Aproximación al ciberdelincuente desde la perspectiva del control social

Approaching the cybercriminal from a perspective of social control

Abordagem do criminoso cibernético a partir de uma perspectiva de controle social

• Fecha de recepción: 2021/08/23
• Fecha de evaluación: 2022/09/19
• Fecha de aprobación: 2023/01/25

Para citar este artículo / To reference this article / Para citar este artigo: Díaz, G., Molina, A., Serrador, L. y Cárdenas, J. (2023). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad, 65*(3), 81-95. https://doi.org/10.47741/17943108.508

Guillermo Augusto José Díaz Samper
Magíster en Comunicación y en Seguridad Pública
Investigador en Ciencia, Tecnología e Innovación
Escuela de Posgrados de Policía Miguel Antonio Lleras Pizarro
Policía Nacional de Colombia, Bogotá D. C., Colombia
guillermo.diaz1008@correo.policia.gov.co
https://orcid.org/0000-0002-8168-5122

Alba Luz Molina Garzón
PhD en Educación
Investigadora en Ciencia, Tecnología e Innovación
Escuela de Posgrados de Policía Miguel Antonio Lleras Pizarro
Policía Nacional de Colombia, Bogotá D. C., Colombia
alba.molina@correo.policia.gov.co
https://orcid.org/0000-0002-4259-2986

Luis Enrique Serrador Osorio
Magíster en Seguridad Pública, Lenguas Modernas
Investigador en Ciencia, Tecnología e Innovación
Escuela de Posgrados de Policía Miguel Antonio Lleras Pizarro
Policía Nacional de Colombia, Bogotá D. C., Colombia
luis.serrador@correo.policia.gov.co
https://orcid.org/0000-0002-2690-5559

Resumen

El presente artículo aporta un acercamiento al ciberdelincuente identificando las características comunes en la personalidad de quienes delinquen en este escenario. Para llevar a cabo la investigación, se tomó una muestra de diecinueve expertos que forman parte de la Dirección de Investigación Criminal e INTERPOL, abordados por entrevista en profundidad. Los datos obtenidos fueron tratados desde un diseño hermenéutico con énfasis en la teoría fundamentada, por medio de tres fases elaboradas en análisis matricial de codificación abierta, selectiva y teórica; a partir de las cuales se establecen algunas de las tácticas del ciberdelincuente desplegadas en el ciberespacio a través de tecnologías de la información y las comunicaciones; su descripción desde el modelo *big five* y se identifican algunas de sus características como la falta de empatía, escrúpulos, incapacidad para el control de emociones, confianza y capacidad de innovar sus *modus operandi* (Sánchez y Robles, 2013). Finalmente, desde las teorías del control social se han estudiado el ciberdelito y los actos del ciberdelincuente de una manera formal que vela por encontrar estrategias de control del Estado, según González (2010), o informal, que busca los motivos que conducen a cometer delitos, como lo afirma López (2015), a partir de lo cual, al final, se presentan algunas recomendaciones.

Palabras clave:

Protección de datos, control social, delincuencia (fuente: Tesauro de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura – UNESCO). Delitos informáticos, seguridad informática, perfiles de delincuentes (fuente: autor).

Abstract

This article provides an approach to cybercriminals by identifying the common characteristics in the personality of those who commit crimes in this scenario. In order to carry out the research, a sample of nineteen experts from the Criminal Investigation Directorate and INTERPOL were interviewed in depth. The data obtained were treated based on a hermeneutic design with emphasis on grounded theory, by means of three phases elaborated in matrix analysis of open, selective and theoretical coding; from which some of the tactics of cybercriminals deployed in cyberspace through information and communication

Jesús María Cárdenas Beltrán
Doctor en Sociología Jurídica e Instituciones
Escuela de Posgrados de Policía
Miguel Antonio Lleras Pizarro
Bogotá D. C., Colombia
jesus.cardenas1231@correo.policia.gov.co
https://orcid.org/0000-0002-8381-3044

technologies are established; their description based on the *big five* model and the identification of several of their characteristics such as lack of empathy, scruples, the inability to control emotions, confidence and the ability to innovate their *modus operandi* (Sánchez y Robles, 2013). Finally, theories of social control have studied cybercrime and the acts of cybercriminals in a formal way that seeks to find strategies to control the State, according to González (2010), or informally, seeking the motives that lead to committing crimes, as stated by López (2015), on the basis of which, at the end, some recommendations are presented.

Keywords:

Data protection, social control, crime (source: Thesaurus of the United Nations Educational, Scientific and Cultural Organisation - UNESCO). Computer crime, computer security, criminal profiles.

Resumo

Este artigo traz uma abordagem sobre os cibercriminosos, identificando as características comuns na personalidade de quem comete crimes nesse cenário. Para a realização da investigação foi recolhida uma amostra de dezanove peritos que integram a Direcção de Investigação Criminal e a INTERPOL, abordados através de entrevista em profundidade. Os dados obtidos foram tratados a partir de um desenho hermenêutico com ênfase na teoria fundamentada, por meio de três fases desenvolvidas em análise matricial de codificação aberta, seletiva e teórica; a partir da qual se estabelecem algumas das táticas cibercriminosas implantadas no ciberespaço através das tecnologias de informação e comunicação; A sua descrição baseia-se no modelo dos *big five* e são identificadas algumas das suas características, como a falta de empatia, escrúpulos, incapacidade de controlar emoções, confiança e capacidade de inovar o seu *modus operandi* (Sánchez y Robles, 2013). Por fim, a partir das teorias de controle social, o cibercrime e os atos dos cibercriminosos têm sido estudados de forma formal, que busca encontrar estratégias de controle do Estado, segundo González (2010), ou informalmente, que busca os motivos que levam ao cometimento dos crimes. , conforme afirma López (2015), a partir do qual, ao final, são apresentadas algumas recomendações.

Palavras-chave:

Proteção de dados, controle social, crime (fonte: Tesauro da Organização das Nações Unidas para a Educação, a Ciência e a Cultura – UNESCO). Crimes informáticos, segurança informática, perfis criminais (fonte: autor).

Introducción

Con el surgimiento de internet, así como de las tecnologías de la información y la comunicación (TIC), los seres humanos han encontrado un nuevo espacio de desarrollo e intercambio social que les permite conectarse en tiempo real con personas, empresas e instituciones educativas, por citar algunos ejemplos, en diferentes lugares del mundo y, a la vez, afrontan el escenario más catastrófico con el fenómeno denominado *ciberdelincuencia*. Así las cosas, frente a este último aspecto, se puede aseverar que los delincuentes y organizaciones que se dedican a esta actividad ilícita han logrado vulnerar a las personas

que han desarrollado, a través de internet y las TIC, diferentes facetas de su vida, lo que menoscaba cada una de las esferas de funcionamiento de sus víctimas.

El uso de herramientas tecnológicas como internet y dispositivos digitales para llevar a cabo actividades delictivas se conoce como ciberdelincuencia. Los perpetradores de estos delitos, o ciberdelincuentes, pueden atacar a personas, empresas, organizaciones e incluso gobiernos. Pueden hacerlo con una variedad de objetivos, como el fraude, la venta ilegal de bienes y servicios, el robo de información confidencial, la infección de sistemas informáticos y los ataques de denegación de servicios. Por ello, se parte de la definición de la Universidad en Internet-UNIR (2021) del ciberdelito que precede la existencia de un ciberdelincuente que tiene diversas herramientas tecnológicas, a través de tecnologías de la información y la comunicación, para operar, así como formas conductuales de hacerlo, sobre personas naturales y jurídicas que son victimizadas en todas sus áreas humanas.

