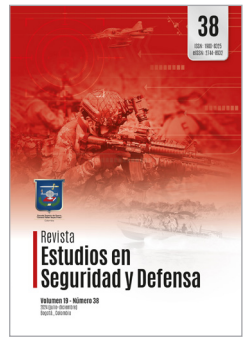
EDITORIAL ESDEG

Revista
Estudios en Seguridad y Defensa
Volumen 19, número 38, julio-diciembre 2024
Bogotá, D.C, Colombia
ISSN: 1900-8325 • eISSN: 2744-8932
Página web: https://esdegrevistas.edu.co/index.php/resd



Análisis y prospectiva para la construcción de capacidades para enfrentar el cibernarcotráfico

Analysis and foresight for capacity building to confront cyber-trafficking

Diego Rodríguez Samora
Luis Manuel Lozano Ramos
Martín Leonardo Bonilla Duitama
Nadia Peralta Romero

CITACIÓN APA:

Rodríguez Samora, D., Lozano Ramos, L. M., Bonilla Duitama, M. L. & Peralta Romero, N. (2024). Análisis y prospectiva para la construcción de capacidades para enfrentar el cibernarcotráfico. *Estudios en Seguridad y Defensa, 19*(38), 205-226. https://doi.org/10.25062/1900-8325.4839

Publicado en línea: **Diciembre 30 de 2024**

Enviar un artículo a la Revista

Revista **Estudios en Seguridad y Defensa**
Volumen 19, número 38, julio-diciembre 2024 (pp. 205-226)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Análisis y prospectiva para la construcción de capacidades para enfrentar el cibernarcotráfico

Analysis and foresight for capacity building to confront cyber-trafficking

DOI: https://doi.org/10.25062/1900-8325.4839

Diego Rodríguez Samora **Luis Manuel Lozano Ramos** **Martín Leonardo Bonilla Duitama**
Policía Nacional de Colombia

Nadia Peralta Romero
Fiscalía General de la Nación, Colombia

Resumen

Este artículo analiza el fenómeno emergente del cibernarcotráfico y las condiciones actuales para enfrentarlo, en términos de avances legales, tecnologías disruptivas y personal adecuado para desarrollar técnicas y estrategias contra este fenómeno. Este análisis se basa en la creación y operación de la primera Unidad Investigativa de Cibernarcotráfico en Colombia, y la implementación de estrategias policiales para enfrentar la creciente cibercriminalidad. Se han identificado tres tendencias clave: el desarrollo de capacidades iniciales, la interoperabilidad e hiperconvergencia de tecnologías, y la construcción de sinergias institucionales. Estos elementos combinados permiten proyectar dos escenarios probables a mediano plazo, así como determinar las necesidades y posibilidades de las instituciones encargadas de combatir este delito.

Palabras Clave: agente encubierto virtual; cibercrimen; ciberespacio; ciberpatrullaje; narcotráfico

Abstract

This article analyzes the emerging phenomenon of cyber-trafficking and the current conditions to confront it, in terms of legal advances, disruptive technologies and adequate personnel to develop techniques and strategies against this phenomenon. This analysis is based on the creation and operation of the first Cybertrafficking Investigative Unit in Colombia, and the implementation of police strategies to confront the growing cybercrime. Three key trends have been identified: the development of initial capabilities, the interoperability and hyperconvergence of technologies, and the building of institutional synergies. These combined elements make it possible to project two likely scenarios in the medium term, as well as to determine the needs and possibilities of the institutions in charge of combating this crime.

Key words: cyber patrolling; cybercrime; cyberspace; drug trafficking; virtual undercover agent

Artículo de reflexión
Recibido: 26 de enero de 2024 • **Aceptado:** 25 de julio de 2024
Contacto: Luis Manuel Lozano Ramos manuel.lozano1075@correo.policia.gov.co

Introducción

Este artículo busca ofrecer una prospectiva sobre la construcción de capacidades para abordar el cibernarcotráfico en Colombia. Esta prospectiva consiste en abordar y planificar la lucha antidrogas hacia el futuro, a partir de la construcción de escenarios donde las herramientas y técnicas disruptivas se constituyen en un factor determinante para afrontar el fenómeno del narcotráfico en el ciberespacio.

En el contexto actual del cibernarcotráfico y las tendencias para afrontarlo, diversos autores convergen en tres aspectos clave: primero, el "fracaso de la lucha antidrogas planteada de manera tradicional" (Gaviria & Mejía, 2011; López, 2016) ante un fenómeno complejo en la red; segundo, la necesidad de buscar alternativas disruptivas para abordar este desafío; y tercero, el incremento de la disponibilidad de drogas ilegales en línea. Esto subraya la responsabilidad institucional de construir un enfoque más efectivo para enfrentar el narcotráfico en el ciberespacio. En este sentido, existen dos posibles caminos institucionales: la adaptación al nuevo entorno o la determinación de influir activamente en el futuro, ya que este es múltiple y susceptible de ser moldeado (Castro, 2014).

En un determinado contexto, "suele considerarse a las instituciones encargadas de proveer el servicio público de seguridad y de confrontar el fenómeno de las drogas ilícitas en nombre del Estado, desprovistas de capacidades de planeación prospectiva" (Rodríguez et al., 2020). No obstante, se están llevando a cabo esfuerzos institucionales para anticipar y abordar futuros fenómenos delictivos, especialmente aquellos que han migrado al ciberespacio. Por ejemplo, años atrás, surgieron análisis prospectivos desde la Policía Nacional de Colombia que sugerían que "el narcotráfico sería dinamizado en el ciberespacio, y que esta tendencia, poco analizada, se encontraba en lógicas de un crecimiento incremental" (Enrique, 2014; Moreno, 2020).

Este artículo aborda el "cibernarcotráfico" como un nuevo desafío en la comprensión del Sistema de Drogas Ilícitas (SDI), un fenómeno en constante crecimiento. A partir de su análisis como un problema tanto presente como futuro, se pretende examinar y tomar decisiones estratégicas sobre cómo prevenirlo. En caso de que la conducta punible se materialice, se plantea la forma en que el servicio de policía debería reaccionar. Este enfoque permite observar el tipo y la implementación de herramientas tecnológicas y emergentes en la lucha contra las drogas en el ciberespacio.

El análisis se centra en caracterizar brevemente el fenómeno del cibernarcotráfico y, posteriormente, en identificar y analizar algunas de las tecnologías que deben ser prioritarias en la implementación de estrategias policiales en el ciberespacio, con el fin de enfrentar la cibercriminalidad y, específicamente, el cibernarcotráfico.

El cibernarcotráfico utiliza tecnologías digitales y la web oscura para comercializar drogas ilícitas y blanquear capitales a nivel nacional e internacional. Para combatir este

fenómeno, es esencial emplear herramientas tecnológicas avanzadas en las actividades policiales. Las nuevas tecnologías de la información y la comunicación (TIC) ofrecen una respuesta más sofisticada y efectiva contra el negocio de las drogas ilícitas en el ciberespacio. A continuación, se exploran diversos escenarios con base en la realidad actual del fenómeno.

