelincuentes, sino también las vulnerabilidades sistémicas y los factores de oportunidad que explotan. Lo que permite que los órganos de investigación orienten sus esfuerzos no solo hacia la investigación *ex post facto* de los delitos, sino también hacia la promoción de medidas preventivas y el fortalecimiento de la ciberseguridad a nivel nacional, mitigando las condiciones que favorecen la comisión de crímenes digitales en Venezuela.

3.1 El Cibercrimen

El cibercrimen, es considerado un fenómeno que ha redefinido el panorama delictivo global, se refiere a cualquier actividad criminal que involucra una computadora, una red o un dispositivo en red. Wall (2008:21)**,** uno de los autores pioneros en la criminología cibernética, proporciona una definición amplia al señalar que "la ciberdelincuencia puede definirse como cualquier actividad criminal que se comete utilizando computadoras y la tecnología de la información, donde la computadora es tanto el instrumento como el objeto del delito". Esta conceptualización es fundamental porque abarca la dualidad del rol tecnológico en la comisión de estos ilícitos.

En este sentido, la clasificación del cibercrimen es variada y dinámica, evolucionando con el avance tecnológico y la inventiva de los delincuentes. Generalmente, se distinguen categorías como delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas (hacking, ataques DDoS); delitos relacionados con el contenido (pornografía infantil, incitación al odio); y delitos relacionados con la propiedad intelectual (piratería, falsificación). Históricamente, el cibercrimen ha pasado de ser una actividad realizada por *hackers* individuales con fines de reconocimiento o curiosidad en las décadas de 1970 y 1980, a una industria criminal organizada y globalizada que opera a través de redes sofisticadas, buscando principalmente el lucro económico o el espionaje, como se observa desde principios del siglo XXI.

3.2 Modalidades Comunes de Cibercrimen

La evolución del cibercrimen ha dado lugar a una miríada de modalidades delictivas que afectan a individuos, empresas y gobiernos por igual. Entre las más

comunes, se encuentran los fraudes electrónicos**,** que van desde estafas con tarjetas de crédito hasta la manipulación de transacciones bancarias en línea. El phishing es una técnica recurrente dentro de los fraudes, donde los atacantes se hacen pasar por entidades legítimas para obtener información confidencial, tal como explican Furnell y Moore (2014:153), "el *phishing* es una forma de ingeniería social en la que un atacante intenta adquirir información sensible, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por una entidad de confianza en una comunicación electrónica".

El ransomware, por su parte, se ha convertido en una amenaza predominante, encriptando los archivos de la víctima y exigiendo un rescate para su liberación. El ciberacoso y el sexting no consentido representan modalidades que impactan directamente en la integridad personal, mientras que el hacking**,** en su sentido más amplio, abarca desde la intrusión no autorizada en sistemas hasta la manipulación de datos. Finalmente, los delitos contra la propiedad intelectual en el ámbito digital, como la piratería de software, música o películas, continúan generando pérdidas económicas significativas a nivel global.

3.3 Fundamentos de la Criminalística Digital / Informática Forense

La criminalística digital, también conocida como informática forense, se ha asumido como una disciplina científica esencial dedicada a la recuperación, análisis y presentación de evidencia digital en investigaciones legales. Su definición va más allá de la recuperación de datos; implica una aplicación rigurosa de principios científicos para garantizar la autenticidad e integridad de la información electrónica. Nelson, Phillips, y Steuart (2019:3), refiere que la criminalística digital es "la ciencia de adquirir, preservar, recuperar, analizar y presentar datos que pueden ser utilizados como evidencia en un tribunal".

Estos planteamientos conllevan una adhesión estricta a principios como la legalidad (actuar siempre dentro del marco jurídico), la integridad (asegurar que la evidencia no sea alterada) y la objetividad (mantener la imparcialidad en el proceso). Estos fundamentos son cruciales para que cualquier hallazgo digital sea admisible y persuasivo en un proceso judicial, diferenciando la mera recuperación de datos de una verdadera investigación forense.

