Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2025,
Volumen 9, Número 3.

https://doi.org/10.37811/cl_rcm.v9i1

IMPORTANCIA DE LA CARACTERIZACIÓN DEL CIBERCRIMINAL. UN ESTUDIO DE CASO EN EL DELITO DE HURTO A TRAVÉS DE MEDIOS INFORMÁTICOS EN LA CIUDAD DE BOGOTÁ D.C.

IMPORTANCE OF THE CHARACTERIZATION OF THE CYBERCRIMINAL. A CASE STUDY IN THE CRIME OF THEFT THROUGH COMPUTER MEANS IN THE CITY OF BOGOTÁ D.C.

Alejandro Pirachican Villate
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana" – Colombia

David Alexander Yañez Rodriguez
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana" – Colombia

Laura Estefania Garcia Villada
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana" – Colombia

Johemir Jesés Pérez Pertuz
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana" - Colombia

DOI: https://doi.org/10.37811/cl_rcm.v9i3.17715

Importancia de la caracterización del cibercriminal. Un estudio de caso en el delito de hurto a través de medios informáticos en la ciudad de Bogotá D.C.

Alejandro Pirachican Villate [1]
aa.pirachican@correo.policia.gov.co
https://orcid.org/0000-0002-1891-3479
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana"
Colombia

David Alexander Yañez Rodriguez
david.yaez@correo.policia.gov.co
https://orcid.org/0009-0005-0036-6808
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana"
Colombia

Laura Estefania Garcia Villada
laura.garciav@correo.policia.gov.co
https://orcid.org/0000-0002-5796-827X
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana"
Colombia

Johemir Jesés Pérez Pertuz
ppjohemir@gmail.com
https://orcid.org/0000-0002-5094-0530
Escuela de Investigación Criminal "TC. Elkin Leonardo Molina Aldana"
Colombia

RESUMEN

La evolución de la tecnología ha colaborado en el desarrollo de múltiples actividades que favorecen la economía y el mejoramiento de las circunstancias de vida de las personas. Al mismo tiempo, ha dado lugar a situaciones que al realizarse de manera malintencionada, afectan tanto a individuos como a empresas. La meta de este artículo es reconocer la importancia de la caracterización del cibercriminal para prevenirse de los delitos por medio de medios informáticos, es decir, que se toma como caso de estudio la ciudad de Bogotá (Colombia), en los años 2022 y 2023. Para ello se hace un análisis descriptivo de la situación, respaldado por datos estadísticos sobre el aumento de los casos de ciberdelitos en los últimos años, los cuales permiten identificar los sectores que han sido más afectados, y se resalta la importancia de caracterizar al cibercriminal para diseñar estrategias de prevención y combate más efectivas. Finalmente, con la información obtenida se procura que sea de beneficio para el desarrollo de estrategias que permitan avisar este tipo de delitos y mejorar la seguridad de los sistemas informáticos.

Palabras clave: ciberdelito, delitos informáticos, cibercriminal

[1] Autor principal.
Correspondencia: alejandropirachican@gmail.com

Importance of the characterization of the cybercriminal. A case study in the crime of theft through computer means in the city of Bogotá D.C.

ABSTRACT

The evolution of technology has contributed to the development of multiple activities that favor the economy and the improvement of people's living circumstances. At the same time, it has given rise to situations that, when carried out maliciously, affect both individuals and companies. The goal of this article is to recognize the importance of characterizing the cybercriminal to prevent crimes through computer means, that is, the city of Bogotá (Colombia) is taken as a case study, in the years 2022 and 2023. To do this, a descriptive analysis of the situation is made, supported by statistical data on the increase in cybercrime cases in recent years, which allow us to identify the sectors that have been most affected, and the importance of characterizing the cybercriminal to design more effective prevention and combat strategies is highlighted. Finally, the information obtained is intended to be of benefit for the development of strategies that allow us to warn of this type of crime and improve the security of computer systems.