Cibernarcotráfico como modalidad delictiva en crecimiento

Según Osorio (2021), el FBI reportó en 2020 un récord de 791 790 denuncias por delitos cibernéticos en Norteamérica, los cuales causaron pérdidas superiores a los 4200 millones de dólares. En comparación con las cifras de 2019, las denuncias de víctimas de diferentes tipos de delitos cibernéticos aumentaron un 69 %. En consonancia con esto, la ONU y la Asociación Colombiana de Ingenieros (ACIS) advirtieron en 2021 sobre un aumento significativo de ciberdelitos en los últimos dos años, destacando un incremento del 600 % en correos electrónicos maliciosos. Esta problemática afecta a países con diferentes niveles de desarrollo de manera similar. Por ejemplo, cifras recientes del Centro Cibernético de la Policía Nacional revelan que los delitos informáticos en Colombia aumentaron en promedio un 59 % durante el periodo analizado (Peralta & Roa, 2021).

En suma, "las diferentes dinámicas criminales están migrando en diferente medida a la red (internet) o se están realizando online, instrumentalizando diferentes alternativas tecnológicas con fines delincuenciales" (Quevedo, 2017). El tráfico de drogas no es la excepción: "las transacciones, comunicaciones y coordinaciones criminales del narcotráfico en la actualidad suceden a través del ciberespacio, garantizando el anonimato, la impunidad y el crecimiento sostenido del fenómeno criminal" (Cárdenas & Lazo, 2014). En el caso de Colombia, la unidad investigativa mencionada ha detectado y seguido en una primera fase de investigación 200 identidades digitales dedicadas a la comercialización de drogas ilegales en la *clearweb* o internet superficial, a través de redes sociales como Facebook, Instagram y Twitter.

"Estas tendencias implican que las instituciones encargadas de la persecución criminal requieren adaptación, modernización y transformación en sus tácticas y técnicas de investigación criminal" (Summers & Rossmo, 2015). El problema identificado justifica la creación de unidades investigativas con focalización tecnológica para confrontar el cibernarcotráfico y otras fenomenologías criminales conexas, así como otros delitos facilitados por el ciberespacio como la explotación infantil, la extorsión o el contrabando. Estas unidades especializadas deben tener la capacidad de implementar herramientas y soluciones informáticas con base en las TIC, además del desarrollo de procedimientos investigativos de carácter cibernético a través del ciberespacio, con el fin de abordar el tráfico de drogas ilícitas de forma digital.

Estas capacidades requieren ser desarrolladas a nivel institucional por las entidades encargadas de confrontar, en diferentes dimensiones, el fenómeno criminal descrito. Este texto, al documentar parte del proceso en la lucha antidrogas colombiana, sugiere que "el desarrollo de las capacidades para enfrentar el tráfico de drogas ilegales a través del ciberespacio se realice bajo tres enfoques" (Lubeck, 2019): los procesos, las tecnologías y las personas. Estos enfoques deberían alinearse con la norma técnica ISO 2701 y el marco de referencia de Mitre (ATT & CK)[1].

Metodología

Este estudio parte de la premisa de que "validar un resultado, en su forma contemporánea, propende porque las técnicas se ajusten al planteamiento y no al contrario" (Hernández, 2018). En este contexto, la investigación se basó en evidencia empírica recolectada de manera etnográfica, en el marco del proyecto que da cuenta de la creación de la Unidad de Investigación en Cibernarcotráfico de la Policía Nacional de Colombia. En dicho proyecto, una serie de expertos interactuaron, agrupando las necesidades de desarrollo de capacidades en una matriz de recolección de datos (Tabla 1), a partir de la cual se construyó el contexto actual y se desarrollaron proyecciones de posibles escenarios frente a la problemática abordada.

Tabla 1. Matriz de recolección de posiciones entre expertos

	Desarrollo de capacidades	Generación de sinergia institucional	Interoperabilidad
Procesos	Técnicas, tácticas y procedimientos	Normas, protocolos, mesas de trabajo y gestión del conocimiento	Fusión de bases de datos
Tecnologías	Inteligencia de fuentes abiertas y señales Agente encubierto virtual	Tecnologías, hiperconvergentes y de código abierto Desarrollos propios y autosoportados Sensibilización, lenguajes comunes	Adquisición de sistemas compatibles Análisis forense digital Investigación forense digital
Personas	Entrenamiento, capacitación y referenciación		Documentar lecciones aprendidas

Fuente: Elaboración propia

1 *Adversarial Tactics, Techniques, and Common Knowledge.* El marco MITRE ATT & CK es una base de conocimientos y un modelo seleccionados para el comportamiento del adversario cibernético.

Luego de la recolección de la información, se elaboró un plano cartesiano en el que el eje Y se define como "adaptación" y el eje X como "determinación de influir". Estos ejes hacen referencia a la aptitud y el enfoque con los que se aborda el desarrollo de capacidades en la institución policial frente al fenómeno del cibernarcotráfico. Las diferentes zonas del plano cartesiano permiten, de manera intuitiva, posicionar los escenarios que se estructuran de acuerdo con las tendencias de cada una de las necesidades en capacidades por desarrollar, con miras a afectar el cibernarcotráfico, y que servirán como insumo para la elaboración de escenarios.

Procedimientos legales frente a este delito

En Colombia, los delitos informáticos motivaron la Ley 1273 de 2009, que adicionó diferentes artículos al Código Penal y reconoció un emergente bien jurídico tutelado, definido como "protección de la información y de los datos", con la intención de preservar a los sistemas que integran las TIC. Para investigar estos delitos se crearon tres procedimientos que se presentan a continuación.

- **Procedimiento para el tratamiento y análisis de la evidencia digital.** Establece los pasos necesarios para recolectar, tratar, analizar, identificar, preservar y presentar la evidencia digital con el fin de que sea legalmente aceptada.
- **Procedimiento para recolectar datos volátiles.** Consiste en recolectar en el menor tiempo posible y sin apagar el dispositivo la mayor cantidad de datos posible sin modificar, para no alterar la evidencia material probatoria (EMP) y la evidencia forense (EF).
- **Procedimiento para realizar imágenes forenses.** Consiste en obtener una copia física (bit a bit) de dispositivos de almacenamiento digital vinculados en un proceso de investigación para tener la réplica original del dispositivo a analizar.

Aparte de lo anterior, frente al fenómeno de la dinamización del SDI a través del ciberespacio se evidencian varios procedimientos y procesos que requieren desarrollo normativo para apropiarlos como técnicas y tácticas a favor de la lucha antidrogas:

- Agente virtual encubierto
- Acceso remoto a móviles, computadores y servicios computacionales en nube
- Descarga de código, instrucciones o desarrollos de *software* a dispositivos
- Escaneo, enumeración y explotación de vulnerabilidades de equipos comprometidos en el tráfico ilegal de drogas ilícitas
- Rastreo, desanonimato e investigación de criptoactivos

Estos son algunos de los procedimientos que requieren un marco normativo sólido para sustentar su aplicación y establecer protocolos claros para su implementación en

la actividad de policía judicial e inteligencia en la lucha antidrogas. Esto es esencial si se quiere garantizar que la recolección de evidencia digital e información privilegiada sea adecuada para respaldar operaciones policiales y facilitar la cooperación en investigaciones a través del ciberespacio (Atkins, 1998). Además, es fundamental que los hallazgos de estas actividades puedan incluirse como elementos materiales probatorios en un proceso judicial. Sin embargo, la implementación de estos procedimientos plantea desafíos en sistemas políticos democráticos, ya que podría generar controversias sobre su legitimidad y posible conflicto con las reglamentaciones existentes en materia de investigación criminal.

