REVISTA ARBITRADA DEL CIEG - CENTRO DE INVESTIGACIÓN Y ESTUDIOS GERENCIALES (BARQUISIMETO - VENEZUELA) ISSN: 2244-8330 DEPÓSITO LEGAL: ppi201002LA3492 / LÓPEZ NAVARRO, LINDBERGH / LA CIBERCRIMINALÍSTICA: FUNDAMENTOS TEÓRICOS, PRINCIPIOS CLÁSICOS Y RETOS EMERGENTES EN LA INVESTIGACIÓN DIGITAL DEL SIGLO XXI / CYBERCRIMINALISTICS: THEORETICAL FOUNDATIONS, CLASSICAL PRINCIPLES AND EMERGING CHALLENGES IN 21ST-CENTURY DIGITAL INVESTIGATION / Número 78 marzo-abril 2026 [páginas 256-268 FECHA DE RECEPCIÓN: 29enero2026/FECHA DE ACEPTACIÓN: 28febrero2026.

LA CIBERCRIMINALÍSTICA: FUNDAMENTOS TEÓRICOS, PRINCIPIOS CLÁSICOS Y RETOS EMERGENTES EN LA INVESTIGACIÓN DIGITAL DEL SIGLO XXI

López Navarro, Lindbergh 1

RESUMEN

El desarrollo acelerado de las tecnologías de la información y la comunicación ha generado profundas transformaciones en la criminalidad contemporánea, dando origen a nuevas modalidades delictivas desarrolladas en entornos digitales. Esta realidad ha impulsado la evolución de la criminalística tradicional hacia nuevas metodologías de investigación, destacándose la cibercriminalística como un campo de estudio orientado al análisis de la evidencia digital y la investigación de delitos informáticos. En este contexto, la investigación criminal enfrenta desafíos derivados de la complejidad de los sistemas tecnológicos, la diversidad de los entornos digitales y las características particulares de la información digital. El objetivo del presente artículo es analizar los fundamentos teóricos de la cibercriminalística, la vigencia de los principios clásicos de la criminalística en el entorno digital y los retos emergentes que enfrenta la investigación criminal en el siglo XXI. La investigación se desarrolla bajo un enfoque cualitativo, de carácter documental, mediante la revisión y análisis de literatura científica relacionada con la criminalística, la informática forense, la evidencia digital y la ciberdelincuencia. Se concluye que la cibercriminalística no sustituye a la criminalística tradicional, sino que la complementa mediante la adaptación de sus principios.

Palabras clave: *cibercriminalística, fundamentos teóricos, principios.*

CYBERCRIMINALISTICS: THEORETICAL FOUNDATIONS, CLASSICAL PRINCIPLES AND EMERGING CHALLENGES IN 21ST-CENTURY DIGITAL INVESTIGATION

ABSTRACT

The rapid development of information and communication technologies has generated profound transformations in contemporary crime, giving rise to new criminal activities developed in digital environments. This reality has driven the evolution of traditional criminalistics toward new investigative methodologies, with cybercriminalistics standing out as a field of study focused on the analysis of digital evidence and the investigation of computer crimes. In this context, criminal investigations face challenges stemming from the complexity of technological systems, the diversity of digital environments, and the unique characteristics of digital information. The objective of this article is to analyze the theoretical foundations of cybercriminalistics, the relevance of classical criminalistics principles in the digital environment, and the emerging challenges facing criminal investigations in the 21st century. The research is conducted using a qualitative, documentary approach, through the review and analysis of scientific literature related to criminalistics, digital forensics, digital evidence, and cybercrime. It is concluded that cybercrime does not replace traditional criminalistics, but rather complements it by adapting its principles.

Keywords: *cybercrime, theoretical foundations, principles, challenges.*

[1] Postdoctorado en Criminalística. Universidad Nacional Experimental de Yaracuy, (UNEY, Venezuela). llopez@unfv.edu.pe

1. **INTRODUCCIÓN**

La criminalística, como disciplina científica orientada a la investigación de los hechos delictivos, ha tenido históricamente la función de estudiar los indicios materiales encontrados en la escena del crimen con la finalidad de identificar a los responsables y reconstruir los hechos investigados. Este enfoque se ha sustentado en el análisis de evidencias físicas tales como huellas, documentos, armas, fluidos biológicos y otros elementos materiales relacionados con la comisión de un delito, siguiendo los principios clásicos de la criminalística establecidos desde los aportes de Locard (1920), quien sostuvo que todo contacto deja un rastro.