***Keywords*:** cybercrime, computer crimes, cybercriminal

Artículo recibido 12 abril 2025

Aceptado para publicación: 15 mayo 2025

INTRODUCCIÓN

La proliferación de las tecnologías de la información y las comunicaciones ha colaborado con el desarrollo significativo de las actividades laborales, académicas, sociales, investigativas, entre otras. Sin embargo, ha dado lugar a nuevos desafíos en materia de seguridad. El aumento exponencial de los delitos cibernéticos, en particular el hurto por medios informáticos, representa una amenaza creciente a nivel mundial (Amaya Cogollo, 2024).

Teniendo en cuenta el informe del Índice Global de Ciberseguridad de 2024 elaborado por la Unión Internacional de Telecomunicaciones, desde el año 2021 se ha venido presentando un incremento en los delitos cibernéticos, equivalente al 27%, teniendo en cuenta que el compromiso de los países por la creación de medidas que mitiguen la situación, ha llegado a una puntuación media global de 65.7/100 . Esto refleja la necedidad de enfrentar los desafíos y acoge medidas que reconozcan a las necesidades de la sociedad en actual.

La INTERPOL también ha venido realizando investigaciones en las que analiza los casos de ciberdelincuencia y coordina Operaciones como la denominada Synergia II, a través de la cual se buscó combatir el cibercrimer y las redes criminales dedicadas al phishing, robo de información y ransomware, a partir de la cooperación de diversos actores a nivel mundial, y con el apoyo de 56 países (Interpol, 2024).

Otras instituciones dedicadas la investigación cibercriminal como SEON, indican que si bien existen países que invierten gran parte de sus recursos para prevenir los delitos cibernéticos, existen otros en los cuales no hay medidas que se adopten para prevenirlos y controlarlos. En las figuras 1 y 2 se presentan a 2024 los países que presentan mayor y menor peligro de ser víctimas de este modo de ataques (SEON, 2024):

Figura 1. 10 Países con mayor riesgo de cibercrímen y su puntuación en ciberseguridad

Fuente: SEON (2024)

Figura 2. 10 Países con menor riesgo de cibercrímen y su puntuación en ciberseguridad

Fuente: SEON (2024)

En Colombia, la ciudad de Bogotá se ha transformado en un epicentro de esta problemática. Según datos del Centro Cibernético Policial, durante los años 2022 y 2023 se registró un incremento significativo en los casos de hurto por medios informáticos, superando las 7.359 denuncias en 2023. Esta situación evidencia la necesidad urgente de comprender las características de los cibercriminales

que operan en la capital colombiana, así como los factores que facilitan la comisión de estos delitos (Garcia Sanchez, 2021).

Esta investigación tiene como proposito clave caracterizar al cibercriminal involucrado en casos de hurto por medios informáticos en Bogotá durante los años 2022 y 2023. A través de un análisis exhaustivo de datos y casos reales, se busca identificar los perfiles de los delincuentes, sus motivaciones, modus operandi y las vulnerabilidades que enfrentan los .

METODOLOGÍA

Esta investigación fue ejecutada basandose en un estudio de tipo descriptivo, si se tiene en cuenta que, estando de acuerdo con Arias, (2012) “la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento” (p. 24), este tipo de investigación permite describir, detallar, especificar y caracterizar un fenómeno de interés, sin buscar explicar las causas o relaciones que lo producen. Su objetivo es recolectar datos que permitan describir todo lo que se esta trabajando.

En efecto, la investigación explora describir las características criminológicas entorno al delito de hurto por medio de medios informáticos en la ciudad de Bogotá durante los años 2022-2023, realizando un análisis detallado de acuerdo con los temas específicos a tratar, así como aplicar el resultado obtenido de los instrumentos que fueron aplicados a la población estudio para fundamentar las conclusiones y cumplir así los objetivos planteados.

Basandonos en el estudio, se logra adquirir la información necesaria, en lo que se refiere a la relación existe con diferentes particulares del impacto de esta modalidad de hurto informático. Algunos items a mostrar en este apartado son los elemntos de las Consideraciones éticas, los Criterios de Inclusión y Exclusión; y las limitaciones si fuese el caso.