3.4 Fases de la Investigación Forense Digital y Tipos de Evidencia

La investigación en criminalística digital sigue un proceso estructurado a través de fases bien definidas para asegurar la validez de la evidencia. La primera es la preservación, donde se asegura el estado original de la escena digital y se previene cualquier alteración de la evidencia. Le sigue la adquisición, que implica la creación de copias forenses bit a bit de los dispositivos, garantizando la inmutabilidad del original, tal como enfatiza Carrier (2005), la importancia de la exactitud de la copia para el análisis posterior. La fase de análisis es donde los especialistas examinan la evidencia adquirida para extraer información relevante,

reconstruir eventos y conectar actividades con posibles autores, utilizando herramientas especializadas.

En este sentido, la presentación implica documentar y comunicar los hallazgos de manera clara y comprensible para el sistema judicial. En cuanto a los tipos de evidencia digital, se distinguen la volátil (información efímera que se pierde al apagar el sistema, como la memoria RAM o conexiones de red activas) y la no volátil (datos persistentes en discos duros, SSD, USB, etc.). Para el manejo de esta evidencia y la ejecución de las fases, se emplean herramientas y software especializados como EnCase, FTK Imager, Autopsy, y Oxygen Forensic Detective, que facilitan desde la adquisición forense hasta el análisis de datos complejos y la generación de informes periciales.

3.5 Marco Legal Aplicable al Cibercrimen en Venezuela

El marco legal aplicable al cibercrimen, tiene su raíz en la Constitución de la República Bolivariana de Venezuela (1999), la cual establece el fundamento para el abordaje del cibercrimen. Esta norma suprema garantiza derechos fundamentales como la privacidad de las comunicaciones, la inviolabilidad del hogar y la protección de los datos personales, derechos que son esenciales en el entorno digital. Al mismo tiempo, la Constitución sienta las bases para el acceso a la información y la seguridad jurídica, legitimando la creación de leyes y organismos destinados a proteger estos principios en el ciberespacio. Las disposiciones constitucionales actúan como el marco superior que orienta y limita la actuación de los órganos de investigación, como el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), asegurando que cualquier intervención en el ámbito digital se realice respetando los derechos y garantías fundamentales de los ciudadanos.

En este mismo orden, se tiene La Ley Especial Contra los Delitos Informáticos (LECDI- 2001), el instrumento legal más específico para la tipificación y sanción de las conductas ilícitas en el ciberespacio venezolano. Esta ley delimita el alcance de los delitos informáticos**,** cubriendo el acceso indebido, el fraude, el sabotaje y la violación de la privacidad de datos, entre otros. Complementariamente, el Código Orgánico Procesal Penal (COPP 2021) es vital al establecer las disposiciones procesales sobre la prueba digital y la cadena de custodia. El COPP reconoce la validez de la evidencia electrónica, pero exige un rigor extremo en su recolección, preservación y análisis para asegurar su autenticidad e integridad y, por ende, su admisibilidad en el proceso judicial. La observancia de estas normativas es indispensable para la actuación legal y efectiva de las autoridades en la investigación y persecución del cibercrimen.

De igual manera, la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo permite abordar las estructuras criminales transnacionales que con frecuencia utilizan el ciberespacio para sus operaciones.

Si bien estas leyes no son exclusivas del ámbito informático, proporcionan herramientas adicionales para desarticular redes delictivas complejas y sus actividades financieras ilícitas. A pesar de la existencia de este corpus legal, el desafío constante reside en la actualización y adecuación de estas normas a la rápida evolución tecnológica y a las nuevas modalidades de cibercrimen, un aspecto crucial para que el Estado venezolano cuente con un arsenal jurídico robusto y pertinente que le permita proteger eficazmente a la sociedad en la era digital.

4. ANÁLISIS

El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) en Venezuela ha desarrollado capacidades actuales en el ámbito de la criminalística digital, esenciales para enfrentar el creciente cibercrimen. Estas capacidades se fundamentan en la existencia de la División de Investigaciones de Delitos Informáticos, la cual agrupa a peritos y funcionarios con formación específica en el análisis de evidencia digital. La existencia de la Ley Especial Contra los Delitos Informáticos (LECDI 2001) les proporciona un marco legal para tipificar las conductas ilícitas, permitiendo la acción policial y judicial contra el acceso indebido, los fraudes electrónicos y el sabotaje, entre otros.