Siendo así, la confrontación en todos los niveles de los delitos asociados al SDI requiere con urgencia una actualización de varias de las figuras utilizadas en el sistema judicial, a la luz de los desafíos que representa el ciberespacio. Aspectos como el "agente encubierto online o virtual" (Molina, 2012), el "registro remoto sobre equipos informáticos" (Lainz, 2017), la "investigación del uso ilegal de criptoactivos y activos digitales" (Rodríguez & Lozano, 2023), el "rastreo de la dirección IP" (Cabello, 2017), y la "cadena de custodia con relación a las pruebas informáticas" (Marqués & Serra, 2014), tanto las obtenidas de manera directa como las obtenidas de forma remota mediante la navegación en internet, son aspectos fundamentales que deben cimentar las estrategias y el uso de tecnologías disruptivas en la lucha contra el narcotráfico en la actualidad.

Para ello, en Colombia se creó la Ley 1908 de 2018 "para fortalecer la investigación y judicialización del crimen organizado". En dicha ley, se formalizan las "Operaciones encubiertas en medios de comunicación virtual" con la adición del artículo 242b al Código Penal (Ley 906 de 2004). Así, la técnica especial de investigación de agente encubierto, según esta adición jurídica, podrá utilizarse de manera virtual al advertir la probable existencia de infracciones penales desarrolladas "por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual". Pese a este avance normativo, su protocolo es poco claro; es decir, en la actualidad no se aplica ni se desarrolla investigación criminal bajo esta figura en la lucha antidrogas.

Tecnologías disruptivas contra el narcotráfico

Estos desarrollos normativos deben entenderse como el soporte jurídico para operar tecnologías disruptivas, las cuales se entienden como la convergencia de "instrumentos, recursos técnicos o procedimientos" utilizados o desarrollados en determinado campo; en este caso, en la lucha contra las drogas ilegales y los delitos conexos al narcotráfico, especialmente los cometidos a través del ciberespacio. En esta línea, y con la sistematización de la experiencia en la confrontación inicial del cibernarcotráfico en el caso de estudio, algunas tecnologías emergen como alternativas a implementar en la persecución

penal del fenómeno a confrontar. Por razones metodológicas, se abordarán cuatro de ellas, sin que ello implique la exclusión de otras tecnologías que también se requieren integrar.

Agente encubierto virtual (AEV)

El agente encubierto virtual a implementar en el ciberespacio en contra del narcotráfico, autorizado bajo la norma antes citada, carece de claridad jurídica y procedimental en la actualidad para Colombia; al respecto, se asume que los investigadores de policía judicial autorizados por la Fiscalía General de la Nación (FGN) "son altamente calificados y capacitados y que prestan su consentimiento de manera libre y espontánea" (Zafra, 2010). Asimismo, se asume "que, ocultando su identidad o usando una identidad supuesta, se infiltran en el crimen organizado haciendo uso de las TIC, con el fin de recolectar información e identificar responsables de conductas criminales y orientar la investigación" (Artavia & Herrera, 2019). En este sentido, se requiere elaborar una propuesta de protocolización de la actividad investigativa a la luz del andamiaje jurídico colombiano.

La finalidad del AEV debe ser esclarecer la comisión de hechos punibles con "elementos materiales probatorios e información legalmente obtenida" a través de esta técnica, especialmente cuando no sea posible aportar pruebas por otros medios y cooperar con procesos internacionales (Atkins, 1998).

Para esto, se requiere un consentimiento formal de quien asume la tarea de ser AEV. De este modo, la policía judicial seleccionada para desarrollar la técnica AEV en operaciones contra el narcotráfico deberá explicitar su consentimiento de manera documentada, dejando clara "su voluntad libre y expresa de asumir la misión" como AEV y su conocimiento sobre los riesgos implicados en la investigación contra el narcotráfico.

Así mismo, partiendo del requerimiento fundamentado del fiscal del caso, un juez competente deberá autorizar la intervención del AEV mediante la formalidad aplicable en cada caso.

Las funciones del AEV son, entre otras, las siguientes:

- Desarrollar un entorno de trabajo ciberseguro para la operación (uso de VPN, máquinas virtuales, creación de una identidad digital y una fachada virtual, etc.).
- Infiltrarse en la organización o en sus actividades criminales investigadas.
- Acceder a información, elementos probatorios y evidencia física para la investigación.
- Identificar e individualizar elementos, bienes, lugares y personas.
- Presentar al fiscal los informes requeridos en los tiempos y formalidades establecidas.

- Llevar a cabo las labores necesarias para el desarrollo efectivo de la actividad investigativa sin incitar o provocar la comisión del hecho punible investigado o asumir su liderazgo.

En cuanto a los procedimientos, en la designación y desarrollo de la técnica del AEV se debe cumplir con algunos aspectos mínimos:

- Informe ejecutivo de policía judicial justificando la aplicación de la técnica de AEV.
- Evaluación de los intervinientes (fiscal e investigador) para avalar la técnica.
- Designación del agente y configuración de la identidad de trabajo.
- Autorización judicial, previa motivación del fiscal del caso.
- Una vez iniciada la actividad investigativa, presentación de avances investigativos del AEV ante la FGN.

Respecto a la responsabilidad del AEV, según la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), como cualquier agente encubierto:

> [Será] responsable, disciplinaria, administrativa, civil y penalmente por todos los actos que realice y recursos que maneje en el ejercicio de sus funciones, con evidente exceso o desproporcionalidad con relación a su misión. También serán responsables los funcionarios que intervienen en el procedimiento de autorización y gestión del AEV, en cuanto al manejo de la confidencialidad de la información y ejecución de la técnica. (UNODC, 2009)

La misión de un AEV y sus actividades investigativas podrían concluir por distintas razones (UNODC, 2009): por decisión y requerimiento del AEV; por orden del fiscal; por finalización de la investigación; por incapacidad sobreviniente, o por deceso del AEV.

El AEV deberá tener presente en el desarrollo de sus actividades algunas prohibiciones (Molina, 2012). Así, el AEV no podrá:

- Incitar la realización del ilícito.
- Extralimitarse en los hechos o desviarse del alcance de la orden con desproporcionalidad, intencionalidad o provecho propio.
- Comprometer su juicio al vincularse con la organización criminal o sus allegados más allá del cumplimiento de la misión de manera fraternal, afectiva o ideológica.
- Usufructuarse con los recursos entregados en el cumplimiento de su misión.
- Evitar excesos, desproporcionalidad y gastos innecesarios con los recursos dispuestos en el desarrollo de la misión.

Así, la técnica del AEV oscila entre la interacción directa del investigador a través del ciberespacio, el uso de identidades digitales creadas para tal fin ("avatares") o el modo

sigilo, y el uso de *software* en los dispositivos digitales que permitan acceder a la información privilegiada del objetivo de la misión. Estos elementos, en la actualidad, cuentan con una caracterización, protocolización y desarrollo normativo incipiente para su aplicación.

Open Source Intelligence (OSINT) o ciberpatrullaje

Los desarrollos y avances actuales de nuevas tecnologías facilitan y amplían el alcance del servicio de policía, para hacerlo más efectivo, innovador y de impacto frente a las necesidades sociales y gubernamentales. Estos avances requieren implementación urgente. En este sentido, se han logrado progresos y se han desarrollado conceptos y tendencias que se han implementado satisfactoriamente en la lucha contra cada nodo del SDI.