No podemos evitar señalar que la ciberdelincuencia puede ser practicada tanto por individuos aislados como por organizaciones criminales, incluidas naciones, lo que amplía su alcance y complejidad. Adicionalmente, existen varios tipos de delitos cibernéticos; algunos dependen únicamente de los medios digitales, mientras que otros utilizan los recursos de internet para cometer delitos tradicionales como la estafa. En el artículo web de Sistemius (2020) se señala que hay cuatro tipos de ciberdelitos: estafas, delitos informáticos de daños, defraudaciones de telecomunicaciones y delitos contra la intimidad.

Así, según la anterior fuente (2020), las estafas informáticas están dirigidas hacia el desplazamiento patrimonial buscando un beneficio lucrativo para el ciberdelincuente en perjuicio de la víctima, particularmente, a partir de la alteración, sustracción o hurto de la información en el ciberespacio; los delitos informáticos de daños implican acciones que buscan el daño, deterioro, pérdida, alteración o supresión de datos informáticos por parte de un tercero a partir del uso de *malware* o *software* malicioso; las defraudaciones de telecomunicaciones implican el acceso indebido o sin consentimiento de las personas a su internet, wifi, entre otros, y ocasionarles algún costo económico a cambio, y los delitos contra la intimidad involucran el acceso delictivo a los datos personales y secretos de alguna persona y usarlos en la generación de algún daño.

De acuerdo con lo anterior, según se describe por Sistemius (2020), las estafas informáticas se encuentran comprendidas por el *phishing*, que consiste en la pesca de información bancaria para ocasionar transferencias fraudulentas a una cuenta de terceros, y el *carding*, que involucra la suplantación o clonación de tarjetas de manera virtual para ocasionar un hurto a un víctima por un ciberdelincuente; por su parte, los delitos informáticos de daños involucran el uso de *malware*, que es un *software* maligno que destruye o utiliza información privada y datos de personas naturales o jurídicas a favor de un agresor, o virus informáticos como el *wanna cry* que se encargan de la defraudación de datos de otras personas; a su vez, las defraudaciones de telecomunicaciones implican el aprovechamiento ilícito de un particular en contra del dueño de las mismas; finalmente, los ciberdelitos en contra de la intimidad comprenden la sustitución de identidad de alguien para perjudicarlo económica o moralmente en redes sociales o portales, mientras que la sextorsión requiere de la sustracción de material multimedia o fotográfico de tipo sexual de un individuo para pedirle dinero a cambio de no revelar la información de manera pública.

En este orden de ideas, la victimización en el ciberespacio se ha incrementado con el uso creciente de las TIC. Al revisar el caso colombiano, entre 2017 y 2019 tuvieron lugar 51 201 denuncias en las cuales se hace visible el hurto informático con 31 058 casos y el robo de identidad con 8037 casos. Al respecto, las ciudades afectadas por estos delitos fueron Bogotá con 5308 casos, Cali con 1190 casos y Medellín con 1186 casos. Aunado a lo anterior, durante el año 2019 se generaron cerca de 45.5 % de denuncias por canales virtuales, cifra que representó alrededor de 28 827 incidentes que afectaron la seguridad de la información empresarial (Tanque de Análisis y Creatividad de las TIC, 2019). Por su parte, el Centro Cibernético de la Policía Nacional, durante el primer semestre del 2020, determinó que esta modalidad de delitos aumentó en un 59 % en comparación con el 2019 (Asociación Colombiana de Ingenieros de Sistemas, 2020).

A esto se suma que durante el 2020 la "suplantación de identidad" fue uno de los delitos cibernéticos con mayor predominancia en Colombia, de acuerdo con las cifras descritas por la Fiscalía General de la Nación (2020), debido al incremento de las cifras de captura de datos personales, las cuales oscilan en 372 % en comparación con el 2019. También se resalta que en el 2020 se presentaron alrededor de 3800 casos denunciados en los que los ataques de cibercriminales de este tipo se presentan en los ámbitos empresarial y personal (Fiscalía General de la Nación, 2020).

En 2021, de acuerdo con la Fiscalía General de la Nación (2020), se establece que el incremento de casos de cibercrímenes con respecto al 2020 fue de un 108 %, lo que representa un total de 6649 casos más que el año anterior, que fue de 3196. Es de resaltar que la suplantación de sitios web a través del *phishing*

fue de 2825 veces con una diferencia de 638 casos en comparación con el año 2020, que presentó cerca de 2187 casos.

El ciberdelito y las diferentes formas en que se configura presentan un incremento sustancial en los últimos años, toda vez que su principal nicho de formación se encuentra en las TIC. Por esto, el andamiaje tecnológico se convierte en un riesgo potencial para las economías lícitas del país y un incremento exponencial de dividendos para los grupos dedicados a su desarrollo.

Aproximaciones teóricas al concepto de ciberdelincuencia

El análisis del ciberdelito tiene su fundamento teórico en la forma de conceptualizarlo como modalidad criminal, en la que la doctrina jurídica que existe en la actualidad desempeña un papel preponderante en la relación existente entre el delito y la pena, la cual se debe abordar de forma exegética cuando tiene lugar la materialización de este delito. En primer lugar, el concepto requiere de una connotación más amplia que los delitos tradicionales, porque la forma de llevarlo a cabo en escenarios de prevalencia inmaterial conduce a transformaciones complejas de elementos que requieren ser tipificados para una adecuada valoración normativa y penal; en segunda instancia, al hacer parte de una sociedad eminentemente digitalizada, tiene como centro de desarrollo la gestión de la información, los datos y los sistemas de computación que se requieren para generar lazos de interacción social, y tercero, es necesario que una delimitación de las conductas ilícitas que caracterizan el cibercrimen tenga lugar para poder explicar de la mejor forma su *modus operandi*, además de los elementos y actores que facilitan su materialización (Arrieta, 2016).

Así las cosas, la teoría de las actividades rutinarias aplicada a internet presenta un aporte fundamental al trabajo en tanto establece cómo el ciberdelito se constituye en un efecto desplegado de la unión de un espacio (ciberespacio), un tiempo y un objetivo de un criminal que no encuentra resistencia en tanto no existe un defensor que evite su accionar; el ciberespacio, por tanto, implica la contracción total de las distancias al facilitar la interacción de las personas a lo largo y ancho de la tierra, pero experimenta la dilatación de las posibilidades de encuentro de ellas en tiempos separados e inmediatos a la vez, lo que produce las condiciones para que los agentes delictivos cuenten con pocas restricciones y la posibilidad de atacar desde cualquier computador en cualquier parte del mundo a cualquier persona natural o jurídica en las mismas condiciones, causándole graves daños, y con grandes posibilidades de escapar, lo que se genera debido a la deslocalización, transnacionalidad, neutralidad y descentralización del ciberespacio, que le ofrece popularización y anonimato a los usuarios, que experimentan incentivos para delinquir en estas características particulares, de modo que presenta un ámbito de oportunidad novedoso para el criminal, que se expresa en nuevas formas creativas de ataque a víctimas (Miró, 2011).

En ese sentido, desde los fundamentos teóricos de la criminología que aplican al campo de la cibernética, la caracterización de los delitos necesita de una valoración normativa más allá del soporte que existe en la actualidad para la atención de las manifestaciones de los delitos que se materializan fuera de internet, y también necesita que la gestión de información que demanda la sociedad actual, una sociedad del conocimiento, presente restricciones como las acciones sociales que tienen lugar fuera de red y, finalmente, la tipificación de aquello que es o no es un delito cibernético (Arrieta, 2016).