Además, el Código Orgánico Procesal Penal (COPP 2021) es clave al establecer los procedimientos para la recolección, preservación y cadena de custodia de la prueba digital, dotando al CICPC de las herramientas procesales para que la evidencia obtenida sea válida en un juicio. Molina Brizuela (2024), en su estudio, subraya cómo la informática forense, como herramienta esencial, permite al CICPC la identificación y presentación de evidencia en averiguaciones criminales, confirmando su rol crucial en la resolución de casos de ciberdelincuencia.

A pesar de las capacidades establecidas, el CICPC enfrenta desafíos significativos en la lucha contra el cibercrimen. Uno de los principales es la rápida evolución tecnológica de los delitos digitales, que a menudo supera la actualización de las herramientas y el software forense disponibles para la institución. Como señala Rodríguez (2025), la eficacia de la criminalística forense depende de su capacidad para investigar y analizar incidentes que atentan contra la seguridad informática, lo que implica una inversión constante en tecnología de punta. Además, la complejidad de los delitos informáticos, que frecuentemente involucran redes transnacionales y el uso de técnicas de anonimato y cifrado, dificulta la identificación de perpetradores y la recolección de evidencia transfronteriza. La brecha en la capacitación especializada del personal también es un reto, ya que el conocimiento en áreas como el análisis de *ransomware*, forense en la nube o análisis de *blockchain* requiere formación continua y avanzada.

Otro desafío primordial para el CICPC es la adecuación del marco legal a las nuevas modalidades de cibercrimen. Aunque la LECDI fue pionera en su momento,

su antigüedad (2001) hace que algunas de sus tipificaciones no abarquen por completo las complejidades de los delitos digitales contemporáneos. Esto puede generar vacíos legales o dificultades en la interpretación de la ley para casos de reciente aparición. La Constitución de la República Bolivariana de Venezuela (1999), si bien garantiza derechos fundamentales, también presenta el reto de equilibrar la privacidad del ciudadano con la necesidad de acceder a datos para la investigación criminal. La lentitud en los procesos de actualización legislativa limita la capacidad de respuesta legal del CICPC frente a amenazas emergentes y sofisticadas, lo que resalta la importancia de una revisión y reforma constante de la normativa.

Asimismo, la colaboración interinstitucional e internacional representa tanto una capacidad en desarrollo como un desafío constante. Si bien existen esfuerzos de cooperación, la efectividad en la lucha contra el cibercrimen transnacional exige una mayor articulación con organismos nacionales como CONAS y el MP, y una integración más fluida con Interpol y otras agencias de seguridad cibernética a nivel global. Los desafíos incluyen la superación de barreras burocráticas, la armonización de legislaciones y la agilización de los procesos de solicitud de información transfronteriza. Para el CICPC, maximizar su efectividad en el abordaje del cibercrimen requerirá una inversión sostenida en recursos tecnológicos y humanos, una actualización legislativa proactiva y un fortalecimiento de las redes de cooperación que le permitan enfrentar un entorno delictivo digital que no conoce fronte.

4.1 Hallazgos del Análisis

El análisis exhaustivo de la criminalística digital en el abordaje del cibercrimen en Venezuela revela varios hallazgos cruciales. Primero, se observa que Venezuela posee un marco legal establecido, con la Ley Especial Contra los Delitos Informáticos (2001) como pilar fundamental, complementada por el Código Orgánico Procesal Penal (2021) y las garantías constitucionales de 1999. Sin embargo, pese a esta base, la rápida y compleja evolución de las modalidades de cibercrimen desde fraudes sofisticados hasta ataques de *ransomware* y ciberacoso genera una tensión constante con la antigüedad de la ley especial, un punto señalado por autores como Molina Brizuela (2024). Esto indica una brecha en la capacidad de la normativa para abarcar las nuevas tipologías delictivas y las tecnologías emergentes, lo que representa un desafío significativo para la persecución efectiva.