Una de las tendencias que ha ganado relevancia mundial es el Open Source Intelligence (OSINT) o *ciberpatrullaje*. Este término se refiere a la recolección, registro, procesamiento, análisis, correlación, evaluación y difusión de información obtenida de fuentes abiertas. Estas fuentes incluyen personas, entidades o temáticas específicas utilizando información de acceso público disponible en el vasto conglomerado de internet. Las redes sociales, los motores de búsqueda, los metadatos, los periódicos, las fotografías, diversos foros, enciclopedias y librerías virtuales, la información del sistema de nombres de dominio (DNS), y las consultas en bases de datos públicas son algunas de las principales fuentes de información en esta metodología (Cascales et al., 2011).

La aplicación y desarrollo del OSINT se considera un tipo de inteligencia que implica la recolección, análisis y procesamiento de información pública. Sin embargo, este concepto ha sido malinterpretado con frecuencia en el contexto cultural colombiano. Así, cuando se habla de actividades de inteligencia, se tiende a pensar erróneamente en acciones que se realizan fuera del contexto público y jurídico, involucrando tecnologías o sistemas de información reservada. En realidad, el término *inteligencia* se refiere a la capacidad mental para aprender, entender, razonar, tomar decisiones y formar ideas determinadas (Sevilla, 2019). Por tanto, en el contexto de la lucha antidrogas a través del ciberespacio, el OSINT se entiende como la recolección, tratamiento, evaluación y procesamiento de datos adquiridos de fuentes abiertas de información, sin vulnerar los derechos humanos, con el fin de tomar decisiones a nivel operativo, estratégico y prospectivo en la lucha institucional contra el narcotráfico.

Por ello, la búsqueda de información mediante actividades de ciberpatrullaje obedece a parámetros claros, que consisten en encontrar y catalogar las fuentes de información, adquirir datos relevantes, procesarlos, analizar y establecer puntos de interés, y finalmente elaborar un producto de inteligencia o un informe de actividades de verificación

digital. Este informe debe presentar las conclusiones de manera sencilla mediante texto, esquemas, gráficas, dibujos, entre otros recursos.

Ante esto, el perfil del investigador y analista emerge como un pilar fundamental del OSINT. No es necesario un perfil académico concreto; una persona con amplia experiencia en el ámbito técnico, comprensión básica de la operacionalización de las TIC y una cultura general, puede formarse efectivamente en esta práctica.

Así, el OSINT, operacionalizado a través de Google Dorks, herramientas y *software* de OSINT, operadores booleanos, inteligencia artificial, entre otras alternativas, es una metodología aplicable a la investigación criminal y a la inteligencia. Esta metodología abarca información pública, de dominio común y accesible a cualquier persona, por lo que no depende de una orden judicial para su realización. Además de ser una fuente óptima de recursos e información, la aptitud y capacidad del talento humano disponible en las instituciones del Estado, junto con su capacitación y actualización, permiten desarrollar ampliamente esta tecnología, proyectándose como una herramienta clave en la lucha antidrogas.

Inteligencia artificial de correlación y *machine learning*

En la actualidad, existen diversas soluciones y herramientas diseñadas para analizar y correlacionar diferentes bases de datos e información obtenida en investigaciones criminales, peritajes y fuentes abiertas. Todos los días se generan cantidades considerables de datos no estructurados, estructurados y abiertos al público en la web. Esto representa una oportunidad para los investigadores, quienes pueden aprovechar los millones de datos disponibles en la red e integrarlos con las bases de datos internas, lo que permite obtener percepciones procesables sobre personas, grupos y temas, y luego focalizar nuevas búsquedas en la red.

Dichas herramientas son de vital importancia para analizar grandes volúmenes de datos no estructurados para proporcionar percepciones informadas e integrales a los analistas e investigadores sobre personas, grupos y temas, incluidos sus círculos sociales, relaciones clave y ocultas, así como influencias y sentimientos predominantes. Gracias a esto, los analistas pueden tomar decisiones para reaccionar rápidamente y de manera eficiente a situaciones en desarrollo o, de manera proactiva, prevenir la escalada de un suceso.

El resultado de estos análisis puede acelerar una investigación, gracias a que suelen identificar relaciones y conexiones previamente desconocidas entre dos personas o identidades distintas. Se obtiene así una comprensión integral y estratificada de la esfera social de la persona y sus preferencias, lo que se puede utilizar para tomar decisiones o adoptar medidas adecuadas.

En cuanto al análisis de grupos, esta tecnología permite comprender el comportamiento colectivo, determinar su dinámica interna, identificar a los miembros principales y reconocer a otros integrantes relevantes para la red. Durante este proceso, se pueden detectar las interconexiones y patrones relacionales, lo que facilita la identificación de subgrupos dentro de la estructura mayor. En muchos casos, esta tecnología ayuda a definir los grupos con mayor precisión o, alternativamente, analizar de forma colectiva a los grupos o canales definidos dentro de una plataforma de redes sociales.

En este sentido, mediante la integración de algoritmos y procesos autónomos de aprendizaje, se automatizan muchos eventos y acciones en la red. Por ello, el *machine learning* se proyecta como una solución a los grandes volúmenes de información y a la necesidad de efectividad en el análisis de información digital, gracias a la identificación de patrones recurrentes, en grandes conjuntos de datos.

Además, actualmente se pueden realizar análisis avanzados sobre imágenes, transformándolas en inteligencia visual. Esta técnica permite descubrir nuevas pistas y realizar un análisis profundo mediante tecnología avanzada de decodificación visual. Las percepciones obtenidas a través de estos análisis facilitan identificar entidades clave, mapear relaciones y evaluar la fuerza de estas. También permite seleccionar personas para un análisis grupal, generar alertas ante patrones específicos y confrontar e identificar rostros, objetos e interacciones.

Análisis de registro de detalles de llamadas (CDR)

El análisis de los registros de detalles de llamadas (CDR, por sus siglas en inglés) como técnica de investigación se implementó en investigación criminal poco después de comprender el funcionamiento de la infraestructura de comunicación móvil o celular y su potencial como tecnología para la persecución criminal. Se basa en la premisa de que "la información digital deja rastros en los medios informáticos" (Martínez, 2009), algo particularmente relevante en las redes de telefonía móvil, donde los teléfonos móviles o celulares se conectan a la infraestructura.

Actualmente, los teléfonos inteligentes generan un registro cada vez que se conectan a una estación base (BTS). Estas acciones quedan reflejadas en los CDR, almacenados en las bases de datos de los proveedores de telefonía celular. Para comprender esta tecnología, es necesario definir algunos conceptos clave, como la función de las BTS en dispositivos de telefonía celular, las caras o vectores de una antena celular y los CDR.

En relación con el primer aspecto, las redes que conectan celulares, según Vaca (2015), "dividen la geografía o área de alcance en células o celdas que quedan cubiertas a nivel radioeléctrico por Estaciones Base o BTS (Base Transceiver Station)", de la siguiente forma: 1) mediante "un canal de *broadcast* los terminales de abonado miden el grado de

cobertura disponible y tratar de cambiar a otra BTS si es preciso (*handover*)"[2]; 2) a través de canales de tráfico permite la transmisión telefónica entre dispositivos; y 3) otorgan conexiones "alámbricas o inalámbricas" hacia los proveedores del servicio y su arquitectura tecnológica dispuesta para mantener la comunicación.