Otra corriente de pensamiento que se relaciona con el cibercrimen es aquella que implica los rasgos de personalidad que predisponen a las personas a inclinarse por el desarrollo de este tipo de actividades ilícitas; entre ellas se destaca la teoría del *big five*, o mejor conocida como el modelo de los cinco factores, con el cual se establece en qué grado están arraigadas, o no; son cinco dimensiones básicas de la personalidad que pueden propiciar este tipo de inclinación delictual (Sánchez y Robles, 2013). Para empezar, el ciberdelincuente se caracteriza por la energía, que hace alusión a la confianza que denota el delincuente en el manejo de las relaciones interpersonales con sus víctimas; también se encuentra la afabilidad, que puede ser interpretada como la falta de sensibilidad frente a las dificultades del otro, por lo que no presenta ningún tipo de menoscabo emocional ante el sufrimiento de quienes eligen como víctimas; el tesón, como tercer factor de medición, comprende la falta de escrúpulos de la persona para lograr cumplir con las actividades trazadas; el cuarto factor se relaciona con la estabilidad emocional, que va en detrimento del delincuente toda vez que presenta poca tolerancia a la frustración y lo lleva a sobredimensionar la ansiedad, la depresión y la irritabilidad, y finalmente, el quinto factor se relaciona con el *modus operandi*, que comprende la falta de valores y de sentimientos que le permitan concientizarse de las acciones y consecuencias de sus actos (Sánchez y Robles, 2013).

En este sentido, los rasgos de personalidad que sobresalen en el ciberdelito apuntan al desarrollo de acciones que van en detrimento de las personas que son seleccionadas como víctimas, las cuales son abordadas para ganar su confianza, lo que se conoce como "ingeniería social", y obtener el máximo de información, para luego, a pesar de generar daño en su vida social

y laboral –por citar algunos ejemplos–, ejecutar el delito o explotar sus vulnerabilidades sin importar las consecuencias que puedan generar en la víctima. Este tipo de comportamiento delictual, por lo general, está enmarcado en una característica sobresaliente de falta de control de impulsos o conductas limítrofes, las cuales se caracterizan por el poco control que tienen de la ansiedad, de la ira e incluso de los cuadros de depresión que puedan llegar a presentar cuando no alcanzan las metas trazadas (Sánchez y Robles, 2013).

Por otra parte, la victimización derivada del ciberdelito puede tener diferentes ámbitos de impacto, pero, más allá de la diversidad de escenarios de afectación a los ciberusuarios, existe un punto común: las habilidades y motivaciones de los delincuentes informáticos. En este orden de ideas, existen estudios someros que intentan encontrar una generalización de los comportamientos habituales del ciberdelincuente y llegan a considerar que los perfiles de estas personas pueden relacionarse con jóvenes obsesionados por el medio informático o la internet; también, por tener el perfil de un empleado decepcionado con su empresa que busca algún tipo de artilugio para hacerla fracasar (Maza, 2021). No obstante, a pesar de este acercamiento, se puede advertir que la cientificidad de los soportes investigativos aún es primigenia, para poder establecer una perfilación clara y de evidencia para los organismos de seguridad que están dedicados a su estudio y seguimiento constante (Cámara, 2020).

Otra teoría que vale la pena tratar, para la comprensión del ciberdelito, se relaciona con el control social, el cual tiene lugar cuando en el escenario donde se materializa pueden ser controladas las condiciones para que las acciones delincuenciales se presenten en su mínima expresión y generen el menor impacto negativo; así las cosas, esta teoría brinda dos perspectivas: la primera relacionada con lo formal, lo cual puede entenderse como un proceso de integración social que se deriva de la criminología en el que se propone el desarrollo de estrategias de control que se llevan a cabo para regular la conducta de los individuos, promover la estabilidad de los grupos sociales y garantizar el orden social con mecanismos de coerción y persuasión (González, 2010). Por otra parte, desde lo informal, tiene relación con la oportunidad del ciberdelincuente para llevar a cabo el delito y las formas de relacionamiento que pueden darse para su debida regulación, con quienes ejercen el control social. De esta manera, el control social tiene fundamento desde cuatro aspectos: (a) la interacción convencional con personas o instituciones; (b) las formas de relacionamiento; (c) por vinculación en actividades cotidianas y rutinarias, y (d) por el valor moral de las reglas sociales (López, 2015).

De igual manera, los delitos tradicionales involucran cada día mayores capacidades tecnológicas y reclutan ciberexpertos que operan con diferentes herramientas, enfoques de ofensa y niveles de anonimato en línea. Esta particularidad del delito informático y de la fusión del delito tradicional con el ciberespacio requiere nuevo conocimiento sobre conductas, factores y características de estos ofensores en línea, con el fin de diseñar estrategias de control y sobre todo de prevención en una sociedad cada vez más conectada.

Por lo anterior, el presente artículo intenta responder a los siguientes interrogantes: ¿cuáles son los factores y características relevantes que permiten describir al ciberdelincuente y de qué manera se podría prever y contener el crecimiento del ciberdelito?

Se realizó un abordaje a este tema desde tres perspectivas: hacer una aproximación teórica a la comprensión del ciberdelincuente; identificar las tipologías más recurrentes, factores y características de los delitos informáticos, y formular pautas de comprensión y análisis sobre los ciberdelincuentes.

Método

Los resultados de la investigación se fundamentaron en cuatro aspectos: el diseño metodológico, la selección de la muestra, las técnicas de recolección y el análisis de datos.

Diseño metodológico

Se estructuró un enfoque cualitativo con el cual fue posible orientar el trabajo de recolección, tratamiento y análisis de información, basado en el paradigma naturalista que permitió establecer una filosofía de interpretación de las múltiples realidades para tener una visión más amplia del tema en estudio; de esta manera, se pudo establecer que, desde una perspectiva cualitativa, "la realidad es subjetiva, no existe una única realidad, sino más bien múltiples realidades" (Miranda y Ortiz, 2020, p. 8). Con frecuencia, estas características sirven para descubrir cuáles son las preguntas de investigación más importantes y después repensarlas y responderlas. La acción indagatoria se mueve de manera dinámica en ambos sentidos: "Entre los hechos y su interpretación, y resulta un proceso más bien circular y no siempre la secuencia es la misma, varía de acuerdo con cada estudio en particular" (Hernández, 2020, p. 14).

En este orden de ideas, los resultados que se obtuvieron de la investigación fueron aplicables y validados para la comprensión del ciberdelincuente. Mediante este diseño, los datos que se obtuvieron del trabajo de campo fueron clasificados por temas, conceptos y teorías, los

cuales fueron trabajados a partir de la experiencia social de los participantes de la investigación. En esencia, el empleo del diseño metodológico permitió construir un mapa de significados compartidos por grupos sociales que tienen características comunes, los cuales regulan la toma de decisiones sobre los aspectos que debería contemplar la construcción de estrategias de prevención y erradicación del ciberdelito.

Con respecto al método de análisis de la información recolectada durante el trabajo de campo, se consideraron las bondades de la hermenéutica por medio de la teoría fundamentada, la cual pudo considerarse la perspectiva de investigación que permitió lograr una comprensión profunda de los resultados de la aplicación de los instrumentos de recolección, en este caso la entrevista en profundidad y la fundamentación teórica que acompañó el desarrollo de la investigación. La aplicabilidad de este método partió de la capacidad que tiene el investigador para descartar toda interferencia o variable extraña que surge respecto a la comprensión del tema en cuestión (Quintana y Hermida, 2019), lo que permite la formulación de unidades de análisis traducidas en aspectos categoriales que pueden llegar a ser teorizados de acuerdo con las características propias que diferencian a cada una de las demás; motivo por el cual es común encontrar, como se había planteado, semejanzas y diferencias que hacen posible la identificación de la categoría, la forma de sus atributos y las condiciones de su aparición (Moreno, 2017).