Durante décadas, la criminalística tradicional se desarrolló en escenarios físicos donde la evidencia material constituía el elemento central de la investigación criminal. Sin embargo, el avance de las tecnologías de la información y la comunicación ha transformado profundamente los escenarios delictivos, generando nuevos espacios en los que se desarrollan actividades humanas y, en consecuencia, nuevas formas de criminalidad en entornos digitales (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2013).

En la actualidad, muchos delitos ya no se cometen únicamente en espacios físicos, sino también en espacios virtuales, redes informáticas, sistemas digitales, dispositivos electrónicos y plataformas tecnológicas, dando origen a la denominada ciberdelincuencia o criminalidad informática. Esta nueva realidad ha generado la necesidad de desarrollar métodos especializados para la identificación, preservación, análisis e interpretación de la evidencia digital, la cual presenta características distintas a la evidencia física tradicional, como su intangibilidad, volatilidad, facilidad de reproducción y posibilidad de alteración (Casey, 2011; Ribas, 2012).

En este contexto surge la cibercriminalística como una evolución de la criminalística tradicional, orientada a la investigación de delitos informáticos y al análisis de la evidencia digital mediante el uso de técnicas de informática forense, análisis de sistemas informáticos y metodologías de investigación digital (Carrier, 2005; Rogers, 2006). Esta disciplina implica la aplicación de métodos científicos y tecnológicos para la identificación, preservación, análisis e interpretación de datos digitales que puedan constituir evidencia en una investigación criminal.

La importancia de la cibercriminalística radica en que la evidencia digital se ha convertido en un elemento fundamental en la mayoría de las investigaciones criminales actuales, debido a que gran parte de las actividades humanas se desarrollan mediante dispositivos electrónicos y sistemas informáticos. En consecuencia, la investigación criminal del siglo XXI requiere la integración de

conocimientos provenientes de la criminalística, la informática forense, la ciberseguridad y el análisis de datos digitales.

En ese sentido, el presente artículo tiene como propósito analizar los fundamentos teóricos de la cibercriminalística, la aplicación de los principios clásicos de la criminalística en el entorno digital y los retos emergentes que enfrenta la investigación digital en el siglo XXI. Tiene como propósito analizar los fundamentos teóricos de la cibercriminalística, la aplicación de los principios clásicos de la criminalística en el entorno digital y los retos emergentes que enfrenta la investigación digital en el siglo XXI.

2. PLANTEAMIENTO DEL PROBLEMA

El acelerado desarrollo de las tecnologías de la información y la comunicación ha transformado de manera significativa las dinámicas sociales y económicas a nivel global, generando nuevos espacios de interacción en entornos digitales. En este contexto, han emergido formas de criminalidad que trascienden los límites tradicionales del espacio físico, dando lugar a los denominados ciberdelitos, los cuales se caracterizan por su complejidad, anonimato, alcance transnacional y constante evolución tecnológica (Oficina de las Naciones Unidas contra la Droga y el Delito. (UNODC: 2013).

Esta transformación plantea importantes desafíos para la investigación criminal, particularmente en lo relacionado con la obtención y tratamiento de la evidencia. La criminalística tradicional, concebida para el análisis de evidencia física en escenarios materiales, presenta limitaciones frente a la naturaleza intangible, volátil y altamente manipulable de la evidencia digital, lo que dificulta su identificación, preservación, análisis e interpretación dentro del proceso investigativo (Casey, 2011; Ribas, 2012).

Asimismo, la ausencia de criterios metodológicos uniformes para el manejo de la evidencia digital, así como la necesidad de fortalecer la formación especializada en áreas como la informática forense, el análisis de sistemas y la ciberseguridad, evidencian la existencia de vacíos en la adaptación de la criminalística a los entornos digitales (Carrier, 2005; Rogers, 2006). A ello se suma la naturaleza transnacional de los ciberdelitos, que incrementa la complejidad de la investigación debido a la dispersión de la evidencia en múltiples sistemas y ubicaciones geográficas, dificultando su adecuada gestión.