Las BTS facilitan las interacciones entre un número específico de abonados (líneas o números celulares) dentro de su área de influencia geográfica, definida por su cobertura radioeléctrica. Esto implica que cada BTS trabaja con un número limitado de canales de tráfico, los cuales permiten las llamadas telefónicas. En situaciones de alta demanda, como ocurre cuando hay saturación de tráfico en estos canales, los abonados adicionales son excluidos temporalmente, impidiéndoles efectuar llamadas hasta que se libere un canal.

En áreas rurales, donde el tráfico de usuarios es generalmente menor, las BTS suelen emitir ondas radioeléctricas de manera multidireccional, cubriendo un amplio espacio con una sola célula. En contraste, en áreas urbanas, debido a la mayor concentración de población, se utiliza una división por sectores. Esto significa que la cobertura se divide en tres zonas o sectores, cada uno de los cuales funciona como una célula independiente, lo que aporta mayor eficiencia en la gestión del tráfico de usuarios.

Respecto a las caras o vectores de una antena, estos se refieren a las direcciones desde las cuales una antena de telefonía móvil emite o recibe ondas de radiofrecuencia. La numeración de estas caras o vectores comienza con la cara uno, que siempre está situada al norte. A continuación, la cara o vector dos se orienta hacia el este, y la cara tres hacia el oeste, siguiendo el sentido de las manecillas del reloj. Este esquema continúa aumentando según la distancia y dirección de la señal de radiofrecuencia. Cada sector o vector de una antena está distribuido en un rango que va del 1 al 9, también en el sentido de las manecillas del reloj. Por lo general, cada sector o vector cubre un ángulo de 120°, aunque esta cobertura puede variar dependiendo de la necesidad del servicio prestado por la empresa de telefonía celular (Vílchez & García, 2014).

En cuanto a los CDR, estos quedan registrados en las bases de datos de los proveedores de telefonía celular. Una BTS, conformada por celdas celulares, permite que las empresas de telefonía a nivel mundial tomen CDR de las llamadas salientes o entrantes de una línea celular. Esta información incluye diferentes tipos de datos, como voz, mensajes de texto entrantes y salientes, y el uso de datos o internet. Además, se registran el tiempo, la duración, el origen y destino de la comunicación, nombre, número de codificación, coordenadas geográficas, direcciones y el nombre del departamento o

2 De acuerdo con Brunner et al. (2006): "Se denomina handover (también handoff) al sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente. Este mecanismo garantiza la realización del servicio".

municipio donde se encuentra la celda o antena de telefonía celular. Esta información de conexión queda registrada en las celdas o antenas donde se produjo la comunicación o en los archivos de las empresas operadoras de telefonía celular, las cuales manejan esta información según sus políticas internas. Los CDR tienen diversos usos en el control de la red, balances y facturación.

Para obtener los CDR, es necesario ubicarse en la zona de cobertura de la antena o celda donde se produce el evento del que se desea obtener la información. A continuación, se procede a utilizar aplicaciones (*apps*) disponibles para el sistema operativo del equipo celular en uso. A través de esto, se puede identificar qué antena o celda tiene cobertura en el equipo celular que se encuentra en un sector o lugar determinado. Se puede obtener información sobre la extensión de la cobertura de los proveedores de la red, los sitios de torre celular e incluso, en ocasiones, las coordenadas de estas antenas o celdas, así como los decibeles de aproximación de la antena al equipo celular, mediante el identificador del área de localización (LAI), utilizado en redes móviles GSM. El LAI es un código único internacionalmente que se utiliza para la actualización de la posición de suscriptores móviles (Vílchez & García, 2014). Está integrado por una triada de códigos decimales. Este código varía según el continente, país o región del mundo donde esté ubicado el equipo celular que posee una *simcard* o chip de línea celular (Sevilla, 2010).

Sin embargo, estas aplicaciones, al ser gratuitas, se utilizan como demos y no recopilan o recolectan toda la información necesaria para un análisis completo. Para obtener información más precisa y que reúna todos los campos necesarios, se utilizan herramientas desarrolladas específicamente para tal fin, como G-NetTrack Pro, G-NetReport Pro, G-NetView Pro y G-NetLooK Pro. Estas aplicaciones funcionan en conjunto para recolectar información más precisa, lo que las convierte en herramientas útiles para aplicaciones forenses en un juicio, ya que reúnen las características necesarias para dicho propósito.

En este sentido, cabe destacar que la dimensión creada por la migración de la cadena criminal del narcotráfico a los entornos digitales, conocida como cibernarcotráfico, representa una transformación en los modelos tradicionales de investigación, procesos y procedimientos en informática forense, investigación forense digital, y para la recolección, análisis y procesamiento de la evidencia digital (Iglesias, 2015).

La metodología de investigación del cibernarcotráfico requiere una capacidad relacional avanzada del talento humano involucrado, en la que se consideren el tiempo y la concatenación de hechos para esclarecer circunstancias de tiempo, modo y lugar. Este talento humano debe poseer competencias altamente especializadas en investigación forense digital, un campo que abarca un conjunto de conocimientos globales. Estos conocimientos integran técnicas, tácticas y procedimientos, junto con actividades

de laboratorio, en un conjunto de habilidades interdependientes orientadas al éxito de una investigación en su aplicación táctica.

Investigación de criptoactivos

En términos generales, las criptomonedas pueden entenderse como parte de los activos virtuales (AV), que se han proyectado como una innovación y una herramienta de eficiencia financiera en los últimos años. Sin embargo, sus características distintivas y su uso indebido "dan oportunidades para el lavado de activos y la financiación de actividades criminales" (GAFI, 2021). En este contexto, el terrorismo y el narcotráfico son dos de las actividades criminales que están incorporando estas tecnologías en sus operaciones ilícitas (Gutiérrez, 2022). Al respecto, la Junta Internacional de Fiscalización de Estupefacientes (JIFE) de la ONU informó en 2022 que "Las criptomonedas son utilizadas cada vez más por carteles mexicanos y colombianos para blanquear millonarias sumas del narcotráfico y otras actividades delictivas" (*El Colombiano*, 11 de marzo de 2022).

Esto plantea un desafío para las agencias encargadas de hacer cumplir las disposiciones legales, especialmente en la investigación de este tipo de transacciones de índole criminal. Desde años atrás, diferentes instituciones han advertido sobre el aprovechamiento criminal del *blockchain*. Por ejemplo, la OCDE (2019), a través del manual de *Lavado de activos y financiación del terrorismo. Manual para inspectores y auditores fiscales*, ha impulsado prácticas investigativas para países emergentes, principalmente ante el uso evidente de criptomonedas para el lavado de activos. En la misma dirección, Interpol (2019) ha advertido sobre el uso indebido de criptomonedas en la red oscura. Finalmente, diferentes documentos académicos han llegado a conclusiones en la misma línea (Pinco & Rodríguez, 2021; Moreno, 2020; Navarro, 2019).

La investigación de estos delitos debe tratar de recolectar, preservar, manejar y documentar diversas evidencias digitales, entre ellas:

- Identificar las direcciones de criptomonedas, billeteras, etc.
- Detectar posibilidades de descifrado y acceso a claves privadas de los activos.
- Establecer direcciones IP.
- Identificar nombres de usuario y alias detrás de los criptoactivos.
- Identificar direcciones electrónicas de acceso a los criptoactivos.
- Caracterizar e identificar dominios de los mercados de la red oscura.
- Monitorear los foros de la red oscura donde se transan criptoactivos.
- Establecer el historial de datos recopilados de los hallazgos.
- Analizar transacciones en su origen y destino.
- Identificar puntos de monetización e intercambiadores.