RESULTADOS Y DISCUSIÓN

La cibercriminalidad se ha convertido en una amenaza potencial de forma global que impacta a individuos, organizaciones y gobiernos. En Colombia, el delito de hurto a través de medios informáticos ha realizado una practica en un desarrollo exponencial en los últimos años. Evaluando las últimas décadas, la proliferación de las tecnologías de la información y la comunicación (TIC) ha transformado radicalmente la forma en que se interactúa (Aizencang, 2024). Sin embargo, esta revolución digital

también ha traído consigo un aumento exponencial de la cibercriminalidad. El delito de hurto que se lleva a cabo por medio de medios informáticos, en particular, se ha transformado en una amenaza global que afecta tanto a individuos como a organizaciones (Sáenz Muñoz, 2023).

Bogotá D.C., es conocida como una de las principales ciudades de América Latina y un centro financiero y tecnológico, no ha sido ajena a este fenómeno. La creciente urbanización, la concentración de actividades económicas y la alta penetración de internet en la población han creado un entorno propicio para la proliferación de este tipo de delitos (Pardo, 2009).

De alli que las motivaciones de los cibercriminales en Bogotá son variadas, incluyendo el lucro económico, el espionaje industrial, el vandalismo digital y el activismo político (Quintana, 2023). Comprender estos objetivos es clave para diseñar estrategias de prevención y detección

Los cibercriminales en Bogotá emplean una amplia gama de técnicas y herramientas, desde el phishing y el malware hasta el ransomware y la ingeniería social (Jaramillo Basantes, 2023). La constante evolución de estas técnicas exige una actualización constante de las medidas de seguridad. Por tanto, los sectores más afectados por los delitos informáticos en Bogotá incluyen empresas, entidades gubernamentales, instituciones financieras y ciudadanos particulares. Identificar a las víctimas más comunes permite diseñar estrategias de prevención específicas (Barragan Matiz, 2021).

En este sentido, los delitos informáticos generan pérdidas económicas millonarias para Bogotá, afectando la competitividad de las empresas y la confianza de los ciudadanos en las transacciones digitales (Peralta, 2021). Además, tienen un impacto social significativo, al erosionar la privacidad y la seguridad de los datos personales (De Mora Rivas & Ramos, 2024).

La escena del crimen digital en Bogotá presenta desafíos únicos, como la volatilidad de la evidencia digital y la importancia de tener con herramientas especializadas para su recolección y análisis.

De acuerdo con Ojeda-Pérez (2010), la investigación de delitos informáticos en Bogotá requiere de equipos especializados con conocimientos técnicos en informática y criminología. La coordinación entre diferentes entidades es fundamental para obtener resultados efectivos, por tanto, la colaboración entre el sector público y el privado es primordial para combatir la cibercriminalidad en Bogotá. La elaboracion de redes de colaboración y el cambio de información son clave para prevenir y responder a los ataques (Leiva, 2015).

La conciencia de la población acerca los riesgos de la cibercriminalidad y la promoción de prácticas seguras en línea son herramientas fundamentales para minimizar la debilidad de los ciudadanos.

La Policía Nacional de Colombia (2022) ha señalado que la criminalidad en el país está marcada por diversas formas delictivas, incluyendo el homicidio, el hurto y la extorsión, además del reconocido narcotráfico vivenciado en la mayoría de las regiones del país. Según el informe anual de criminalidad de la Policía Nacional, el año 2022 mostró un aumento en ciertos tipos de delitos.

La criminalidad en Colombia es un fenómeno complejo que requiere una atención integral y multidimensional. A pesar de los esfuerzos realizados, persisten retos significativos que deben ser abordados para lograr una paz duradera y un desarrollo sostenible (Blanco Tifaro & Osorio Escobar, 2023).

Para caracterizar al cibercriminal y las dinámicas del delito de hurto informático en Bogotá, se realizaron encuentros focales con uniformados y investigadores. Estos permitieron identificar los elementos criminológicos y victimológicos clave, así como analizar cómo estos factores interactúan en el contexto de la ciudad. A través de un análisis comparativo de las perspectivas de ambos grupos, se busca comprender la incidencia del cibercrimen en esta modalidad delictiva (Méndez & Monjaraz, 2023).