Las fases de la investigación se fundamentaron en un tipo fenomenológico mediante el cual se llevó a cabo la búsqueda de los elementos que explican la realidad circundante del objeto de estudio, desde la comprensión de los componentes de cada aspecto que hace posible la elaboración de un conocimiento acorde con las necesidades investigativas, por lo que en este tipo de investigación es necesario tener en cuenta pasos como la preparación de la recolección de datos, su organización, análisis y reducción de datos, así como el resumen, las implicaciones y los resultados (Aguirre y Jaramillo, 2012, p. 64). De esta manera, desde la fenomenología se contempló la identificación de la población, la selección de la muestra que permitió establecer los parámetros de representatividad de esta para la generalización de la información y el instrumento de recolección adecuado, en este caso, una entrevista en profundidad y el marco teórico establecido para su triangulación.

Selección de la muestra

Teniendo en cuenta que la población es el conjunto de elementos que tienen las mismas características objeto de análisis (Mucha y Chamorro, 2021), se puede establecer que, en el desarrollo de la investigación, se abordaron aquellos actores que tuvieron relación con la ciberdelincuencia y el ciberdelito en Colombia. En este orden de ideas, la muestra se convierte en una parte representativa de la población; para el presente estudio, se tomaron como muestra representativa 19 expertos en ciberdelincuencia, ciberdelito y ciberseguridad, que estudian las características de los tipos de conducta más sobresalientes que permiten aproximarse a la descripción del ciberdelincuente.

En este sentido, el tipo de muestreo que se utilizó para la obtención de la población representativa fue no probabilístico propositivo o intencional (Cortés et al., 2020), teniendo en cuenta que se parte de la elección de sujetos conocedores del tema, cuyos conocimientos fueron esenciales para la descripción del ciberdelincuente.

Técnicas de recolección

Para el desarrollo de la fase de recopilación de información se construyó una técnica cualitativa que permitió obtener información que pudo ser complementada o contrastada desde la subjetividad. En este sentido, se empleó una entrevista en profundidad, la cual puede ser interpretada como "una interacción entre dos personas, planificada y que obedece a un objetivo, en la que el entrevistado da su opinión sobre un asunto y el entrevistador recoge e interpreta esa visión particular" (Sordini, 2019, p. 78).

Así, esta técnica se aplicó a los expertos que reunían las condiciones suficientes de conocimiento y experticia en las temáticas abordadas para la comprensión del objeto de investigación. Para aplicar este instrumento fue necesario seguir los parámetros relacionados con la introducción, el desarrollo y el final o cierre. La fase introductoria hizo referencia a la planeación de la entrevista o la definición del objetivo que se persigue, así como la duración y la formulación de preguntas que orientarán el diálogo con el entrevistado.

En cuanto a la fase de desarrollo, tuvo relación con la aplicación de las preguntas orientadoras, las cuales, por lo general, debieron inducir a la obtención de respuestas argumentadas por parte del entrevistado. Y la fase de finalización o cierre es aquella en la que se realizan preguntas de confirmación frente a temas que no se hayan entendido y se plasma la oportunidad para próximas entrevistas frente al tema objeto de estudio. Estas entrevistas pueden ser individuales o colectivas según criterio del investigador y el objetivo que se persiga con su aplicación (Sordini, 2019).

Análisis de datos

Con los fundamentos de la hermenéutica, es preciso advertir que esta metodología de análisis incluyó los repositorios de información provenientes de la entrevista y de los postulados teóricos consultados; estos últimos, con alto contenido científico en los resultados, los cuales fueron sometidos a la comparación. Es importante resaltar que el diseño metodológico seleccionado para estos fines es una práctica científica emergente, toda vez que permite mejorar la pregunta de investigación e incluir el análisis de contexto junto con la información en estudio para develarlos como hallazgos dentro de la investigación.

De esta manera, los datos en su totalidad fueron codificados en todas las formas posibles desde los siguientes cuestionamientos: ¿qué indica la categoría que fue extraída de las familias analizadas?, ¿cuál es el dilema principal que busca dilucidar el investigador con la aplicación de las técnicas implementadas? y ¿cómo se explica la continua búsqueda de información para responder a los vacíos de información que contempla la formulación problémica? Desde esta perspectiva fue posible que el investigador llevara a cabo movimientos repetitivos hacia adelante y hacia atrás a lo largo de la información recolectada, con el fin de realizar comparaciones constantes entre códigos, categorías y conceptos (Southby y Cooke, 2019).

Desde esta perspectiva, el análisis de información tiene lugar desde el primer momento de la recolección de información, partiendo de que esta primera aproximación al objeto de estudio es eminentemente inductiva, por lo que se convierte en un escenario asequible que permite la inclusión de información que explicita o se acerca a la comprensión del objeto de investigación, como es el ciberdelincuente. En esencia, este tipo de análisis permite una precomprensión que tiene lugar desde los primeros acercamientos teóricos y del papel exhaustivo de la inducción de concepciones, lo cual da vía libre a la emergencia de la deducción y la especulación.

Materiales y equipos

Para determinar las características más relevantes que definen al ciberdelincuente, se aplicaron entrevistas en línea a 19 expertos que por su campo de trabajo en la Dirección de Investigación Criminal e INTERPOL son conocedores del comportamiento y las principales características de la ciberdelincuencia, el ciberdelito y la ciberseguridad.

La entrevista se construyó en función de 15 preguntas enmarcadas en cuatro categorías:

Ciberdelincuencia, entendida como las actividades en las que está presente el uso de computadores y redes informáticas para la manipulación de datos digitales por personas que tienen habilidades avanzadas en este campo y cuya acción va en detrimento de la persona que se convierte en víctima (Shick y Toro, 2017).

Características del ciberdelincuente, categoría orientada a comprender el análisis científico de los aspectos psicosociales de una persona que presenta repertorios conductuales delictivos, a fin de anticipar su comportamiento, prevenirlo y minimizar su impacto delincuencial (Norza y Vargas, 2016).

Control social, que se relaciona con los elementos normativos que crean las instituciones frente al cumplimiento de los fines que persigue el sistema político imperante en los Estados para el logro del orden social (Restrepo y Cortina, 2020).

Prevención y contención del delito, la cual está relacionada con las acciones, estrategias, procesos o medidas, planes, entre otros, que se llevan a cabo para desincentivar conductas delictivas en la sociedad (Restrepo y Cortina, 2020).

Aunado a lo anterior, se complementó la aplicación de la entrevista semiestructurada con la búsqueda de teorías que avalan o debaten los hallazgos que pueden ser obtenidos de los expertos con la revisión sistemática de documentos científicos (Villasís et al., 2020) que se han construido en torno al ciberdelincuente, y que desde la metodología dio lugar a la determinación de los criterios de inclusión consistentes en documentos avalados por la comunidad académico-científica y que tengan relación con el tema en investigación y de exclusión de aquella información que es consultada a través de blogs, columnas de opinión y documentos que se alejen del ciberdelincuente.

De igual manera, se seleccionaron palabras clave para la construcción de fórmulas que permitieron la búsqueda de información mediante operadores booleanos "and & or" en bases de datos como Scielo y Redalyc, por citar algunos ejemplos. En definitiva, se dieron a conocer los criterios que se tuvieron en cuenta para llevar a cabo la pesquisa documental en torno al tema de investigación, entre los que sobresalen la estrategia de exploración y la metodología de recolección.