- Mapear la operación ilegal y presentar gráficos intuitivos para la comprensión judicial.

Al finalizar estas investigaciones, se debe informar de manera detallada a las autoridades judiciales sobre el proceso de identificación de los atributos de las direcciones y billeteras criptográficas implicadas, las transacciones y atribuciones relevantes, así como la trayectoria de las transacciones. Este informe debe incluir un análisis detallado del caso que contemple la asociación con direcciones criminales identificadas, ubicaciones geográficas, cantidades de dinero transado y la tipología criminal usada.

La mayoría de estas investigaciones recurren al uso de *software* y complementos virtuales de investigación digital, como la apertura de billeteras con recursos criptos amparadas judicialmente para realizar interacciones; el uso de figuras de agente encubierto con alcances virtuales; correos y medios electrónicos de pago gestionados desde terminales móviles, y, finalmente, un análisis realizado por un perito contable forense.

Sin embargo, algunos de los temas de relevancia en estas investigaciones digitales están asociados a desarrollos normativos, como las regulaciones para reportar transacciones de criptoactivos a las unidades de inteligencia financiera, así como las regulaciones para la incautación e imposición de medidas cautelares sobre criptoactivos. Además, se deben considerar los aspectos procedimentales relacionados con el manejo, transferencia, custodia y administración de criptoactivos, así como su disposición final y las formas de monetización a favor del Estado.

Personal contra el cibernarcotráfico

En el ciberespacio se desarrollan múltiples actividades criminales como el cibernarcotráfico. Su abordaje y confrontación implican que las agencias policiales desarrollen las capacidades tecnológicas necesarias, y que las puedan utilizar en "un marco jurídico acorde a este nuevo entorno, en el que el anonimato de los autores y la deslocalización de conductas son las características más relevantes" (Écija, 2017). Pero, además, se requiere contar con el personal adecuado para ello. En Norteamérica, se sugiere el desarrollo del rol, las funciones y el marco de actuación de una "ciberpolicía", como lo explica Carlos Sánchez Almeida (2000): se trataría de "un cuerpo de intervención rápida que pudiese actuar en cualquier país del mundo sin autorización judicial, a fin de perseguir el cibercrimen allí donde ocurra".

Aunque el perfil no esté claramente definido y actualmente no existan programas de incorporación, capacitación y fortalecimiento de competencias para la nueva era de policías del ciberespacio en algunos países, es necesario iniciar programas de fortalecimiento de capacidades institucionales con ese objetivo.

Más allá de definir el perfil a desarrollar, la experiencia en el desarrollo de estas capacidades refleja el seguimiento de recomendaciones de expertos, que implican decisiones como reclutar policías con experiencia en investigaciones de narcóticos y delitos informáticos, así como policías con formación en áreas afines como "ingeniería de sistemas, seguridad de la información, ciberseguridad, desarrollo de *software*, ingeniería de comunicaciones y electrónica, entre otras" (Sánchez, 2000).

Posterior a ello, el personal seleccionado deberá integrarse a un proceso de capacitación en evidencia digital, informática forense, ciberinteligencia, investigación criminal, investigación en narcóticos y entrenamiento en ciberseguridad ofensiva. El objetivo es formar investigadores integrales que puedan intervenir en la recolección, análisis, peritaje, judicialización y en operaciones contra el cibernarcotráfico.

Todavía es prematuro definir el éxito de este tipo de unidades especializadas frente al fenómeno que enfrentan; sin embargo, iniciar rápidamente su creación permitirá evaluar aciertos y desaciertos, lo que facilitará efectuar los ajustes necesarios para formar un talento humano adecuado y con las capacidades requeridas en la investigación del cibernarcotráfico. El éxito de este proceso dependerá en gran medida de su continuidad y de una adecuada planeación presente para el desarrollo de estas capacidades en el futuro cercano.

Resultados

Un análisis exhaustivo del cibernarcotráfico revela un incremento considerable en las denuncias de delitos en el ciberespacio, con un aumento del 69 % en las denuncias al FBI y un 59 % en denuncias en Colombia entre los años 2019 y 2020. Esto refleja la creciente amenaza que representan las actividades delictivas en el entorno digital, especialmente las relacionadas con drogas ilícitas y el lavado de dinero. Se logra establecer que las estrategias tecnológicas emergentes como la inteligencia en las fuentes abiertas, la inteligencia artificial y las investigaciones en criptoactivos productos del narcotráfico son fundamentales para una respuesta efectiva contra estos crímenes.

Análisis

La implementación de legislaciones como la Ley 1273 de 2009 y la Ley 1908 de 2018 en Colombia son avances frente a la imperiosa necesidad de un marco normativo sólido para regular y combatir el cibernarcotráfico, puesto que estas leyes facilitan operaciones encubiertas en el ciberespacio. No obstante, el desarrollo del agente encubierto virtual está aún en una fase incipiente, ya que requiere consentimiento documentado y autorización judicial para su ejecución, lo que destaca la complejidad y el rigor necesario en las operaciones de inteligencia judicial.

Es necesario desarrollar capacidades institucionales que integren herramientas tecnológicas avanzadas con un marco jurídico sólido. La adaptación de las instituciones encargadas de combatir el crimen es perentoria para abordar las dinámicas cambiantes del negocio de las drogas ilícitas, especialmente frente al aumento en el uso de criptomonedas y la evolución de la web oscura. Por otro lado, hay que recalcar la necesidad de capacitar a los agentes policiales en la realización de procedimientos en el ciberespacio, asegurando que estos operen dentro de comportamientos éticos y legales que respeten los derechos humanos. Asimismo, se reitera la importancia de la cooperación internacional y la estandarización de los protocolos para abordar de manera coordinada y eficiente la amenaza global de la venta y consumo de drogas ilícitas.

Exploración de escenarios

La exploración de escenarios se basa en la deseabilidad y la plausibilidad como forma de construcción de visiones del futuro idealizado, lo que impulsa los esfuerzos para alcanzar los escenarios posibles, sean estos probables o realidades materializadas. Este proceso clarifica cómo una institución debe prepararse para desarrollar capacidades, teniendo como guía el horizonte deseable (Tapia, 2019). Así, tomando como variables del escenario la capacidad de adaptación y la voluntad de influir, se proyectan dos escenarios como probables (Figura 1).

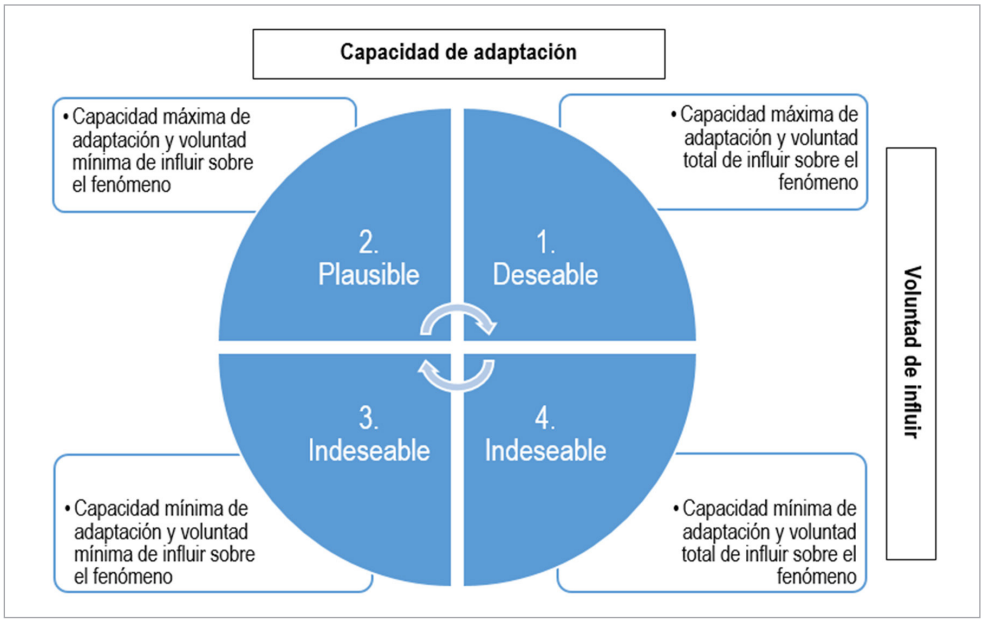


Figura 1. Matriz para la elaboración de escenarios.