En este escenario, se hace evidente la necesidad de desarrollar enfoques teóricos y metodológicos que permitan adaptar la criminalística a los entornos digitales, dando lugar a la cibercriminalística como una disciplina orientada al estudio, tratamiento y análisis de la evidencia digital en la investigación criminal.

En virtud de lo anterior, surge la siguiente interrogante: ¿de qué manera los fundamentos teóricos de la cibercriminalística, junto con la adaptación de los principios clásicos de la criminalística, permiten enfrentar los retos emergentes de la investigación digital en el siglo XXI?

En atención a esta problemática, el objetivo del presente artículo es analizar los fundamentos teóricos de la cibercriminalística, la vigencia de los principios clásicos de la criminalística en el entorno digital y los retos emergentes que enfrenta la investigación criminal en el siglo XXI.

3. FUNDAMENTACIÓN TEÓRICA

La cibercriminalística surge como una evolución de la criminalística tradicional ante la necesidad de investigar delitos cometidos mediante el uso de tecnologías de la información y la comunicación. La criminalística clásica ha sido definida como la disciplina científica encargada del estudio de los indicios materiales relacionados con la comisión de un delito, con la finalidad de descubrir la verdad de los hechos y determinar la responsabilidad de los autores (Locard, 1920). Sin embargo, el desarrollo tecnológico ha generado nuevas formas de criminalidad en las cuales la evidencia ya no es exclusivamente física, sino también digital, lo que ha obligado a replantear los métodos tradicionales de investigación criminal (Casey, 2011).

En este contexto, la cibercriminalística puede definirse como la disciplina científica y técnica que se encarga de la identificación, preservación, análisis e interpretación de la evidencia digital relacionada con la comisión de delitos informáticos o delitos cometidos mediante el uso de tecnologías digitales. Esta disciplina integra conocimientos de criminalística, informática forense, ciberseguridad, análisis de sistemas y análisis de datos digitales, lo que la convierte en una disciplina de carácter interdisciplinario (Carrier, 2005; Rogers, 2006).

Desde el punto de vista teórico, la cibercriminalística se fundamenta en el principio de que toda actividad realizada en un sistema informático deja un rastro digital. Estos rastros pueden consistir en registros de actividad, archivos, metadatos, direcciones IP, correos electrónicos, registros de acceso, historial de navegación, registros de servidores, entre otros elementos digitales que pueden ser utilizados como evidencia en una investigación criminal (Ribas, 2012).

Asimismo, la cibercriminalística mantiene los principios fundamentales de la criminalística clásica, tales como el principio de intercambio, el principio de correspondencia de características, el principio de probabilidad y el principio de reconstrucción de los hechos, los cuales deben ser reinterpretados en función de la evidencia digital. El principio de intercambio, formulado por Locard, establece

que todo contacto deja un rastro, lo cual en el entorno digital se traduce en que toda interacción con un sistema informático genera registros o huellas digitales que pueden ser analizadas posteriormente.

La evidencia digital presenta características particulares que la diferencian de la evidencia física tradicional. Entre estas características se encuentran su intangibilidad, volatilidad, capacidad de reproducción, facilidad de alteración y su carácter transnacional, lo que implica que la evidencia puede encontrarse almacenada en servidores ubicados en diferentes lugares. Estas características generan nuevos desafíos para la investigación criminal, especialmente en la preservación y análisis de la información digital (Casey, 2011).

Por ello, la cibercriminalística no debe entenderse como una disciplina independiente de la criminalística, sino como una especialización o evolución de esta, adaptada a los nuevos escenarios tecnológicos y a las nuevas formas de criminalidad del siglo XXI. En este sentido, la cibercriminalística se configura como una disciplina científica que surge de la necesidad de adaptar los métodos de investigación criminal a los entornos digitales, donde los delitos se cometen mediante sistemas informáticos, redes de comunicación, dispositivos electrónicos y plataformas digitales.

Desde el punto de vista teórico, la cibercriminalística se fundamenta en la teoría de la evidencia digital, la teoría de los indicios digitales y la teoría de la investigación criminal aplicada a entornos virtuales. La evidencia digital se define como cualquier información de valor probatorio almacenada o transmitida en formato digital, que puede ser utilizada para demostrar la comisión de un delito o la participación de una persona en un hecho investigado.