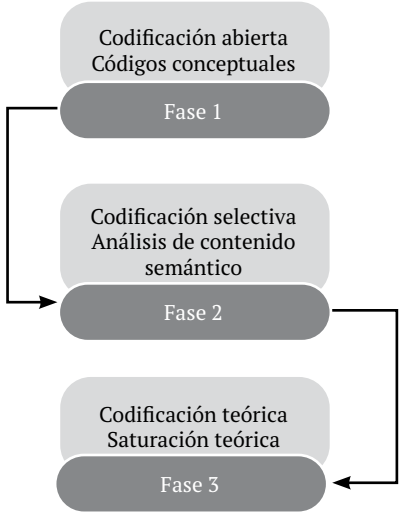
Procedimiento

Una vez se llevó a cabo la recolección de información, se realizó su ordenamiento conceptual, aplicando

los postulados del método comparativo constante, consistente en la codificación de la información hasta llegar a la saturación teórica en diagramas para la interpretación del tema objeto de estudio (Morguen et al., 2019), lo que permitió dilucidar las categorías centrales de la investigación. También, desde esta perspectiva fue posible la recolección y el análisis de datos simultáneos, el diseño de categorías de datos y las relaciones de memo escritura con el fin de elaborar las categorías.

Además, para la presentación teórica del tema en investigación se tuvo en cuenta el desarrollo de tres fases, como se describe en la figura 1.

Figura 1. | Fases de la teoría fundamentada para el ciberdelincuente



Nota: se describen las tres fases de la teoría fundamentada que fueron implementadas para la construcción de información con el propósito de resolver los vacíos de información que motivaron la formulación problémica de la investigación.

En la primera fase, conocida como codificación abierta, se llevó a cabo un exhaustivo análisis de los datos recopilados en el trabajo de campo. En esta etapa se buscaba identificar patrones, tendencias y conceptos fundamentales que permitieran comprender y definir de manera teórica al ciberdelincuente.

A medida que se examinaban los datos, se descubrieron códigos conceptuales y categorías apriorísticas que resultaron ser de gran utilidad para organizar y clasificar la información obtenida. Estos códigos conceptuales representaban elementos esenciales y recurrentes relacionados con el comportamiento, las características y las motivaciones de los individuos involucrados en la ciberdelincuencia.

Al emplear estos códigos conceptuales y categorías apriorísticas, se logró establecer una estructura teórica inicial que proporcionaba una visión general del ciberdelincuente. Estos conceptos y categorías permitieron establecer conexiones significativas entre los diversos aspectos analizados, lo que contribuyó a la comprensión más profunda de la naturaleza y dinámica de la ciberdelincuencia, a partir de la información obtenida en el trabajo de campo (Bonilla y López, 2016), como se observa en la tabla 1.

La segunda fase, entendida como codificación selectiva, se centra en el análisis minucioso de la información recopilada utilizando las técnicas de recolección de datos previamente establecidas para la investigación. En este caso se utilizaron dos métodos principales: entrevistas en profundidad y análisis de información científica.

Tabla 1. | Codificación abierta

Ámbito temático	Objetivo general	Objetivos específicos	Categorías	Subcategorías
Ciberdelincuente	Describir al ciberdelincuente mediante el análisis de sus principales características, teorías y aspectos relevantes de los delitos informáticos, con el fin de contribuir a las estrategias institucionales de seguridad y prevención.	Hacer una revisión teórica para la comprensión del delincuente informático.	Ciberdelito	Tácticas Información
		Identificar las tipologías más recurrentes, factores y características de los delitos informáticos.	Características del ciberdelincuente	Conducta delictiva *Modus operandi*
		Formular pautas de comprensión y análisis sobre los delincuentes informáticos.	Control social	Integración social Herramientas de control

Nota: en la fase 1 se generó la hoja de ruta de la codificación de la información recolectada durante el trabajo de campo, lo cual permitió orientar el proceso de análisis frente al desarrollo de los insumos de información obtenidos de la entrevista en profundidad y de la revisión de documentos científicos.

Durante las entrevistas en profundidad se tuvo la oportunidad de interactuar directamente con personas relacionadas con el tema de estudio, como expertos, profesionales y posibles víctimas de ciberdelincuencia. Estas entrevistas permitieron obtener información valiosa y perspectivas únicas sobre el fenómeno de la ciberdelincuencia. Las transcripciones de estas entrevistas fueron posteriormente analizadas en detalle para extraer patrones, ideas clave y tendencias relevantes.

Por otro lado, el análisis de información científica consistió en examinar estudios y publicaciones académicas previas relacionadas con la ciberdelincuencia. Esto incluyó la revisión de artículos, informes, estadísticas y otros recursos científicos que proporcionaron una base sólida de conocimiento teórico sobre el tema.

En esta fase de codificación selectiva se aplicaron técnicas de interpretación semántica siguiendo los principios de la hermenéutica. Esto implica analizar cuidadosamente el contenido de cada transcripción de entrevista para identificar significados ocultos, interpretar las expresiones y comprender el contexto en el que se desarrollaron las conversaciones. Este enfoque permitió una comprensión más profunda y completa de las perspectivas y experiencias compartidas por los participantes en las entrevistas. Así se observa en la tabla 2.

Tabla 2. | Resumen de codificación selectiva

Categoría 1: Ciberdelito					
Exp	**P1C1**	**P2C1**	**P3C1**	**P4C1**	**P5C1**
19	Conjunto de tácticas con fines maliciosos que se llevan a cabo por medio de ordenadores y redes.	Modalidades como la ingeniería social, la anonimización, la inteligencia artificial, el criptoactivo, el cifrado y la criptografía a la inversa.	Estafas con medios digitales, portales falsos, falsos productos, falsas ofertas de trabajo.	La falsificación informática, el fraude informático, como la modalidad más común.	Se desarrolla a través del teléfono celular, aplicaciones de mensajería instantánea, plataformas de videoconferencia, correo electrónico y redes sociales.
Categoría 2: Características del ciberdelincuente					
Exp	**P1C2**	**P2C2**	**P3C3**	**P4C4**	**P5C5**
19	Conocimientos avanzados en sistemas.	En la mayoría de los casos los ciberdelincuentes utilizan un perfil falso.	Delitos que atentan contra la propiedad intelectual (piratería), la tranquilidad y la libertad (amenazas, injurias, calumnias, ciberacoso o *ciberbullying* y ciberacecho o *ciberstalking),* la intimidad (descubrimiento y revelación de secretos) y la indemnidad sexual.	Características como ciberexitoso y ciberejecutor.	Habilidades para el desarrollo de códigos fuente y explotación de vulnerabilidades, conocimiento amplio del medio digital con el cual van a cometer la estafa, fraude o crimen.
Categoría 3: Control social					
Exp	**P1C3**	**P2C3**	**P3C3**	**P4C3**	**P5C3**
19	Crear conciencia y responsabilidad en la utilización de redes sociales y medios informáticos (85 %); la creación de nuevas herramientas tecnológicas al servicio de las instituciones de seguridad.	La identificación de *softwares* maliciosos es una medida efectiva, ya que cuando se identifican se pueden controlar.	Las técnicas requieren actualización y fortalecimiento permanente.	La protección de la evidencia digital, la concientización, el *hardening*, el *ethical hacking*, *bug bounty*.	Las instituciones de seguridad que van un paso adelante de los ciberdelincuentes.

Nota: para representar esta fase, se elaboró un resumen general de las respuestas que hacen parte del formato de la entrevista semiestructurada aplicada en el trabajo de campo a expertos de la DIJIN.

La tercera fase es la de codificación, la cual implica alcanzar la saturación teórica. En esta fase se recolecta y analiza una cantidad suficiente de datos para poder explicar el tema en estudio y responder a las preguntas o problemas de investigación planteados. Para lograr esto, se utilizaron herramientas de análisis que permiten organizar y examinar los datos de manera estructurada. Una de estas herramientas es la matriz de doble entrada, la cual se utiliza para clasificar y relacionar los distintos elementos identificados en el estudio.