Fuente: Elaboración propia

Escenario 1. Retos frente a la migración de la lucha antidrogas al ciberespacio

Dado el actual interés policial para afrontar el incremento del problema de las drogas ilícitas y sus delitos conexos en el ciberespacio y las capacidades de adaptación de los cuerpos de policía, se proyecta que en un futuro cercano se contará con técnicas, tácticas y procedimientos en ciberinteligencia, informática forense, ciberseguridad ofensiva e investigación criminal a través del ciberespacio. Estas estarán soportadas en normas, protocolos y acuerdos interinstitucionales, utilizando tecnologías disruptivas como el AEV, el OSINT o ciberpatrullaje, la inteligencia artificial, el rastreo y desanonimización de criptoactivos. Todo esto estará sustentado y desarrollado por profesionales de policía con un perfil técnico idóneo, capacitación y entrenamiento para afrontar las tendencias criminales en el ciberespacio.

Escenario 2. Transformación de cómo afrontar las drogas ilícitas en un entorno digital

Ante tomadores de decisión que no deseen afrontar el desarrollo de capacidades para abordar eficazmente el problema del cibernarcotráfico, y considerando las capacidades de adaptación de las instituciones de policía, es probable que en un futuro cercano se postergue el desarrollo de las técnicas, tácticas y procedimientos mencionados. Este retraso podría ser crítico, ya que dichas capacidades, soportadas en normas, protocolos y acuerdos interinstitucionales, utilizando las tecnologías disruptivas abordadas, son esenciales para la lucha contra el cibernarcotráfico y sus delitos conexos.

La falta de desarrollo en este campo generaría un vacío en las capacidades de los ciberpolicías, quienes necesitan un perfil técnico idóneo, capacitación y entrenamiento para enfrentar esta problemática. Sin estas capacidades, es probable que en los próximos años no se cuente con las herramientas necesarias para abordar el fenómeno criminal en el ciberespacio, lo que propiciaría un crecimiento exponencial de este.

Escenarios 3 y 4

Estos escenarios, aunque no desarrollados, serían catastróficos, dado que podría darse un incremento exponencial del fenómeno ante la limitación institucional para desarrollar capacidades y adaptarse a este cambio disruptivo en la criminalidad. La migración y adaptación tecnológica del SDI, hoy en día instrumentalizando el ciberespacio y las TIC, podría quedar desatendida. Aunque históricamente las instituciones de la lucha antidrogas consideran este escenario poco probable, existe el riesgo de que se traslade la responsabilidad de su abordaje a otras unidades de policía que requerirán desarrollar estas capacidades en el futuro mediano.

Conclusiones

Luego de realizar el análisis y proyectar los posibles escenarios, se llega a las siguientes conclusiones:

- La tendencia actual de la migración de los mercados criminales tradicionales a internet mediante la instrumentalización de nuevas tecnologías que facilitan la comisión de ciberdelitos, como el tráfico ilegal de drogas ilícitas, representa un reto que exige que todos los profesionales involucrados en la investigación del cibernarcotráfico se conviertan en dinamizadores de la cultura de la ciberseguridad, autodidactas en la formación en investigación digital forense, y expertos en redes y entornos virtuales, así como en seguridad de la información.
- La ciberseguridad es un ámbito muy desatendido aún, incluso en los campos de desarrollo y producción de las fuerzas de seguridad, las organizaciones y los entornos industriales de comunicación. A nivel regional y local, también se tiene un atraso particular en materia de preparación e investigación de ciberdelitos.
- El aumento del fenómeno de la cibercriminalidad, impulsado por la migración de los modelos tradicionales y las cadenas criminales al ciberespacio, provocará un cambio inevitable en la manera en que los países gestionan su información y en cómo actúan las fuerzas de la ley ante esta amenaza. Dicho cambio será una oportunidad positiva para los profesionales en TIC que estén preparados para asumir estos nuevos retos.
- El crecimiento exponencial de los fenómenos criminales en el ciberespacio exige que las instituciones encargadas de confrontarlos planteen proyectos para el desarrollo de capacidades en dicha materia en un futuro cercano.
- El desarrollo de estas capacidades debe tener en cuenta tres ejes: los procesos, las tecnologías y las personas.

Agradecimientos

Los autores desean agradecer a la Universidad de los Andes y a la Policía Nacional en sus direcciones de Educación Policial y de Antinarcóticos, instituciones que, a través de sus aportes o sus funcionarios, han permitido desarrollar el proyecto de "Cibernarcotráfico", del cual surge este artículo.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. Este artículo es fruto de la investigación titulada "Nuevos desafíos del cibernarcotráfico al sistema de las drogas ilícitas (SDI) desarrollada por la Escuela Antidrogas "Mayor Wilson Quintero Martínez" (ESAND).

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Autores

Diego Rodríguez Samora. Doctor en ciencias políticas con énfasis en relaciones internacionales, Universidad de los Andes, Bogotá. Magíster en ciencia política y en ciberseguridad e informática forense. Administrador de empresas, administrador policial y profesional en criminalística, con especialización en investigación criminal. "Primer Líder Grupo de Investigacion ESAND".

https://orcid.org/0000-0002-8456-5871
Contacto: stetid.rodriguez@correo.policia.gov.co

Luis Manuel Lozano Ramos. Suboficial de la Policía Nacional de Colombia. Magíster en psicología de la salud; magíster en psicología forense en evaluación del daño; especialista en pedagogía universitaria; psicólogo y filósofo. Experiencia en la lucha contra las drogas ilícitas. Docente en ética, derechos humanos, pedagogía, andragogía y habilidades sociales. "Segundo Líder Grupo de Investigacion ESAND".

https://orcid.org/0000-0001-5125-8894

Contacto: manuel.lozano1075@correo.policia.gov.co

Martín Leonardo Bonilla Duitama. Tecnólogo en telemática; estudiante de ingeniería electrónica, Universidad Nacional Abierta y a Distancia (UNAD). Docente de electrónica e informática forense, análisis de *malware* y ciberseguridad de la Policía Nacional de Colombia.

https://orcid.org/0000-0003-3546-6268
Contacto: martin.bonilla2736@correo.policia.gov.co

Nadia Peralta Romero. Abogada y fiscal seccional. Magíster en derecho penal. Especialista en derecho penal, Universidad Rosario, Bogotá; especialista en negociacion, conciliacion y arbitraje MASC; especialista en manejo de escena del crimen, Miami Dade College. Egresada del William J. Perry Center for Hemispheric Defense Studies. Docente y conferencista.

https://orcid.org/0009-0002-9298-4969 - Contacto: nadia.peralta@fiscalia.gov.co

Referencias

Artavia Artavia, Y., & Herrera Pérez, M. (2019). *El agente encubierto en contra de la criminalidad organizada y frente a las garantías del proceso penal costarricense (en especial el derecho de abstenerse a declarar y la inviolabilidad del domicilio)* [tesis]. San José de Costa Rica.

Atkins, T. B. (1998). La cooperación internacional policial en el ciberespacio. *Informática y Derecho: Revista Iberoamericana de Derecho Informático, 27*, 277-290.

Brunner, C., Garavaglia, A., Mittal, M., Narang, M., & Bautista, J. V. (2006, septiembre). Inter-system handover parameter optimization. En *IEEE Vehicular Technology Conference* (pp. 1-6). IEEE.

Cabello Gil, L. M. (2017). Geolocalización a través de direcciones IP. *Revista de Derecho UNED, 20*, 283-301.

Cárdenas, R., & Lazo, L. (2014). *Delitos informáticos y el rol de la división de investigación de delitos de alta tecnología, Lima 2013*. https://tinyurl.com/235a2vls

Cascales Martínez, A., Real García, J., & Marcos Benito, B. (2011). Redes sociales en internet. *Edutec. Revista Electrónica de Tecnología Educativa, 38*, a180. https://tinyurl.com/27zjfgfa

Castro Sarmiento, R. (2014). *Análisis prospectivo del Grupo de Investigación Criminal de la Dirección de Antinarcóticos de la Policía Nacional de Colombia* [tesis, Universidad Militar Nueva Granada, Bogotá]. https://tinyurl.com/2bnt5zfv

Écija, Á. (2017). Ciberespacio, dark web y ciberpolicía. *Diario La Ley, 8940*. https://tinyurl.com/22bdjc56

El Colombiano. (2022, 11 de marzo). Narcotraficantes colombianos usan criptomonedas para blanquear ganancias: ONU. https://tinyurl.com/2y7s59oq

GAFI. (2021). *Activos virtuales "Señales de alerta de LD/FT"* [informe]. https://tinyurl.com/2bt9yb34

Gaviria Uribe, A., & Mejía Londoño, D. (2011). *Políticas antidroga en Colombia: éxitos, fracasos y extravíos*. Universidad de los Andes.

Gutiérrez, F. (2022, 10 de abril). Caso Zaragoza, el referente para la UIF en materia de criptomonedas y lavado de dinero. *El Economista*. https://tinyurl.com/24xfhmph

Iglesias, L. (2015). Herramientas open source para informática forense [tesis doctoral, Facultad de Ciencias Económicas, Universidad de Buenos Aires].

Interpol. (2019). *La red oscura y las criptomonedas*.

Lainz, J. L. R. (2017). Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción. *Diario La Ley, 8896*, 2.

López Mendoza, J. M. (2016). La nueva política frente a las drogas tras el gobierno Santos: del fracaso histórico al cambio de política exterior.

Marqués Arpa, T., & Serra Ruiz, J. (2014). Cadena de custodia en el análisis forense: Implementación de un marco de gestión de la evidencia digital. *Proceedings of the RECSI 2014* (Universitat Oberta de Catalunya, Alicante, España). https://rua.ua.es/dspace/handle/10045/40423

Martínez, J. J. C. (2009). *Computación forense: Descubriendo los rastros informáticos*. Alfaomega.

Molina Pérez, M. T. (2012). Técnicas especiales de investigación del delito: el agente provocador, el agente infiltrado y figuras afines (y II). *Anuario Jurídico y Económico Escurialense, 42*, 153-174.

Moreno García, A. (2020). *Protocolo de actuación ministerial: investigación del delito de defraudación fiscal mediante el empleo de criptomonedas* [tesis, Infotec]. https://tinyurl.com/2982mpzg

Navarro, F. (2019). Criptomonedas (en especial, bitcóin) y blanqueo de dinero. *Revista Electrónica de Ciencia Penal y Criminología, 21*(14). http://criminet.ugr.es/recpc/21/recpc21-14.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2009). *Manual de técnicas especiales de investigación agente encubierto y entrega vigilada*. https://tinyurl.com/3xy6jazm

Organización para la Cooperación y el Desarrollo Económico (OCDE). (2019). *Lavado de activos y financiación del terrorismo: Manual para inspectores y auditores fiscales*. https://doi.org/10.1787/6141c153-es

Peralta M., & Roa, E. (2021). *El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia* [trabajo de grado, Universidad de Córdoba, Montería]. https://tinyurl.com/29twpjzw

Pinco, F., & Rodríguez, R. (2021). El delito de lavado de activos y la utilización o uso de criptomonedas [tesis, Maestría en Derecho, Universidad Continental, Huancayo, Perú]. https://tinyurl.com/4fp7ppu3

Quevedo, J. (2017). *Investigación y prueba del ciberdelito*. Universitat de Barcelona. https://tinyurl.com/yrhm6nbp

Rodríguez Samora, D., & Lozano Ramos, L. M. (2023). Prospectiva de las redes sociales, cibercrimen y criptoactivos como herramientas criminales del narcotráfico. *Estudios en Seguridad y Defensa, 18*(36), 163-180. https://doi.org/10.25062/1900-8325.348

Rodríguez Samora, D., Pulido Blasi, C., Peralta Romero, N., & Díaz Velásquez, C. (2020). Nuevas miradas al rol de las mujeres en el Sistema de Drogas Ilícitas: enfoque de género y participación de mujeres policías. *Estudios en Seguridad y Defensa, 15*(30), 353-371. https://doi.org/10.25062/1900-8325.287

Sánchez Almeida, C. (2000). España: Intimidad: Un derecho en crisis. La erosión de la privacidad. *Revista Electrónica de Derecho Informático, 24*.

Sevilla Jaimes, W. (2019). *Pensamiento creativo*.

Sevilla, E. S. U. (2010). *Diseño y parametrización de una estación de telefonía móvil 2G/3G*. https://tinyurl.com/2buy4ags

Summers, L., & Rossmo, K. (2015). Aplicaciones prácticas de la teoría de las actividades rutinarias a la investigación criminal. En F. Miró, J. Agustina, & L. Summers (Eds.), *Crimen, oportunidad y vida diaria* (pp. 171-186). Dykinson.

Tapia Uribe, M. (2019). Historia y prospectiva de la responsabilidad de la seguridad pública en los municipios. En *500 años del municipio en México: Perspectivas multidisciplinarias*. Universidad de Guanajuato; Instituto de Investigaciones Jurídicas UNAM. https://tinyurl.com/28gwmg9t

Vaca Parra, J. L. (2015). *Plan de negocio para la implementación de redes heterogéneas (HETNET) en la ciudad de Quito para proveedores de equipos de telecomunicaciones*.

Vílchez, N. B., & García Sánchez, I. A. (2014). *Diseño de una estación base para su integración en una red celular basadas en tecnologías GSM/UMTS* [tesis doctoral, Universidad Nacional de Ingeniería, Nicaragua]. http://ribuni.uni.edu.ni/id/eprint/1148

Zafra, R. (2010). *El policía infiltrado: Los presupuestos jurídicos en el proceso penal español*. Tirant Lo Blanch. https://tinyurl.com/mwzmk762