La teoría de los indicios digitales establece que toda interacción con un sistema informático genera rastros o huellas digitales que pueden ser recuperadas mediante técnicas de informática forense. Estos rastros pueden consistir en registros de actividad del sistema, archivos eliminados, metadatos, direcciones IP, correos electrónicos, registros de acceso, historial de navegación, registros de servidores, conversaciones en redes sociales, registros de geolocalización, entre otros.

Asimismo, la cibercriminalística se fundamenta en la teoría de la reconstrucción del hecho digital, la cual consiste en reconstruir la secuencia de eventos ocurridos en un sistema informático antes, durante y después de la comisión de un hecho delictivo digital. Esta reconstrucción se realiza mediante el análisis de registros del sistema, archivos, bases de datos, registros de red, dispositivos de almacenamiento y otros elementos digitales que permiten establecer la cronología de los hechos investigados.

Otro aspecto teórico importante es la relación entre la cibercriminalística y la criminología digital, la cual estudia el comportamiento del delincuente informático, sus motivaciones, sus métodos de ataque, sus perfiles y las tipologías de ciberdelincuentes. En este sentido, la cibercriminalística no solo se limita al análisis técnico de la evidencia digital, sino que también implica el estudio del fenómeno de la ciberdelincuencia desde una perspectiva criminológica y tecnológica, lo que la convierte en una disciplina compleja y en constante evolución.

3.1 Principios de la Criminalística Digital

La criminalística digital, al igual que la criminalística tradicional, se rige por una serie de principios científicos que orientan la investigación criminal y el análisis de la evidencia digital. Estos principios constituyen la base metodológica para la investigación de delitos informáticos y el tratamiento de la evidencia digital.

Uno de los principios fundamentales es el principio de intercambio digital, el cual establece que toda interacción con un sistema informático deja un rastro digital. Este principio es una adaptación del principio de intercambio de Locard aplicado al entorno digital, donde toda acción realizada en un sistema informático genera registros de actividad que pueden ser analizados posteriormente.

Otro principio importante es el principio de persistencia de la información digital, el cual establece que la información digital no desaparece completamente, incluso cuando es eliminada, ya que puede permanecer en sectores del disco duro, copias de seguridad, memoria del sistema, registros del sistema o servidores remotos.

El principio de integridad de la evidencia digital establece que la evidencia digital debe ser preservada en su estado original, evitando cualquier modificación, alteración o contaminación de los datos. Para ello se utilizan técnicas como la creación de imágenes forenses, el uso de funciones hash y la cadena de custodia digital (Carrier, 2005).

El principio de trazabilidad digital establece que todas las acciones realizadas durante la investigación digital deben quedar registradas, documentadas y justificadas, con el fin de garantizar la confiabilidad del análisis de la evidencia digital.

El principio de reproducibilidad establece que los resultados obtenidos en el análisis de la evidencia digital deben poder ser reproducidos por otros especialistas utilizando los mismos métodos y herramientas, lo que garantiza la confiabilidad del análisis forense digital (Rogers, 2006).

Estos principios constituyen la base científica de la criminalística digital y permiten garantizar que la evidencia digital sea obtenida, preservada, analizada y documentada mediante procedimientos técnicos y científicos.

3.2 Cadena de Custodia Digital

La cadena de custodia digital constituye uno de los elementos más importantes en la cibercriminalística, ya que garantiza la autenticidad, integridad, confiabilidad y trazabilidad de la evidencia digital durante todo el proceso de investigación. La cadena de custodia digital puede definirse como el conjunto de procedimientos técnicos y administrativos que permiten garantizar el control, registro, preservación y documentación de la evidencia digital desde su obtención hasta su análisis y almacenamiento.

A diferencia de la evidencia física, la evidencia digital puede ser fácilmente modificada, copiada, eliminada o alterada, por lo que su manejo debe realizarse mediante protocolos técnicos especializados. Por esta razón, en la investigación digital no se trabaja directamente sobre el dispositivo original, sino sobre una copia forense o imagen digital del dispositivo, con el fin de preservar la evidencia original y evitar su alteración (Carrier, 2005).