La recolección de datos en esta fase se realizó a través de diversas fuentes, como entrevistas, encuestas, revisión de documentos y análisis de casos, entre otros. Estos datos se sometieron a un análisis minucioso, en el cual se buscaron patrones, conexiones y tendencias significativas. El objetivo principal de esta fase fue lograr una comprensión profunda y completa del tema de investigación; se obtuvieron respuestas claras y fundamentadas a las preguntas planteadas. La saturación teórica se alcanza cuando se ha recopilado y analizado suficiente información para construir una explicación sólida y respaldada por evidencia sobre el tema en estudio, tal como se determina en la tabla 3.

Tabla 3. | Resumen de codificación teórica

Categoría 1: Ciberdelito			
Exp	**PTCT**	**Fundamento teórico**	**Teorización**
19	• Conjunto de tácticas con fines maliciosos que se llevan a cabo por medio de ordenadores y redes. • Modalidades como la ingeniería social, la anonimización, la inteligencia artificial, el criptoactivo, el cifrado y la criptografía a la inversa. • Estafas con medios digitales, portales falsos, falsos productos, falsas ofertas de trabajo. • La falsificación informática, el fraude informático, como la modalidad más común. • Se desarrolla a través del teléfono celular, aplicaciones de mensajería instantánea, plataformas de videoconferencia, correo electrónico y redes sociales.	Escenarios: los modos y formas y los delitos asociados con los cuales se pueden tipificar y sancionar este tipo de delitos (Shick y Toro, 2017).	Cúmulo de tácticas que tienen fines delincuenciales por medio de redes informáticas que permiten su desarrollo en el ciberespacio.
Categoría 2: Características del ciberdelincuente			
Exp	**PTCT**	**Fundamento teórico**	**Teorización**
19	• Conocimientos avanzados en sistemas. • En la mayoría de los casos los ciberdelincuentes utilizan un perfil falso. • Delitos que atentan contra la propiedad intelectual (piratería), la tranquilidad y la libertad (amenazas, injurias, calumnias, ciberacoso o *ciberbullying* y ciberacecho o *ciberstalking*), la intimidad (descubrimiento y revelación de secretos) y la indemnidad sexual. • Características como ciberexitoso y ciberejecutor. • Habilidades para el desarrollo de códigos fuente y explotación de vulnerabilidades, conocimiento amplio del medio digital con el cual van a cometer la estafa, fraude o crimen.	La teoría del *big five* o mejor conocida como el modelo de los cinco factores, mediante el cual se establece en qué grado están arraigadas, o no, cinco dimensiones básicas de la personalidad que pueden conducir a este tipo de inclinación delictual (Sánchez y Robles, 2013).	Las características del ciberdelincuente tienen su fundamento en la teoría del *big five*, que se relaciona con la falta de empatía emocional, la falta de escrúpulos, incapacidad para el control de emociones, la confianza para llevar a cabo el delito y la capacidad de innovar sus *modus operandi*.

(*Continúa*)

Categoría 3: Control social			
Exp	**PTCT**	**Fundamento teórico**	**Teorización**
19	• Crear conciencia y responsabilidad en la utilización de redes sociales y medios informáticos (85 %); la creación de nuevas herramientas tecnológicas al servicio de las instituciones de seguridad. • La identificación de *softwares* maliciosos es una medida efectiva, ya que cuando se identifican se pueden controlar. • Las técnicas requieren actualización y fortalecimiento permanente. • La protección de la evidencia digital, la concientización, el *hardening*, el *ethical hacking*, *bug bounty*. • Las instituciones de seguridad que van un paso adelante de los ciberdelincuentes.	El control social del ciberdelito se relaciona con un proceso de integración social propio de la criminología, consistente en la generación de estrategias de control que se destinan a regular la conducta de los individuos, promover la estabilidad de los grupos sociales y la garantía del orden social (González, 2010).	Proceso de integración social en el cual confluyen estrategias encaminadas a la anticipación, prevención y contención del ciberdelito.

Nota: para efectos de representatividad de esta fase, se elaboró un resumen de la triangulación de resultados y de lecturas especializadas.

Resultados

A continuación se presenta el análisis correspondiente a la triangulación de información procedente de la contrastación del marco referencial con los resultados obtenidos en las entrevistas en profundidad, los cuales guardan relación con los objetivos específicos que dieron vida al proyecto de investigación que sirve de soporte científico del presente artículo. En general, esta información permite responder la pregunta problema de la investigación a partir de los factores y características relevantes que permiten describir al ciberdelincuente y algunas recomendaciones que podrían prever y contener el crecimiento del ciberdelito.

Aproximación teórica a la comprensión del ciberdelincuente

Según la información común más importante de los entrevistados, como se ilustra en la tabla 3, se puede establecer que una definición apropiada para el ciberdelito tiene relación con las actividades ilícitas que suceden a través de las TIC con el desarrollo de modalidades como el fraude informático, la ingeniería social, la anonimización, la inteligencia artificial, el criptoactivo, el cifrado y la criptografía a la inversa, que afectan el *habeas data* y la disposición de la información de ciudadanos y gremios empresariales, que pueden ser tipificados para las debidas sanciones desde la legislación nacional e internacional, al clasificarlas por el escenario en que tienen lugar, las formas de presentación y los delitos conexos.

Como complemento de lo anterior, un primer acercamiento al ciberdelito en Colombia se fundamenta en el tipo de tecnología, como lo expone el Centro Cibernético Policial (2021), a través del cual se determinan las TIC como su plataforma de desarrollo. Es de resaltar que el ciberdelito *per se* contiene multiplicidad de aristas que tienen su base de desarrollo en el mundo digital, bien sea porque implica desarrollos tecnológicos que conducen a la apertura informática o porque la ampliación de los sitios web permite que existan *softwares* malintencionados que estén en constante relacionamiento con los usuarios de este tipo de tecnología. A la luz de los anteriores argumentos y al revisar las diferentes posturas teóricas frente a la definición del término ciberdelito, existen tres características de este a la hora de revisar su definición, que, aunque presentan acercamientos diferentes al abordarlo, tienen un punto en común: el intangible "información" (Shick y Toro, 2017).

Otro aspecto para rescatar, según la información más relevante expuesta en la tabla 3, tiene relación con los elementos del ciberdelito; es común encontrar como principal activo la información porque alrededor de ella se hacen evidentes modalidades como la ingeniería social, la anonimización, la inteligencia artificial, el criptoactivo, el cifrado y la criptografía a la inversa. Así las cosas, como lo expresa Posada Maya (2017) en su teoría de la tipicidad, la ciberdelincuencia se hace explícita con el uso de la información desde diferentes modalidades, lo que permite determinar el tipo de infracción que puede contener el delito, el cual comprende desde el *habeas data* hasta la disposición de la información que conduce al funcionamiento de la sociedad en términos generales, y de los individuos que forman parte de ella desde la particularidad.

Implicaciones del control social frente al ciberdelito

Al respecto, se puede establecer que el control social en el desarrollo del ciberdelito tiene lugar cuando se dan las condiciones propicias o los controles para que las diferentes modalidades que caracterizan este delito tengan lugar (González, 2010). De esta manera, a continuación, se describen aquellos aspectos formales e informales que desde la teoría pueden limitar su materialización y los aspectos validadores que los expertos consultados consideran propicios para su contención.