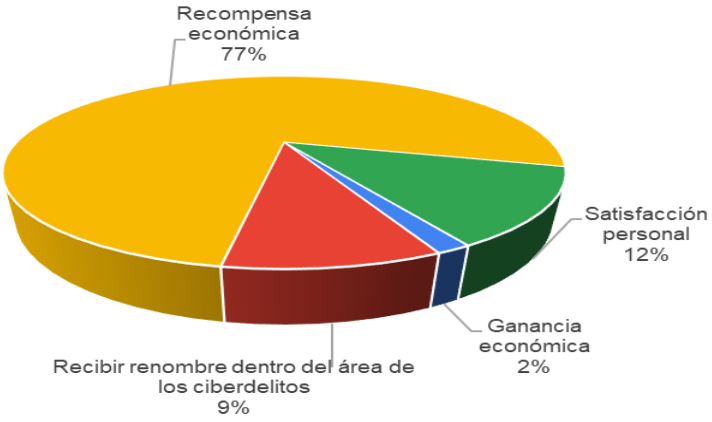
Para analizar la caracterización criminológica del hurto por medios informáticos, se aplicó una encuesta semiestructurada a 63 expertos en ciberseguridad y psicología forense. Los resultados de este instrumento permitieron identificar los elementos distintivos del perfil del cibercriminal en Bogotá durante el período 2022-2023.

La investigación se centró en tres dimensiones: la caracterización del perfil del cibercriminal (Barahona, 2021), la evaluación de su nivel de conocimiento en materia de seguridad (Mondonedo, et.al., 2023) y el análisis del impacto de sus acciones. Este enfoque permitió establecer una base sólida para la descripción detallada del delincuente cibernético y la identificación de los elementos fundamentales para su estudio.

El análisis de los resultados arrojaron datos mostrando que el 89% de los encuestados percibe la existencia de grupos organizados detrás de los ciberdelitos. El perfil del cibercriminal, según los expertos consultados, corresponde en su mayoría a personas con formación media o básica, motivadas

principalmente por ganancias económicas (77%), seguidas por la satisfacción personal y el reconocimiento social (figura 3).

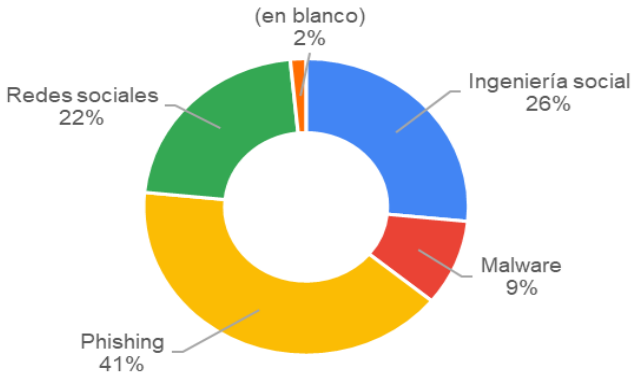
Figura 3. Motivaciones de los cibercriminales en casos de hurto



Fuente: Elaboración propia

Según los encuestados, el perfil del ciberdelincuente se centra en jóvenes entre 18 y 30 años, quienes utilizan principalmente técnicas de phishing (41%), ingeniería social (26%) y redes sociales (22%) para cometer hurtos informáticos (figura 4).