El proceso de cadena de custodia digital generalmente incluye las siguientes etapas: identificación de la evidencia digital, recolección de dispositivos electrónicos, preservación de la evidencia mediante la creación de imágenes forenses, análisis de la evidencia digital, documentación de los procedimientos realizados, almacenamiento seguro de la evidencia y presentación de los resultados del análisis.

Durante la cadena de custodia digital se utilizan herramientas técnicas como funciones hash, que permiten verificar que la evidencia digital no ha sido modificada durante el proceso de análisis. Si los valores hash de la evidencia original y de la copia forense coinciden, se puede garantizar que la evidencia se mantiene íntegra durante todo el proceso de investigación.

La cadena de custodia digital es fundamental para la confiabilidad de la evidencia digital, ya que si no se garantiza la integridad de la evidencia, los resultados del análisis podrían ser cuestionados. Por ello, la correcta aplicación de la cadena de custodia digital constituye uno de los pilares fundamentales de la cibercriminalística.

3.3 Inteligencia Artificial y Cibercriminalística

La inteligencia artificial se ha convertido en una herramienta de gran importancia para la cibercriminalística y la investigación digital, debido a su capacidad para

analizar grandes volúmenes de datos, identificar patrones, detectar anomalías y automatizar procesos de análisis forense digital.

En la investigación de ciberdelitos, la inteligencia artificial puede ser utilizada para el análisis de grandes cantidades de información digital, como correos electrónicos, registros de acceso a sistemas, transacciones digitales, redes sociales, registros de navegación y bases de datos. Mediante algoritmos de aprendizaje automático, la inteligencia artificial puede identificar patrones de comportamiento, relaciones entre usuarios, redes de actividad y eventos relevantes dentro de una investigación digital.

Asimismo, la inteligencia artificial puede utilizarse en el análisis de software malicioso, detección de intrusiones informáticas, análisis de imágenes y videos digitales, reconocimiento de patrones, análisis de documentos digitales y detección de fraudes electrónicos. Estas herramientas permiten acelerar las investigaciones digitales y mejorar la eficiencia en la identificación de evidencias digitales.

Sin embargo, la utilización de la inteligencia artificial en la investigación digital también plantea desafíos relacionados con la privacidad, la protección de datos y la confiabilidad de los sistemas automatizados, por lo que su uso debe realizarse de manera responsable y bajo criterios técnicos y científicos.

En el futuro, la inteligencia artificial, el análisis de grandes datos, la analítica forense digital y la automatización de procesos de investigación transformarán la cibercriminalística, convirtiéndola en una disciplina cada vez más tecnológica, interdisciplinaria y especializada.

3. METODOLOGÍA

El presente artículo se desarrolla bajo un enfoque cualitativo, de tipo documental, orientado al análisis teórico de la cibercriminalística como disciplina emergente dentro de las ciencias criminalísticas. La investigación se fundamenta en la revisión bibliográfica y documental de textos doctrinarios, artículos científicos y literatura especializada en criminalística, informática forense, evidencia digital, ciberdelincuencia y ciberseguridad, con la finalidad de construir un análisis teórico sobre los fundamentos de la cibercriminalística y su importancia en la investigación criminal contemporánea.

El método utilizado es el método analítico–sintético, mediante el cual se estudian los elementos que conforman la criminalística tradicional y su evolución hacia la cibercriminalística, analizando sus fundamentos teóricos, principios, características de la evidencia digital y los retos emergentes en la investigación digital. El análisis permitió descomponer el fenómeno de estudio en sus elementos teóricos y

conceptuales, mientras que la síntesis permitió integrar dichos elementos en una visión estructurada de la cibercriminalística como disciplina científica.

Asimismo, se emplea el método deductivo, partiendo de los principios generales de la criminalística para analizar su aplicación en el entorno digital y en la investigación de ciberdelitos, lo que permitió establecer la relación entre la criminalística tradicional y la criminalística digital desde una perspectiva teórica y metodológica.

La técnica de investigación utilizada fue la revisión documental, que permitió recopilar información proveniente de libros, artículos científicos y documentos académicos relacionados con la criminalística, la informática forense, la evidencia digital y la investigación digital. La información recopilada fue organizada, analizada e interpretada con el propósito de desarrollar la fundamentación teórica del estudio y analizar la evolución de la criminalística hacia la cibercriminalística en el contexto de la investigación criminal del siglo XXI.