Así, desde la perspectiva formal de González (2010), el control social del ciberdelito se relaciona con un proceso de integración social propio de la criminología, consistente en la generación de estrategias de control que se destinan a regular la conducta de los individuos, promover la estabilidad de los grupos sociales y la garantía del orden social desde la aplicación de recursos de coerción y persuasión; se puede afirmar que en la entrevista se afirma que la aplicación de las leyes del contexto colombiano: 1273 de 2009 (con relación a la protección de información y datos) y 1266 de 2008 (sobre *habeas data* y manejo de información), respectivamente, junto con el Convenio de Budapest (marco internacional de escenarios, modos, formas y delitos asociados para sancionar y tipificar en el ciber espacio), tienen un limitado alcance con relación a la evolución del ciberdelito y sus tipologías de carácter cambiante, tal y como lo señala la teoría de la cibercriminología en general (Shick y Toro, 2017).

Y desde la perspectiva informal, como lo determina López (2015), la oportunidad se convierte en el eje central de los motivos que conducen a cometer un delito y que a su vez limitan los motivos para regularla; además, los vínculos que se establecen entre el control social y el delincuente se fundamentan en cuatro aspectos de importancia: (a) la interacción convencional con personas o instituciones; (b) por relacionamiento; (c) por vinculación en actividades cotidianas y rutinarias, y (d) por el valor moral de las reglas sociales.

Lo anterior se sustenta con la generación de conciencia y responsabilidad en la utilización de redes sociales y medios informáticos; la creación de nuevas herramientas tecnológicas al servicio de las instituciones de seguridad que van un paso adelante de los ciberdelincuentes; la identificación de *softwares* maliciosos es una medida efectiva, ya que cuando se detectan se pueden controlar. Y la investigación, la protección de la evidencia digital, la concientización, el *hardening*, el *ethical hacking*, *bug bounty* –si se evalúa a nivel macro si han sido efectivas, no se han tenido ciberataques de gran magnitud; si se evalúa a nivel micro, se tienen muchas víctimas–, todas las técnicas requieren actualización y fortalecimiento permanente, como se expone en la tabla 2.

La identificación de acciones que contribuyan a la anticipación y prevención del ciberdelito se convierte en uno de los aspectos de interés para las instituciones de seguridad que tienen por finalidad el monitoreo y neutralización definitiva de las organizaciones que se dedican a este tipo de delito. Para los expertos, esto permite fortalecer los protocolos de seguridad de la información.

Conclusiones

Las conclusiones que se describen a continuación se derivan de la contrastación de los resultados obtenidos en el trabajo de campo y los documentos científicos consultados, los cuales responden a cada uno de los objetivos específicos planteados para responder al vacío de información correspondiente a las características relevantes que definen el ciberdelincuente y la manera como se podría prever y contener el crecimiento del ciberdelito.

Definición del ciberdelito

El *ciberdelito* se define como el cúmulo de tácticas que tienen fines delincuenciales por medio de redes informáticas que permiten su desarrollo en el ciberespacio a través del teléfono celular, aplicaciones de mensajería instantánea, plataformas de videoconferencia, correo electrónico y redes sociales, así como bombas lógicas (*logic bombs*), gusanos y virus informáticos, entre otros, tal como lo ilustra la tabla 2.

También es importante resaltar que el principal activo de este concepto es la información, porque a su alrededor se hacen evidentes modalidades como la ingeniería social, la anonimización, la inteligencia artificial, el criptoactivo, el cifrado y la criptografía a la inversa. También, la falsificación informática, el fraude informático –como la modalidad más común– y como delito con mayor afluencia se encuentra la pornografía infantil, según la tabla 2.

Este tipo de ciberdelitos tiene lugar a partir de acciones que se presentan en el ciber espacio, que tienen que ver con la pesca de información a partir de la generación de señuelos informativos que orientan al engaño de las personas, según se ilustra en la tabla 2.

Finalmente, desde el punto de vista legal, como lo exponen Shick Choi y Toro Álvarez (2017), al revisar el Convenio de Budapest en tres de sus títulos, en los

que se describen los escenarios, los modos y formas y los delitos asociados con los cuales se puede tipificar y sancionar este tipo de delitos, se coincide con lo expresado en la Ley 1273 de 2009, que identifica los malos usos de los sistemas y datos informáticos que pueden desembocar en obstaculizaciones, interceptaciones y daños generalizados, dirigidos a ocasionar incidentes de victimización de los usuarios y así fomentar la protección general de toda la información por parte de la norma, que vela por ofrecer seguridad a partir de su conceptualización e implementación a nivel nacional: todas estas medidas son necesarias para el combate del ciberdelito y deben estar en constante mejora y actualización para lograr este propósito.

El ciberdelincuente

En definitiva, se puede establecer que las características del ciberdelincuente tienen su fundamento en la teoría del *big five*, que se relaciona con la falta de empatía emocional, la falta de escrúpulos, incapacidad para el control de emociones, la confianza para llevar a cabo el delito y la capacidad de innovar sus *modus operandi* (Sánchez y Robles, 2013).

El *big five* de la conducta delictiva se caracteriza por *la energía*, entendida como la confianza que denota el delincuente para llevar a cabo la actividad delictiva por su manejo interpersonal de las relaciones que establece con sus víctimas; *la afabilidad*, que puede ser interpretada por la falta de empatía emocional ante el sufrimiento de sus víctimas o de las personas que llegan a ser parte de sus actividades extorsivas; *el tesón* se relaciona con la perseverancia y la falta de escrúpulos para llevar hasta el final las metas que se propone ante cada actividad delincuencial; *la estabilidad emocional*, lo que comprende la incapacidad para controlar los efectos negativos de la ansiedad, de la depresión, de la irritabilidad y de la frustración y la apertura mental, o que se refiere a la capacidad de generar ideas que favorezcan su *modus operandi* y a la falta de valores y de sentimientos que le permitan tener conciencia de las acciones que realiza y de las consecuencias que puede tener contra los demás (Sánchez y Robles, 2013).

También, desde las entrevistas, el ciberdelincuente se destaca por reunir una serie de comportamientos guiados hacia el desarrollo de códigos fuente y amplio conocimiento del medio digital, su capacidad de involucrar a poblaciones menos favorecidas por su poco conocimiento en el manejo de las redes sociales y los medios tecnológicos y su alto nivel de profesionalización y adaptación tecnológica, con características de ciberexitoso y ciberejecutor, es decir, orientación al logro de objetivos a partir de la experticia, según la tabla 2.

El control social

Desde el *control social*, entendido como un proceso de integración social en el cual confluyen estrategias encaminadas a la anticipación, prevención y contención del ciberdelito (González, 2010), es preciso enfatizar que sus preceptos están enfocados en la regulación de la conducta de los individuos y la estabilidad de la sociedad en general, desde la formulación de legislaciones o normas justas y equiparables a la gravedad de los delitos.

Las estrategias de control que se realizan con las víctimas, como se cita a continuación: crear conciencia y responsabilidad en la utilización de redes sociales y medios informáticos, la creación de nuevas herramientas tecnológicas al servicio de las instituciones de seguridad que van un paso adelante de los ciberdelincuentes. La identificación de *softwares* maliciosos es una medida efectiva, ya que cuando se identifican se pueden controlar, tal como se evidencia en la tabla 2.

Y la investigación, la protección de la evidencia digital, la concientización, el *hardening*, el *ethical hacking*, *bug bounty* –si se evalúa a nivel macro si han sido efectivas, no se han tenido ciberataques de gran magnitud; si se evalúa a nivel micro, se tienen muchas víctimas–, todas las técnicas requieren actualización y fortalecimiento permanente, según la tabla 3.

Recomendaciones

Por lo anterior, surge como principal recomendación el desarrollo de soluciones tecnológicas que permitan crear redes informáticas que contengan el despliegue de *softwares* maliciosos, como lo propone Osorio Sierra (2020), y que tienen relación con la generación de acciones que reduzcan riesgos con actividades preventivas que se derivan de una adecuada arquitectura de seguridad, la definición de una segmentación en red y los controles con funciones preventivas y correctivas, como los *firewalls* y los sistemas de detección de intrusos. Desde la perspectiva de los expertos, lo anterior evita abrir o ingresar a enlaces desconocidos y de dudosa procedencia, para no ser víctima de estos ciberdelincuentes y que tengan dominio de sus datos personales; también se deben aplicar las prácticas preventivas y reactivas, así como las políticas públicas digitales (CONPES).

Una segunda acción se fundamenta en la creación de servidores, estaciones y almacenamiento direccionados a los usuarios y sus puntos de trabajo o de acceso a la red, así como servidores y redes de almacenamiento que permitan el análisis de comportamiento de usuario (UBA), bloqueos de la reproducción automática de

medios extraíbles y el cifrado de archivos y prevención de pérdida de datos (DLP): los entrevistados señalan la necesidad de generar estrategias de comunicación orientadas a fomentar en el personal un compromiso en la implementación de todas estas medidas.

La tercera acción contempla las aplicaciones (en todas sus versiones) y los servicios informáticos para la predicción por aprendizaje de máquina, listas blancas o negras de todas las aplicaciones, bloquear ventanas emergentes o *pop-ups* y deshabilitar macros. Lo anterior es validado por los expertos al referirse al diseño de modelos de prevención basados en evidencia científica mediante segmentación por clase de victimización. No todos los ciberdelitos crecieron durante la pandemia; de tal manera que no se puede establecer una respuesta estándar, según la categoría de control social expuesta en la tabla 2.

Un último aspecto para resaltar por parte de los expertos es la creación de las unidades de trabajo coordinado de atención de los ciberdelitos, como es el caso de la integración de funciones del Centro Cibernético Policial (CECIP), de las unidades de especialidades de la Fiscalía designadas para dicho fin y de Interpol y Europol, para robustecer las herramientas de ciberseguridad.

Conflicto de interés

No se presentó conflicto de interés entre los autores de la presente investigación académica. Declaramos que no tenemos ninguna relación financiera o personal que pudiera influir en la interpretación y publicación de los resultados obtenidos. Asimismo, aseguramos cumplir con las normas éticas y de integridad científica en todo momento, de acuerdo con las directrices establecidas por la comunidad académica y las dictaminadas por la presente revista.

Referencias

Aguirre, J., y Jaramillo, L. (2012). Aportes del método fenomenológico a la investigación educativa. *Revista Latinoamericana de Estudios Educativos, 2*(8), 51-74. https://www.redalyc.org/articulo.oa?id=134129257004

Arrieta, H. (2016). El análisis gramatical de tipo penal. *Justicia*, (29), 53-71.

Asociación Colombiana de Ingenieros de Sistemas (2020, 2 de junio). *Un 600 % han aumentado los ciberdelitos en pandemia, ¡asegúrese para iniciar el 2021!* https://shre.ink/2vFU

Bonilla, M., y López, A. *(2016).* Ejemplificación del proceso metodológico de la teoría fundamentada. *SConta de Moebio, (57).* https://doi.org/10.4067/S0717-554X2016000300006

Cámara, S. (2020). La cibercriminalidad y el perfil del ciberdelincuente. *Derecho y Cambio Social*, (60), 412-520.

Centro Cibernético Policial. (2021, 11 de octubre). *Estadística de incidentes informáticos.* https://caivirtual.policia.gov.co/

Congreso de la República de Colombia. (2009, 5 de enero). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial* 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia (2008, 31 de diciembre). Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. *Diario Oficial* 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Cortés, M., Mur, N., Iglesias, M., y Cortés, M. (2020). Algunas consideraciones para el cálculo del tamaño muestral en investigaciones de las Ciencias Médicas. *MediSur, 18*(5), 937-942.

Fiscalía General de la Nación (2020, 10 de diciembre). Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020. *Portafolio.* https://shre.ink/lsd9

González, M. (2010). *El control social desde la criminología.* Feijóo.

Hernández, R. (2020). Research Methods for the Study of Small and Medium-Sized Enterprises. En *Handbook of Research of Increasing the Competitiviness os SMEs* (pp. 125-151). IGIGlobal, 1-20.

López, R. (2015, 6 de julio). *Teorías del control social*. Crimipedia. https://shre.ink/lsdD

Maza, P. (2021, 14 de enero). ¿Cómo es el delincuente informático? Delitos informáticos. https://shre.ink/lsdd

Miranda, S. y Ortiz, J. (2020). Los paradigmas de la investigación: un acercamiento teórico para reflexionar desde el campo de la investigación educativa. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *11*(21),1-18.

Miró. (2011). La oportunidad criminal en el ciberespacio-aplicación y desarrollo de la teoría de las actividades cotidianaspara la prevención del cibercrimen. *Revista electrónica de ciencia penal y criminología, 13* (07), 1-55.

Moreno, R. (2017). Hermenéutica y ciencias sociales: a propósito del vínculo entre la interpretación de la narración de Paul Ricoeur y el enfoque de investigación biográfico-narrativo. *Análisis*, *49*(90), 205-228.

Morguen, N., Castellaro, M. y Peralta, N. (2019). Modalidades de razonamiento en díadas durante la resolución de problemas lógicos. *Psicogente, 23*(43), 17-42. https://doi.org/10.17081/psico.23.43.3092

Mucha, L. y Chamorro, R. (2021). Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado. *Desafíos, 12*(1), 44-51.

Norza, E. y Vargas, N. (2016). Perfilación criminológica: estado del arte en una muestra de instituciones académicas en Colombia. *Psicología desde el Caribe, 33*(2), 206-222.

Osorio Sierra, A. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías, 19*(3), 131-142.

Portal Sistemius. (2020, 24 de abril). Ciberdelincuencia: los 4 delitos informáticos más comunes. Sistemius. https://shre.ink/lsvR

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad. *Revista Nuevo Foro, 13*(88), 72-112.

Quintana, L. y Hermida, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Perspectivas en Psicología: Revista de Psicología y Ciencias Afines, 16*(2), 73-80.

Restrepo, J. y Cotrina, Y. (2020). Participación ciudadana en el sistema de seguridad social en salud en Colombia. *Revista de Ciencias Sociales, 25*(2), 230-239.

Sánchez, D. y Robles, M. (2013). El modelo "Big Five" de personalidad y conducta delictiva. *International Journal of Psychlogical Research*, *6*(1), 102-109.

Shick Choi, K. y Toro Álvarez, M. M. (2017). *Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital.* Universidad Antonio Nariño.

Sordini, M. (2019). La entrevista en profundidad en el ámbito de la gestión pública. *Reflexiones, 98*(1), 75-88.

Southby, C. y Cooke, A. (2019). It´s now or never -nulliparous women's experiences of pregnancy at advanced maternal age: a grounded theory study. *Midwifery, 68*, 1-8.

Tanque de Análisis y Creatividad de las TIC. (2019, 29 de octubre). *Tendencias del cibercrimen en Colombia 2019-2020.* Cámara Colombiana de Informática y Telecomunicaciones. https://shre.ink/lsvX

UNIR. (2021, 6 de mayo). Ciberdelincuencia: ¿qué es y cuáles son los ciberdelitos más comunes? UNIR. https://mexico.unir.net/ingenieria/noticias/que-es-ciberdelincuencia/

Villasís, M. Á., Rendón, M. E., García, H., Miranda, M. G. y Escamilla, A. (2020). La revisión sistemática y el metaanálisis como herramientas de apoyo para la clínica y la investigación. *Revista Alergia México, 67*(1), 50-62.