Figura 4. Principales modalidades de hurto cibernético



Fuente: Elaboración propia

Adicionalmente, el 49% de las personas encuestadas se discurre que la población en general tiene un bajo nivel de conocimiento sobre el hurto por medios informáticos. Esta falta de conocimiento es aprovechada por los ciberdelincuentes, quienes utilizan las redes sociales como su principal instrumento para cometer estos delitos

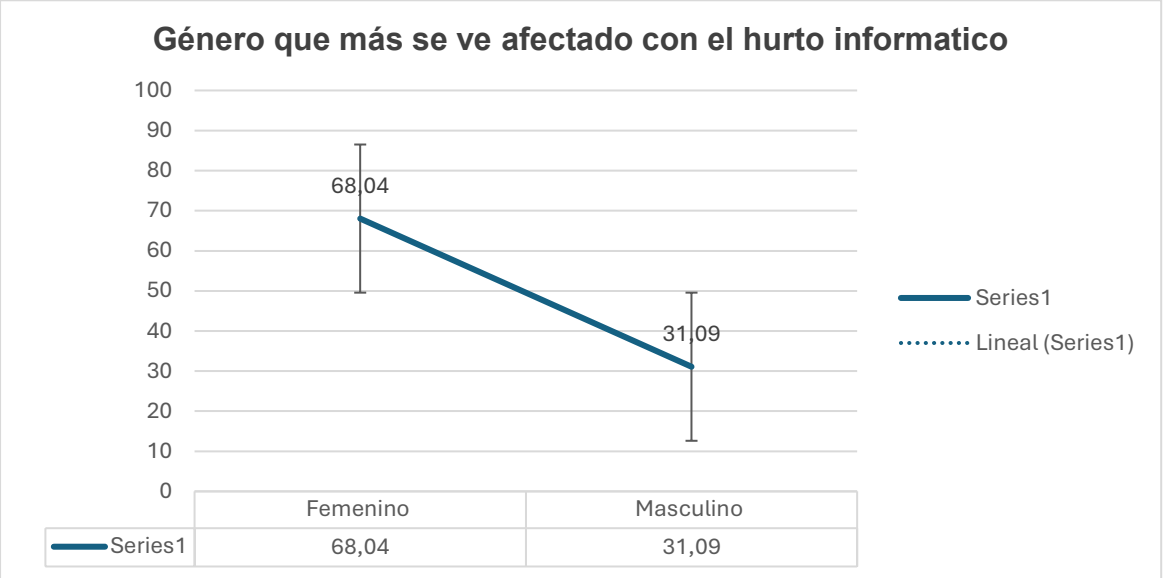
De esta manera, se puede generar una matriz que permita identificar los elementos que componen la caracterización criminológica del ciberdelincuente y los perfiles que son utilizados para la generación del delito (tabla 1).

Tabla 1. Elementos que componen la caracterización criminológica en los casos de hurto

Elementos	Características	Perfil
Perfil del delincuente	Edad Sexo Nivel Educativo Ocupación Motivación Criminal	- Rango de Edad: Jóvenes adultos (18-35 años). - Interés en las nuevas tecnologías y búsqueda de beneficios económicos. - Nivel educativo medio o superior en áreas tecnológicas (informática, ingeniería de sistemas, etc.). - Fraude financiero, ransomware y tráfico de datos. - Bajo nivel de empatía, búsqueda de anonimato y sensación de impunidad.
Tipos de fraude / Ciberdelito	Suplantación de identidad (phishing) Malware y Ransomware Clonación de tarjetas Fraude en línea	Profesionales de la tecnología que se encuentran en diferentes ámbitos profesionales relacionados. Se distingue por tener una gama de habilidades técnicas avanzadas en el uso de herramientas cibernética.
Características de las Víctimas	Edad Género Nivel Socioeconómico Conocimiento en Seguridad Informática Dispositivos Utilizados	Las víctimas de ciberataques suelen ser personas con bajo conocimiento en seguridad informática, como jóvenes, adultos mayores o individuos de estratos socioeconómicos bajos. Incluso organizaciones con medidas de seguridad insuficientes pueden ser blanco de ataques
Proceso de Investigación y Resolución	Métodos de Detección Tiempo de Resolución Colaboración Internacional	La investigación de delitos cibernéticos requiere de un enfoque meticuloso que abarca desde la recepción de denuncias hasta la verificación de la evidencia digital, pasando por la identificación del tipo de delito y un análisis inicial de la situación. Importante tener en cuenta la legislación de cada país

El análisis de los datos nos mostró que los ciberdelincuentes utilizan diversas tácticas para llevar a cabo sus ataques. Los encuestados coincidieron en que la incidencia de estos delitos ha aumentado significativamente en Bogotá durante los últimos años (figura 5)

Figura 5. Género con mayor afectación por el hurto informático en Bogotá



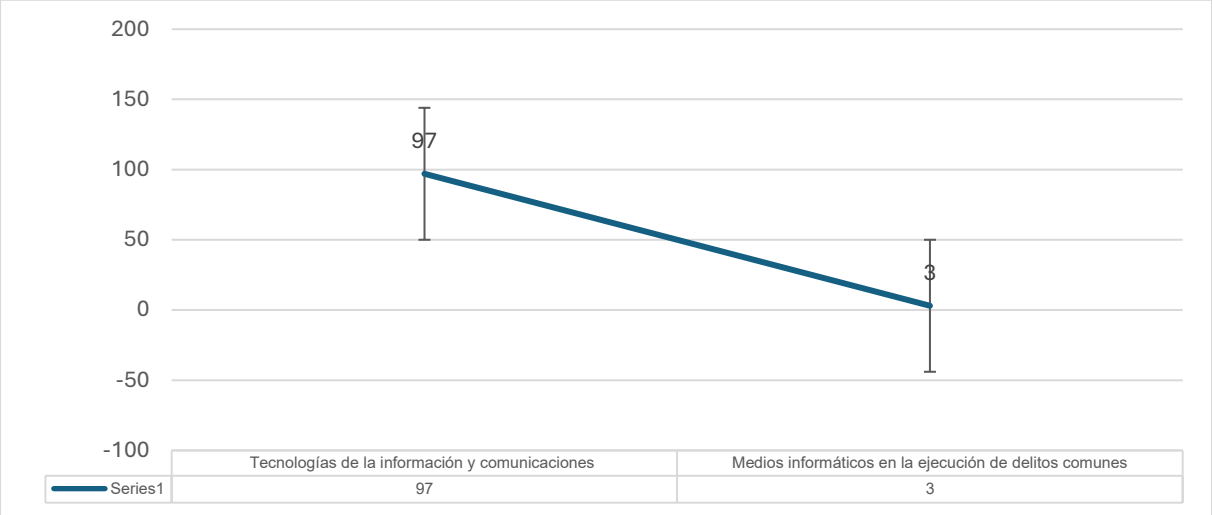
Nota. La Policía Nacional reportó que en lo corrido del año se han presentado 23.640 delitos cibernéticos en el país, lo que significa una reducción del dos por ciento en comparación al mismo periodo del 2022, cuando ocurrieron 24.111 hurtos a los ciudadanos en la red.
Fuente. Estadística delictiva [Tomado] https://www.policia.gov.co/revistacriminalidad.

En Bogotá, durante el período 2022-2023, se registró una disminución del 19.9% en los casos de hurto por medios informáticos, con una reducción de 33 casos en comparación con el año anterior. Las mujeres resultaron ser las principales víctimas (68.04%), seguidas por los hombres (31.9%). Los encuestados consideran que el público en general es el más vulnerable, seguido de las empresas y el sector público. La creciente sofisticación de los ciberdelitos y el bajo nivel de conocimiento de la población sobre este tema contribuyen a esta tendencia.

El 56% de los casos de hurto a través de informáticos que se concentran en establecimientos comerciales, seguido por la vía pública (17%), lugares de esparcimiento (8%), entidades financieras (6%), educativas (5%) y otros (5%).

Los delitos cometidos dentro de esta categoría informáticas entre los años 2022-2023 en Bogotá, el 71% son atribuidos a afectación económica, seguido por 21% de afectación patrimonial, 1% de afectación ambiental y 1% de afectación a la moral administrativa, y aparte el 6% de otros.

Figura 6. Total casos de hurto por medios informáticos en Bogotá en el 2022-2023



Nota. La Policía Nacional reportó que en lo corrido del año se han presentado 23.640 delitos cibernéticos en el país, lo que significa una reducción del dos por ciento en comparación al mismo periodo del 2022, cuando ocurrieron 24.111 hurtos a los ciudadanos en la red. Fuente. Estadística delictiva [Tomado] https://www.policia.gov.co/revistacriminalidad

Los siguientes datos son el total de los casos de hurto llevándolo por medio de medios informáticos, el 97% corresponde a hurto a través de medios informáticos mediante el uso de tecnologías de la información y las comunicaciones, mientras que el restante 3% corresponde a medios informáticos en la ejecución de delitos comunes.

El análisis de los datos muestra que el 97% de los hurtos por medios informáticos están vinculados al uso de tecnologías digitales. No se logró evidenciar una relación reveladora entre el nivel socioeconómico de las víctimas y la incidencia de estos delitos. Los ciberdelincuentes utilizan tácticas como la ingeniería social y la suplantación de identidad para perpetrar sus ataques.

La creciente complejidad de los ciberdelitos ha dado paso a la formación de organizaciones criminales cada vez más sofisticadas (Guzmán, et.al., 2023). Estas organizaciones aprovechan la vulnerabilidad de las instituciones y de la población en general para perpetrar sus ataques, además, aprovechan la falta de conocimientos técnicos y la insuficiencia de las medidas de seguridad facilitan la labor de estos ciberdelincuentes (Lizarazo, 2023).

Asimismo, en la época digital ha tenido consigo una serie de cambios en la sociedad, lo que ha generado nuevos desafíos para las fuerzas del orden (Rubia, 2024). De allí que la creciente sofisticación de los ciberdelincuentes exige una respuesta ágil y adaptada a las nuevas realidades (Miranda Goncalves, 2024).

La ciberdelincuencia plantea una amenaza en constante evolución, caracterizada por una asimetría de poder entre atacantes y defensores. Es allí cuando los cibercriminales aprovechan los avances tecnológicos, mientras que las víctimas a menudo se encuentran desprotegidas, razón por la cual se considera fundamentar la cooperación internacional para contrarrestar esta amenaza (Gallardo Urbini, 2022).

Finalmente, las características homogéneas cuando se contrastan con el delito que comparten con el escenario online entre los ciberdelincuentes, se entiende que la identificación de las personalidades de los ciberdelincuentes como en otros campos de la criminología (Mariel, 2024), sigue estando revelada no tanto por los comportamientos delictivos en red, sino indagando en las características de la conducta patológica o desviada que acompaña y precede a estas acciones delincuenciales.

CONCLUSIONES

La caracterización del cibercriminal en Bogotá durante 2022-2023 ha revelado patrones comportamentales y motivacionales clave que son fundamentales para diseñar estrategias efectivas de prevención y combate al cibercrimen en la región.

Asimismo, la investigación permitió reconocer la necesidad de comprender las motivaciones y técnicas de los ciberdelincuentes para diseñar medidas de seguridad más robustas y eficaces.

Es de resaltar que, el análisis comparativo de los perfiles de ciberdelincuentes y víctimas en Bogotá durante 2022-2023 revela una compleja dinámica de interacciones delictivas. Comprender estos patrones es esencial para desplegar estrategias de prevención y respuesta que aborden de manera integral la creciente amenaza del cibercrimen.

REFERENCIAS BIBLIOGRÁFICAS

Amaya Cogollo, G. S. (2024). Implicaciones legales y desafíos en la persecución de fraudes, estafas y otros delitos cibernéticos en el comercio electrónico en Colombia.

Arias, F. (2012) El Proyecto de la Investigación Introducción a la Metodología Científica. 6ta Edición. Editorial Episteme. Caracas, República Bolivariana de Venezuela

Aizencang, P. (2024). Diáspora digital: una nueva dimensión conceptual. Revista mexicana de ciencias políticas y sociales, (252), 211-226.

Barahona, S. S. (2021). Perfiles del ciberdelito: un campo de estudio inexplorado. Revista de Derecho, (30), 67-76.

Barragan Matiz, J. I. (2021). Estrategias de prevención de delitos de alto impacto en la ciudad de Bogotá, el caso del cuadrante empresarial de Santa Bárbara.

Blanco Tifaro, L. M., & Osorio Escobar, L. M. (2023). Carácter vinculante de las recomendaciones del informe de la Comisión de la Verdad.

De Mora Rivas, A. C., & Ramos, M. H. (2024). Análisis comparativo de las tendencias y principios perseguidos en Occidente en materia de Inteligencia Artificial y su relación con la protección de los datos personales. Revista Jurídica, 9(1), 129-179.

Garzón Santos, J. L., Ruiz Otálora, J. H., Castro Duarte, J. G., & Pérez Pertuz, J. J. (2024). Importancia de la inteligencia artificial para los cuerpos de policía: Un análisis bibliométrico. Revista Logos Ciencia & Tecnología, 17(1), 119-134. https://doi.org/10.22335/rlct.v17i1.2009

Garcia Sanchez, E. Y. (2021). Delitos contra el patrimonio económico, el phishing en Colombia, aproximación criminológica (Doctoral dissertation, Universidad Nacional de Colombia).

Gallardo Urbini, I. M. (2022). Estrategia de Ciberseguridad distribuida, aplicando el concepto de Operación de Inteligencia (Doctoral dissertation, Universidad Nacional de La Plata).

Guzmán, C., Palacios, D., & Palacios, E. (2023). Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá. Revista Semilla Científica, (4), 524-539.

Jaramillo Basantes, F. P. (2023). Modelo de Machine Learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social en la Facultad de Ingeniería en Sistemas Electrónica e Industrial (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Tecnologías de la Información).

Leiva, E. A. (2015). Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local. Archivo de la Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.

Lizarazo, G. A. A. (2023). Aproximación Teórica a los Factores Armados de Inestabilidad, que afectan la Seguridad y Defensa Nacional en el Ciberespacio. Revista Ciberespacio, Tecnología e Innovación, 2(3), 25-56.

Mariel, P. R. L. T. (2024). Cibercriminología: ensayos y reflexiones. Editorial Alfil.

Méndez, M. G. B., & Monjaraz, M. Y. A. (2023). Sociedad de la información y nuevas formas de victimización.

Miranda Goncalves, R. (2024). Amenazas digitales: estrategias efectivas para enfrentar y combatir el cibercrimen. Novos Estudos Jurídicos.

Mondonedo, F. S. C., Del Carpio, C. M. F., Barreto, H. O. V., Rivero, C. A. A., Silverio, E. F. E., & Cruz, M. R. E. (2023). Ciberseguridad y su relación con la empleabilidad para egresados de Ingenieria de Sistemas en una Universidad Pública. Revista de Climatologia Edición Especial Ciencias Sociales, 23, 1511.

Moreno, H. A. C., Rincón, H. C., Roncancio, L. E. T., & Pertuz, J. J. P. (2025). Sandbox virtual con herramientas open source para pentesting: Una propuesta tecnológica aplicada a la seguridad cibernética de las pymes. *Sapiens in Artificial Intelligence*, *2*(2).

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41-66.

Pardo, C. F. (2009). Los cambios en los sistemas integrados de transporte masivo en las principales ciudades de América Latina.

Peralta Cuadrado, M. L., & Roa Ibarra, E. E. (2021). El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia.

Policía Nacional de Colombia (2022). Observatorio del crimen. Extraido de https://caivirtual.policia.gov.co/prevencion

Quintana, Y. (2023). Ciberguerra. Los libros de la Catarata.

Rubia, J. M. I. (2024). Inteligencia Artificial y Derechos Humanos: desafíos y oportunidades en la era digital. Introducción al monográfico. Deusto Journal of Human Rights, (14), 11-31.

Sáenz Muñoz, S. (2023). El delito interceptación de datos informáticos: un análisis en el derecho penal colombiano.

SEON (2024). Informe global sobre ciberdelincuencia: ¿Qué países corren mayor riesgo?

Unión Internacional de Telecomunicaciones (UIT). Informe del Índice Global de Ciberseguridad de 2024.