En este sentido, la metodología empleada permitió abordar el estudio de la cibercriminalística desde una perspectiva teórica y documental, orientada a comprender sus fundamentos, principios y desafíos dentro de la investigación criminal en entornos digitales.

4. RESULTADOS Y ANÁLISIS

El análisis desarrollado permite establecer que la cibercriminalística constituye una evolución de la criminalística tradicional y no una disciplina completamente independiente, en tanto conserva sus principios fundamentales, adaptándolos a las particularidades del entorno digital (Locard, 1920; Casey, 2011). En este sentido, se evidencia una continuidad epistemológica entre ambas, sustentada en la reinterpretación de los principios clásicos frente a nuevas formas de evidencia.

En primer lugar, se confirma la vigencia del principio de intercambio formulado por Locard, el cual, trasladado al ámbito digital, implica que toda interacción con un sistema informático genera rastros susceptibles de análisis. Estos rastros se manifiestan en forma de registros de acceso, direcciones IP, archivos temporales, historiales de navegación y metadatos, constituyéndose en elementos relevantes para la investigación digital (Ribas, 2012).

En segundo lugar, se identifica que la evidencia digital presenta características diferenciadas respecto de la evidencia física tradicional, tales como su intangibilidad, volatilidad, capacidad de reproducción y facilidad de alteración. Estas particularidades generan mayores exigencias en los procesos de obtención, preservación y análisis de la evidencia, lo que refuerza la importancia de aplicar

procedimientos técnicos especializados en la investigación digital (Casey, 2011; Carrier, 2005).

En este contexto, la cadena de custodia digital adquiere un rol fundamental, al garantizar la integridad, autenticidad y trazabilidad de la evidencia digital durante todo el proceso investigativo. Su correcta aplicación permite asegurar la confiabilidad de los resultados del análisis forense digital y evitar la alteración de los datos, lo cual resulta esencial en la investigación criminal en entornos digitales (Carrier, 2005).

Otro aspecto relevante identificado es el carácter interdisciplinario de la cibercriminalística, que integra conocimientos provenientes de la criminalística, la informática forense, la ciberseguridad, la criminología y el análisis de sistemas. Esta característica evidencia la necesidad de una formación especializada por parte de los operadores encargados de la investigación, orientada al manejo adecuado de la evidencia digital y al uso de herramientas tecnológicas (Rogers, 2006).

Asimismo, se determina que uno de los principales desafíos de la investigación digital es la naturaleza transnacional de los ciberdelitos, debido a la dispersión de la evidencia en múltiples sistemas y ubicaciones, así como al uso de tecnologías que dificultan la identificación de los responsables. Esta situación incrementa la complejidad de la investigación y exige mecanismos de cooperación y coordinación a nivel internacional (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2013).

Finalmente, se observa que el desarrollo de tecnologías emergentes como la inteligencia artificial, el análisis de grandes datos, la computación en la nube, el internet de las cosas y las criptomonedas ha generado nuevos escenarios para la comisión de delitos, lo que plantea desafíos adicionales para la cibercriminalística. Estas transformaciones requieren la actualización constante de los métodos de investigación y la incorporación de herramientas tecnológicas avanzadas para el análisis de la evidencia digital.

5. DISCUSIÓN

Los resultados del análisis permiten afirmar que la cibercriminalística representa una transformación necesaria de la criminalística tradicional frente a los cambios tecnológicos y las nuevas formas de criminalidad digital. La evidencia digital se ha consolidado como uno de los elementos más relevantes en las investigaciones contemporáneas, debido a que una gran parte de las actividades humanas se desarrollan mediante dispositivos electrónicos y sistemas informáticos.

No obstante, la investigación digital plantea importantes desafíos de carácter técnico y metodológico. En este sentido, se evidencia la necesidad de fortalecer la formación especializada en áreas como la informática forense, el análisis de sistemas y la cibercriminalística, así como de desarrollar capacidades institucionales orientadas al análisis de evidencia digital en entornos complejos.