En segundo lugar, se constata que el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) ha desarrollado capacidades operativas en criminalística digital, materializadas en divisiones especializadas y la aplicación de las fases esenciales de la investigación forense (preservación, adquisición, análisis y presentación), conforme a los principios de la prueba digital. No obstante, estas capacidades se ven constantemente desafiadas por la necesidad de

actualización tecnológica y de formación especializada. La disponibilidad y el dominio de herramientas y software forense de última generación, así como la capacitación continua del personal en las complejidades de la evidencia digital volátil y no volátil, son insuficientes frente a la sofisticación de los ciberdelincuentes, una preocupación también planteada por Rodríguez (2025) al analizar la eficacia de la criminalística forense en el contexto venezolano.

5. REFLEXIONES FINALES

Es evidente que, aunque el CICPC ha sentado bases importantes, la lucha contra el cibercrimen es una carrera armamentista en la que la inercia puede tener consecuencias graves para la seguridad ciudadana y la estabilidad digital del país.

La complejidad intrínseca del cibercrimen, que trasciende fronteras y explota vulnerabilidades globales, exige que Venezuela no solo fortalezca sus capacidades internas, sino que también intensifique la cooperación internacional y la armonización de marcos jurídicos.

La efectiva criminalística digital, como se desprende del análisis de autores como Casey (2011) y Wall (2008), es una disciplina dinámica que requiere no solo pericia técnica, sino también una profunda comprensión del contexto legal y las motivaciones criminológicas.

El éxito del CICPC en el abordaje del cibercrimen dependerá de una inversión sostenida y estratégica en talento humano, infraestructura tecnológica y desarrollo legislativo. Esto implica la creación de programas de capacitación que no solo cubran las técnicas forenses básicas, sino que también aborden las emergentes amenazas cibernéticas y las tecnologías disruptivas.

Una proactiva actualización de la Ley Especial Contra los Delitos Informáticos es indispensable para garantizar que el CICPC disponga de las herramientas jurídicas adecuadas para enfrentar las nuevas modalidades delictivas. La criminalística digital no es solo una herramienta de investigación *ex post facto*, sino un componente crítico de la estrategia nacional de ciberseguridad, cuyo fortalecimiento es vital para proteger la infraestructura crítica, la economía y los derechos fundamentales de los venezolanos en la era digital.

6. REFERENCIAS

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.

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

Código Orgánico Procesal Penal (2021). Publicado en Gaceta Oficial de la República Bolivariana de Venezuela N.º 6.649 Extraordinario. Caracas, Venezuela

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach [Cambio social y tendencias de la tasa de criminalidad: un enfoque de la actividad rutinaria]. *American Sociological Review*, *44*(4), 588–608.

Constitución de la República Bolivariana de Venezuela (1999). Publicada en Gaceta Oficial de la República Bolivariana de Venezuela N.º 36.860 Extraordinario. Caracas, Venezuela.

Flick, U. (2018). *An introduction to qualitative research*. Sage Publications.

Furnell, S., & Moore, P. (2014). *Cybercrime: Vandalizing the Information Society* [Cibercrimen: vandalizando la sociedad de la información]. Springer.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (7a ed.). McGraw-Hill Education.

Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012). Publicada en Gaceta Oficial de la República Bolivariana de Venezuela N.º 39.912. Caracas, Venezuela.

Ley Especial Contra los Delitos Informáticos (LECDI 2001). Publicado en Gaceta Oficial de la República Bolivariana de Venezuela N.º 37.313. Caracas, Venezuela

Molina Brizuela, J. R. (2024). La Informática Forense como Herramienta Esencial en la Lucha contra el Cibercrimen Venezolano. *Insitus, Revista de Ciencias y Humanidades*. https://www.spanishdict.com/translate/la%20revista.

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations* (5th ed.). Cengage Learning.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations* (6th ed.). Cengage Learning.

Rodríguez, M. (2025). Delitos Informáticos: Análisis Forense de la Ciberseguridad en Venezuela: CYBERCRIMES: FORENSIC ANALYSIS OF CYBERSECURITY IN VENEZUELA. *UBAIUS*, *(16)*, 80–90. https://revistasuba.com/index.php/UBAIUS/article/view/1236

Wall, D. S. (2008). *Cybercrime: The Transformation of Crime in the Information Age* [Cibercrimen: la transformación del crimen en la era de la información]. Polity Press.