Otro aspecto relevante es la necesidad de establecer mecanismos de cooperación internacional para la investigación de ciberdelitos, considerando que estos no se limitan a fronteras territoriales y pueden involucrar múltiples jurisdicciones de manera simultánea. Esta situación incrementa la complejidad de la investigación y exige la articulación de esfuerzos entre diferentes actores y sistemas.

Asimismo, la cibercriminalística plantea retos relacionados con la protección de la información y el manejo adecuado de datos en entornos digitales, especialmente cuando la investigación implica el acceso a información contenida en dispositivos electrónicos, redes digitales o sistemas de almacenamiento remoto.

En este sentido, el desarrollo de la cibercriminalística debe orientarse hacia la construcción de enfoques equilibrados que permitan fortalecer la investigación criminal en entornos digitales, garantizando al mismo tiempo el uso adecuado de los procedimientos técnicos y el respeto a criterios científicos en el tratamiento de la evidencia digital.

En consecuencia, la cibercriminalística se proyecta como una de las áreas más relevantes de la criminalística contemporánea, en tanto la mayoría de las conductas delictivas actuales dejan algún tipo de rastro digital, lo que convierte a la investigación digital en un componente fundamental dentro del análisis criminal en el siglo XXI.

6. CONCLUSIONES

La cibercriminalística surge como una respuesta necesaria frente a la evolución de la criminalidad en el entorno digital, constituyéndose en un campo de conocimiento que integra aportes de la criminalística tradicional, la informática forense, la ciberseguridad y el análisis de sistemas digitales. Su desarrollo responde a la necesidad de investigar hechos delictivos cometidos mediante tecnologías digitales y de analizar adecuadamente la evidencia digital dentro de la investigación criminal contemporánea.

Se determinó que los principios clásicos de la criminalística mantienen su vigencia en el entorno digital, especialmente el principio de intercambio, el principio de correspondencia de características, el principio de reconstrucción de los hechos y el principio de probabilidad, los cuales deben ser reinterpretados y adaptados a la naturaleza de la evidencia digital. Esto permite afirmar que la cibercriminalística no

sustituye a la criminalística tradicional, sino que constituye una evolución metodológica de esta en función de los cambios tecnológicos y de las nuevas formas de criminalidad.

Asimismo, se concluye que la evidencia digital presenta características particulares como su intangibilidad, volatilidad, capacidad de reproducción y facilidad de alteración, lo que exige la aplicación de procedimientos técnicos especializados para su identificación, preservación, análisis e interpretación. En este contexto, la cadena de custodia digital se convierte en un elemento fundamental para garantizar la integridad y trazabilidad de la evidencia digital durante el proceso de investigación.

Otro aspecto relevante es el carácter interdisciplinario de la cibercriminalística, debido a que en la investigación digital intervienen conocimientos de criminalística, informática forense, ciberseguridad, análisis de datos y tecnología de la información, lo que implica la necesidad de formación especializada de los profesionales encargados de la investigación criminal en entornos digitales.

Se concluye también que uno de los principales retos de la cibercriminalística es la naturaleza transnacional de los delitos informáticos, así como el uso de tecnologías emergentes como la computación en la nube, las criptomonedas, el internet de las cosas y la inteligencia artificial, las cuales generan nuevos escenarios delictivos y nuevas dificultades para la investigación criminal.

Finalmente, la cibercriminalística se consolida como un campo fundamental dentro de la criminalística contemporánea, debido a que gran parte de las actividades humanas se desarrollan en entornos digitales, lo que implica que muchos hechos delictivos dejan rastros digitales que pueden ser analizados mediante técnicas de investigación digital. En este sentido, el fortalecimiento de la investigación digital, el desarrollo de metodologías especializadas y la formación interdisciplinaria constituyen elementos esenciales para el desarrollo de la cibercriminalística en el contexto de la investigación criminal del siglo XXI.

8. REFERENCIAS

Beebe, N. L., & Clark, J. G. (2007). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 4(3–4), 147–167.

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.

Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press.

Locard, E. (1930). Traité de criminalistique. Desvignes.

Maras, M. H. (2016). Cybercriminology. Oxford University Press.

Ribas, A. (2012). La prueba electrónica en el proceso judicial. La Ley.

Rogers, M. (2010). Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes. Wiley.

United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive study on cybercrime. United Nations.

ISO/IEC. (2012). ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization.