UNIVERSIDAD SIGLO 21

La educación evoluciona

TRABAJO FINAL DE LA CARRERA DE ESPECIALIZACIÓN EN CIBERCRIMEN

EL CIBERCRIMEN EN LA INVESTIGACIÓN PENAL PREPARATORIA

Principales Obstáculos para llegar a una Imputación en Casos de Cibercrimen en el Sur de la Provincia de Córdoba, Argentina

AUTOR:

Julián Testa

2023

NOTA DE CONFIDENCIALIDAD

La información contenida en el presente trabajo, especialmente la utilizada en el planteamiento del problema, proveniente de datos estadísticos de una Unidad Judicial de la provincia de Córdoba, si bien es de acceso público según lo estipulado por la ley nacional n° 27.275 y ley de la provincia de Córdoba n° 8.803 (no aportándose aquí datos privados de personas, ni encontrándose la información utilizada dentro de las excepciones a la publicidad de la información pública contenidas en ambas legislaciones), es de uso exclusivo para este trabajo de investigación y únicamente con fines académicos y no de divulgación de ninguna especie. Queda por tanto reservada la publicación de este trabajo a la expresa conformidad de su autor, debiendo permanecer el mismo accesible solo al tribunal evaluador de tesis y otras autoridades universitarias vinculadas con dicho proceso. No se autoriza la publicación, total o parcial, del presente trabajo, en ninguna plataforma de acceso público ni privado, así como tampoco la difusión de su contenido por cualquier medio, sin expresa autorización del autor.

RESUMEN

Un relevamiento estadístico realizado a partir de datos consignados en el Libro de Sumarios de la Unidad Judicial N° 3 de la ciudad de Río Cuarto correspondiente al periodo 2021-2023 (julio), arrojó como diagnóstico que a pesar de estar identificados los autores de diferentes tipos de ciberdelitos, solo 2 resultaron imputados. Este dato motivó la necesidad de investigar cuáles son las causas y obstáculos que enfrentan en esta Unidad Judicial para el proceso de Investigación Penal Probatoria en los casos de cibercrimen. Para ello se desarrolla un análisis cuantitativo a partir de encuestas a una muestra conformada por 20 representantes claves que incluyen: miembros del Ministerio Público Fiscal (funcionarios, secretarios, prosecretarios, ayudantes fiscales y fiscales); representantes de áreas jurisdiccionales (Cámaras del Crimen, Juzgado de Control de Garantías); policías de investigaciones y técnicos informáticos del Poder Judicial.

Las principales conclusiones de este trabajo muestran que existe una combinación de circunstancias que contribuyen negativamente a la efectiva imputación de los delitos, como la escasez de personal, la insuficiente capacitación específica en investigaciones de cibercrimen, la centralización de recursos investigativos científico/técnicos en la ciudad de Córdoba y que el marco normativo – tanto nacional como provincial – resulta insuficiente para dar respuesta a estas modalidades delictivas.

ABSTRACT

A statistical survey carried out from data recorded in the Summary Book of the Judicial Unit No. 3 of the city of Río Cuarto corresponding to the period 2021-2023 (July), showed as a diagnosis that despite the authors of different types of cybercrimes being identified, only 2 were charged. This data motivated the need to investigate what are the causes and obstacles faced in this Judicial Unit for the process of Evidentiary Criminal Investigation in cases of cybercrime. A quantitative analysis is developed based on surveys of a sample made up of 20 key representatives that include: members of the Public Prosecutor's Office (officials, secretaries, pro-secretaries, assistant prosecutors and prosecutors); representatives of jurisdictional areas (Chambers of Crime, Court of Control of Guarantees); investigative police and computer technicians of the Judiciary.

The main conclusions of this work show that there is a combination of circumstances that contribute negatively to the effective imputation of crimes, such as the shortage of personnel, insufficient specific training in cybercrime investigations, the centralization of scientific/technical investigative resources in the city of Córdoba and that the regulatory framework – both national and provincial – is insufficient to respond to these criminal modalities.

TABLA DE CONTENIDO

Índice de Tablas

Índice de Figuras

1. INTRODUCCIÓN

El uso de las nuevas tecnologías provoco la emergencia de nuevas modalidades delictivas que desafían las capacidades de los distintos miembros que conducen una investigación judicial. El cibercrimen es una de estas nuevas modalidades delictivas, y se refiere a aquellos delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo (por ejemplo: smartphone, pendrive, tablet, etc.). Las mismas características de este tipo de delitos presentan algunas dificultades para la investigación penal probatoria. La primera de ellas es que la evolución de estos hechos delictivos se produce de manera constante y acelerada, siguiendo el ritmo y aprovechando las nuevas oportunidades que ofrece la propia evolución tecnológica. En palabras de Borzi Cirilli (2018):

> (…) nos encontramos con nuevas modalidades investigativas que se van creando y adaptando a modo de espejo con las modalidades delictivas; lamentablemente, esta circunstancia hace que aquellas siempre vayan detrás de estas. Es así como ahora las tareas de inteligencia habituales en cualquier investigación se traducen en "ciberpatrullajes" y nos encontramos ante la necesidad de identificar computadoras, celulares e inspeccionar smartphones, entre otros dispositivos en constante evolución y cambio (p.176).

Otra dificultad es que este tipo de delitos ocurren en un "lugar" o ámbito deslocalizado como el ciberespacio (Miró Llinares, 2012), que se constituye en un primer obstáculo que deben afrontar los investigadores en cibercrimen cuando deben ocuparse de delitos en los cuales existe una multiplicidad de jurisdicciones por la propia naturaleza de internet. De esta manera, si un operador judicial debe validar una información generada en otro país, debe esperar una resolución internacional que demora la investigación judicial (Justo, 2017).

Otra dificultad la constituyen los problemas probatorios de criminalidad informática, con grandes inconvenientes en torno a la debida acreditación de los tipos subjetivos, ya que el ciberespacio puede ser considerado como un "no lugar", en términos del antropólogo Marc Augé (1993), es decir, un espacio donde el ser humano permanece anónimo. A esto se suman otras dificultades como la conservación de la evidencia digital, el inadecuado precinto de celulares o la falta de preservación de otras pruebas digitales

por falta de copias adecuadas, entre otros problemas para construir una imputación o, por el contrario, contrarrestar una acusación mediante contrapruebas (Borzi Cirilli, 2018).

Estos aspectos ponen en evidencia la necesidad de contar con recursos técnicos y una legislación adecuada. Justo (2017) señala que para desarrollar investigaciones sobre cibercrimen más exitosas es necesario incorporar mejores herramientas judiciales y procesales que permitan proveer al perito de los elementos necesarios para que luego el operador judicial haga la valoración final de toda la actividad de investigación técnica. Por otra parte, Justo (2017) también advierte que la escasa interacción entre los operadores judiciales, los investigadores y los peritos dificulta la tarea de investigación, que además se ve comprometida por la falta de recursos para el investigador.

Los conocimientos y experiencia técnica son una condición necesaria pero no suficiente para un eficaz desempeño de los diferentes actores que intervienen en el proceso de investigación probatoria de la criminalidad informática, en un campo cada vez más específico y especializado, donde la necesidad de expertos concretos crece cada día, así como también la necesidad de capacitación y formación específica en el tratamiento de evidencia digital y en los aspectos legales y procesales vinculados.

Arce et al (2011) advierten que:

> (…) el avance tecnológico hace que los instrumentales técnicos queden obsoletos con el corto paso del tiempo. Se debe tratar de contar con herramientas que cubran la mayor parte del espectro de casos conocidos y posibles, como así también la constante capacitación del personal técnico. Lo que no nos exime de tener que comprar instrumental específico para una causa en particular en situaciones extraordinarias. (p.9).

Estas dificultades que se plantean desde la literatura revisada se confirman en la realidad. Un relevamiento estadístico realizado a partir de datos consignados en el Libro de Sumarios de la Unidad Judicial N° 3 de la ciudad de Río Cuarto correspondiente al periodo 2021-2023 (julio), arrojó como diagnóstico que a pesar de estar identificados los autores de diferentes tipos de ciberdelitos, solo 2 resultaron imputados. Este dato motivó la necesidad de investigar cuáles son las causas y obstáculos que enfrentan en esta Unidad Judicial para el proceso de Investigación Penal Probatoria en los casos de cibercrimen. Para ello se desarrolla un análisis cuantitativo a partir de información proporcionada por

representantes claves que incluyen: miembros del Ministerio Público Fiscal (funcionarios, secretarios, prosecretarios, ayudantes fiscales y fiscales); representantes de áreas jurisdiccionales (Cámaras del Crimen, Juzgado de Control de Garantías); policías de investigaciones y técnicos informáticos del Poder Judicial.

1.1. Planteamiento del Problema

1.1.1. Contexto

Para comprender mejor el problema de investigación es necesario presentar el contexto en el que se desarrolla. Así, nos remitimos en primer lugar, al ámbito del Ministerio Público Fiscal que tiene a su cargo la investigación de los delitos y la promoción de la acción penal pública contra los autores o partícipes. Le corresponde la carga de la prueba y debe probar en el juicio oral y público los hechos que fundamenten su acusación. La distribución de las funciones de los miembros del Ministerio Público Fiscal se realiza de conformidad a las normas que regulan su ejercicio, procurando la especialización de la investigación y persecución penal mediante fiscalías temáticas. En la Figura 1 se presenta el organigrama del Ministerio Público Fiscal de la provincia de Córdoba.

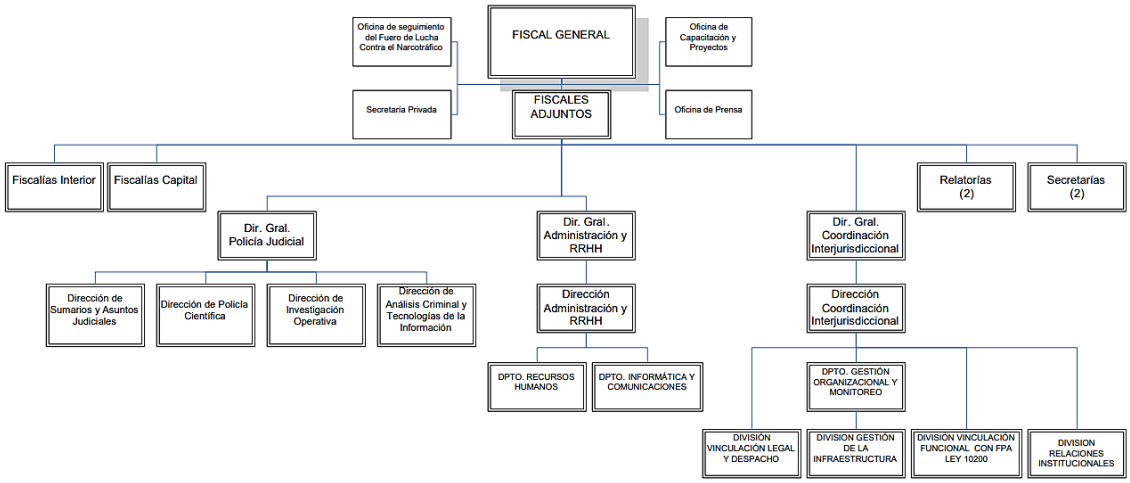


Figura 1. Organigrama del Ministerio Público Fiscal de la provincia de Córdoba.

Fuente: https://www.justiciacordoba.gob.ar/transparencia/pdf/personal/Organigramas%20Poder%20Judicial.pdf.

De la Fiscalía General depende, entre otras, la Dirección General de Policía Judicial, que se encarga de las tareas técnico/científicas, y es considerada como una de las más completas de Argentina, tanto a nivel técnico como de recursos humanos, con

sede central en Córdoba Capital. Esta Policía Judicial que pertenece al Ministerio Público Fiscal y por ende, está dentro de la esfera del Poder Judicial de la provincia, cuenta con:

- un área de Cibercrimen, que tramita intervenciones a páginas webs, perfiles de redes sociales, etc. a solicitud judicial, a través de un convenio con las distintas empresas prestadoras de telefonía o internet del país, así como con las propias empresas que brindan los servicios de redes sociales (Facebook, WhatsApp, etc.) con sede mayormente en Estados Unidos. La escasez de personal y la necesidad de tramitar todos los pedidos que se hacen desde toda la provincia claramente deja en evidencia que la capacidad de procesamiento en esta área es muy acotada, debiendo hacerlo únicamente en causas de gravedad (delitos contra la integridad sexual, secuestros extorsivos, homicidios, desapariciones de personas, etc.).
- una sección de Tecnología Forense que se dedica a la apertura de elementos tecnológicos secuestrados para analizar su contenido. La demora estimada para procesar un celular o una computadora que se le envíen para su apertura es de aproximadamente un año y medio, siempre y cuando se justifique esta apertura en función de la gravedad de la causa.
- una sección de Análisis de las Telecomunicaciones cuya función es tramitar con las distintas empresas de telefonía del país las solicitudes que se hagan, en el marco de una investigación, de sábanas telefónicas, titularidades de líneas, antenas de telefonía celular que captan llamadas, etc. La demora en dar respuesta de esta oficina depende de cuánto demore en contestar la empresa prestataria del servicio, pero suele variar entre uno y cuatro meses.

En la ciudad de Río Cuarto, pero con competencia en todo el sur de la provincia de Córdoba, existe una delegación de la Dirección General de Policía Judicial, cuya función está destinada a trabajar en el lugar del hecho ante delitos contra las personas y/o contra la propiedad. Es pertinente aclarar que no hay personal ni equipamiento destinado a la investigación de Ciberdelitos en el ámbito de la ciudad de Río Cuarto específicamente.

En esta estructura general, las Unidades Judiciales son dependencias del Ministerio Público Fiscal cuya función es llevar adelante los primeros actos de investigación, en la primera etapa del procedimiento penal. Están a cargo de los Ayudantes Fiscales, que son asistidos por los Secretarios de Actuaciones, todos funcionarios del Ministerio Público Fiscal.

El Ayudante Fiscal es el responsable último de impartir las directivas investigativas, así como cumplir las que reciba del fiscal de instrucción y, junto con la Fiscalía de Instrucción, disponer el destino final de las causas (depósito judicial, continuar en instrucción porque falta reunir prueba, elevar en el caso de que el autor ya esté individualizado e imputado, o girar la causa, en caso de que la misma haya ocurrido en otra jurisdicción). También hay un jefe de área que se encarga de llevar adelante el despacho diario de la oficina, control del personal e incluso de dar directivas en el marco de algunas investigaciones, aunque nunca dispone qué se hace con las causas, tal como lo hace el Ayudante Fiscal.

Además de esta estructura, la Unidad Judicial N° 3 de Río Cuarto está conformada también por sumariantes, repartidos en tres turnos –más una guardia nocturna pasiva- que permiten que la Unidad Judicial atienda al público las 24 hs. Estos sumariantes son los encargados de recibir las denuncias y tramitar todas las causas de acuerdo con las directivas que reciban del Ayudante Fiscal. La investigación "de calle" está a cargo de cuatro comisionados policiales que están asignados a la Unidad Judicial –pero no son parte de la estructura del MPF, si no de la policía administrativa – que se encargan de realizar las tareas de campo, diligenciar allanamientos, citar a testigos, etc.

Como colaboración a este personal de investigaciones, existe una brigada de investigaciones principal dentro de la ciudad, pero que trabaja en causas muy complejas y posee una baja disponibilidad de agentes para colaboraciones con las investigaciones de la Unidad Judicial. Es importante mencionar que la Unidad Judicial N° 3 posee una competencia territorial en aproximadamente el 30% de la superficie de la ciudad de Rio Cuarto, sector que tiene una población de alrededor de 80.000 habitantes (sobre un total de 200.000 que tiene la ciudad).

El personal asignado a la Unidad Judicial no cuenta con capacitación específica para investigar ciberdelitos, así como tampoco el personal policial de investigaciones asignados a dichas tareas en el ámbito de la U.J.

1.1.2. Datos Estadísticos

Según datos del Libro de Sumarios de la Unidad Judicial N° 3 de la ciudad de Río Cuarto correspondiente al periodo 2021-2023 (julio), se consignan 6752 delitos, de los cuales 236 (3%) son hechos relativos a cibercrímenes, siendo el año 2022 el de mayor

registro, y las estafas el tipo de delito informático con mayor frecuencia (81%), como se puede observar en la Tabla 1.

Tabla 1. Ciberdelitos cometidos en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, por modalidad de comisión. 2021-2023.

	2021	**2022**	**2023**	**TOTALES**	**%**
Amenazas	9	6	8	**23**	10%
Denuncia formulada	3	3	3	**9**	4%
Estafas	56	82	54	**192**	81%
Integridad sexual	2	-	-	**2**	1%
Robo/Hurto	7	2	1	**10**	4%
TOTAL	**77**	**93**	**66**	**236**	100%

Nota: para el año 2023 se consignan datos hasta 26/7/2023.

Aunque en todos los casos está identificado el/los autores del delito, solo 2 hechos (uno correspondiente al año 2022 y otro al 2023), se encuentran en estado de "Elevado", que significa que ya finalmente se concluyó con la investigación a través de la imputación del autor y se giró a la Fiscalía para que eleve la causa a juicio. El 73% de los ciberdelitos cometidos en este periodo se encuentran en "Depósito Judicial", que significa que la causa está archivada pero susceptible de volver a instruirse; el 22% se encuentra "En instrucción", es decir que aún se continúa investigando en la Unidad Judicial; y el 3% se encuentra "Girado", que equivale a que se remitió a otra dependencia por cuestión de competencia (ver Tabla 2).

Tabla 2. Ciberdelitos cometidos en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, por estado de los expedientes. 2021-2023.

	2021	**2022**	**2023**	**TOTALES**	**%**
Depósito Judicial	69	65	39	**173**	73%
Elevado	-	1	1	**2**	1%
En Instrucción	3	25	23	**51**	22%
Girado	2	2	2	**6**	3%
No informado	3	-	1	**4**	2%
TOTAL	**77**	**93**	**66**	**236**	**100%**

Nota: para el año 2023 se consignan datos hasta 26/7/2023.

En el periodo analizado la proporción de causas/delitos por cada sumariante e investigador de la Unidad Judicial N° 3 es muy alta, como se puede observar en la Tabla 3.

Tabla 3. Cantidad de causas/delitos por cada sumariante en la Unidad Judicial N° 3 de la ciudad de Río Cuarto. 2021-2023.

	Total de delitos por sumariante*	**Ciberdelitos**
Sumariante 1	207	0
Sumariante 2	171	1
Sumariante 3	699	25

	Total de delitos por sumariante*	Ciberdelitos
Sumariante 4	803	42
Sumariante 5	394	12
Sumariante 6	161	6
Sumariante 7	155	6
Sumariante 8	608	13
Sumariante 9	544	19
Sumariante 10	214	5
Sumariante 11	622	13
Sumariante 12	62	4
Sumariante 13	294	12
Sumariante 14	369	15
Sumariante 15	77	12
Sumariante 16	225	6
Sumariante 17	972	40
Sumariante 18	152	2
Sumariante 19	5	0
Sumariante 20	99	1
Sumariante 21	90	2
TOTAL	**6752**	**236**

Nota: en el total de delitos por cada sumariante están contabilizados los ciberdelitos, pero estos últimos se desagregaron en la siguiente columna. La cantidad de sumariantes en el período de tiempo analizado varia, siendo la planta permanente de aproximadamente 12 sumariantes.

Del relevamiento de casos judicializados surge que existe en la actualidad un insignificante porcentaje de imputados; la gran mayoría de las causas de ciberdelito ingresadas a modo de denuncia, no resultan instruidas ni investigadas, dando como resultado que no se produzcan imputaciones de los autores de estos hechos delictivos, a pesar de haber sido identificados.

1.1.3. Pregunta de Investigación

Los datos relevados despiertan el interés por indagar:

- ¿Cuáles son los principales obstáculos que enfrentan en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, provincia de Córdoba, Argentina para la Investigación Penal Probatoria en los casos de cibercrimen?

1.2. Hipótesis

En este contexto se produce una combinación de circunstancias que contribuyen negativamente a la efectiva imputación de los delitos. Como hipótesis se plantean:

H1: la *escasez de personal* frente al gran volumen de trabajo hace muy difícil que el instructor de la causa pueda dedicarse a instruir un expediente por un hecho de

cibercrimen, el que casi siempre comienza como N.N. y debe tramitarse de forma compleja, acudiéndose a aquellas oficinas de Policía Judicial de Córdoba u oficiando a entidades bancarias (sin que haya una oficina que centralice estas consultas), cuando al mismo tiempo debe tramitar hechos de violencia familiar, homicidios, robos calificados, etc. que representan mayor gravedad y urgencia, quedando relegadas las causas por ciberdelitos.

H2: la *capacitación específica en investigaciones de cibercrimen* es escasa o nula, especialmente en el tratamiento de evidencia digital y en los aspectos legales y procesales vinculados, teniendo en cuenta también que, como se mencionó anteriormente, la evolución de estos delitos se produce de manera constante y acelerada, lo que obliga a una constante actualización de los conocimientos para contar con personal especializado.

H3: la *centralización de recursos investigativos científico/técnicos en la ciudad de Córdoba* atenta contra un diligenciamiento rápido de la instrucción desde una ciudad como Rio Cuarto, ubicada a 200 km de la capital, a pesar de que actualmente todo el trámite judicial está casi digitalizado.

H4: el *marco normativo* – tanto nacional como provincial – resulta insuficiente para dar respuesta a estas modalidades delictivas, que evolucionan constantemente y en consecuencia, hace que la ley siempre vaya detrás de estas, entorpeciendo la investigación de este tipo de delitos.

1.3. Objetivos

1.3.1. Objetivo General

- Identificar los principales obstáculos que enfrentan en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, provincia de Córdoba, Argentina para la Investigación Penal Probatoria en los casos de cibercrimen.

1.3.2. Objetivos específicos

1. Analizar la incidencia de la escasez de personal en la Unidad Judicial N° 3 de la ciudad de Río Cuarto para la efectiva imputación de los delitos.
2. Conocer el grado de capacitación en cibercrimen y suficiencia/insuficiencia de recursos técnicos en el desarrollo de las causas judiciales.

3. Examinar el impacto de la centralización de recursos investigativos científico/técnicos en la ciudad de Córdoba en la investigación en cibercrimen.
4. Indagar si el marco normativo – tanto nacional como provincial – resulta suficiente para dar respuesta a estas modalidades delictivas.

1.4. Justificación

La utilidad de este trabajo radica en que aporta conocimiento sobre los factores que influyen en la investigación de cibercrimen en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, provincia de Córdoba, Argentina y que arroja como resultado que prácticamente no haya imputados en este tipo de delitos, que van creciendo sostenidamente en las últimas décadas. Por lo tanto, presenta una utilidad práctica para los actores involucrados en esta Unidad Judicial pero también para el sistema de justicia cordobés en su conjunto ya que se espera que este conocimiento sea un insumo importante para plantear estrategias que permitan superar los desafíos, obstáculos y limitaciones para la correcta y completa resolución de estos hechos delictivos.

2. MARCO TEÓRICO

2.1. Conceptualizaciones sobre Ciberdelito

Como ya fue mencionado, se entiende por Ciberdelito a todo hecho contrario a la ley que utilice herramientas informáticas para preparar, consumar o garantizar la impunidad a la hora de cometer un hecho delictivo. En este caso es atendible la cuestión que expresa que no todo delito en el cual intervenga un medio informático puede considerarse Ciberdelito, si no en los casos en que el uso de esta tecnología es preponderante e indispensable, haciendo imposible el acometimiento criminoso sin la utilización de dicho artificio tecnológico.

La Organización para la Cooperación Económica y el Desarrollo (OCDE) define al "delito informático" como "Cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos" (citado en Temperini, 2018, p.54). Resulta de interés el aporte de Téllez Valdés (2008), quien al referirse al concepto de delitos informáticos los clasifica en: "actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas,

antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico). (p.188).

En última instancia, es destacable la opinión de Marcelo Temperini, quien sostiene que, en principio debe dejarse en claro que la mera intervención de un elemento informático no convierte a un delito clásico en un delito informático. Sin embargo, es necesario reconocer que, en determinados tipos penales, el ingrediente tecnológico es tan poderoso que hace necesario que para su identificación, investigación y persecución intervengan especialistas dedicados a los delitos informáticos. Es decir, hablamos de aquellos casos donde el tipo penal clásico es perfeccionado utilizando a las nuevas tecnologías como medio para su comisión, dotándolo de esa manera de muchos de los inconvenientes o desafíos clásicos de los delitos informáticos, tales como el anonimato, internacionalidad, dificultad en la obtención de evidencia digital, entre otros (Temperini, 2018).

2.1.1. Características del Ciberdelito y los Ciberdelincuentes

Téllez Valdés (2008) enumera las principales características de los delitos informáticos (p.188):

1. Son conductas criminales de cuello blanco, *white collar crimes*, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas[1].
2. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
3. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" a aquellos que los realizan.
4. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin presencia física.
5. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel nacional e internacional.

[1] En este sentido, Téllez Valdés (2008) señala que una de las características principales de los delitos "de cuello blanco" es que "el sujeto activo del delito es una persona de cierto estatus socioeconómico y su comisión no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional" (p.189).

6. Presentan grandes dificultades para su comprobación, por su carácter técnico.
7. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
8. Ofrecen a los menores de edad facilidades para su comisión.
9. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica, especialmente en el ámbito internacional.

También resulta de interés analizar cuáles son las características de los ciberdelincuentes, entre las que Téllez Valdés (2008) destaca las siguientes:

- Son personas con habilidad para manejar los sistemas informáticos;
- En líneas generales, por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible;
- Son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sin embargo, no se pueden generalizar estas características, ya que son muy diferentes las motivaciones de una persona que ingresa en un sistema informático sin intenciones delictivas a las de un empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. En este sentido, Téllez Valdés (2008) señala que "el nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos no revela delincuencia informática, mientras otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico" (p.189).

De acuerdo con la investigación realizada por Mateos (2013), existe un número elevado de estudios que han demostrado que el perfil típico del ciberdelincuente se corresponde con una persona de sexo masculino, entre los 25 y 35 años de edad y con ciertos conocimientos tecnológicos e informáticos que le permiten utilizar internet para ejecutar sus actividades. Hay que tener en cuenta que, tratándose de un tipo de delito en constante evolución, investigaciones posteriores han demostrado que la edad de inicio en la ciberdelincuencia es cada vez menor, por lo que se deben estudiar cuáles son los precipitantes de este hecho (González García y Campoy Torrente, 2018).

Marta Violat, criminóloga experta en Cibercrimen y Ciberseguridad, advierte que no existe un perfil típico o único de la figura de "cibercriminal", aunque comparten ciertas características comunes que se pueden agrupar en (Violat, 2020):

- **Capacidades tecnológicas**. Se trata de delincuentes "especializados", es decir que poseen cierta destreza tecnológica para llevar a cabo cualquier ilícito a través de medios digitales. Sin embargo, existen diferentes niveles en estas capacidades, ya que se requiere de distintos niveles de competencia para suplantar una identidad, para acceder a un sistema o para crear un Malware (virus informático).
- **Expectativas sociales**. El ciberdelincuente suele cometer estos los delitos por fantasías y motivaciones. Por ejemplo, algunos de estos criminales no consideran como delito vulnerar un sistema sino que buscan el reconocimiento social, además de experimentar un sentimiento de superioridad por sus conocimientos.
- **Sentimiento de seguridad**. Al moverse en un ámbito de clandestinidad como es internet, el ciberdelincuente puede cometer sus acciones delictivas bajo cualquier seudónimo o restricción de su identidad, que garantiza su anonimato y le permite realizar los delitos desde un cierto margen de comodidad y seguridad. En este aspecto también influye la transnacionalidad del ciberdelito, característica que fomenta el anonimato y que obtiene las mismas consecuencias de falsa seguridad.
- **Sentimiento de superioridad**. El cibercriminal, como cualquier otro delincuente, tiende a sentirse por encima de la ley y por ello la vulnera.

Sin embargo, el motivo principal por lo que un cibercriminal delinque, al igual que cualquier otro, es la motivación, o sea, el conjunto de impulsos que lo llevan a realizar cualquier ilícito ya sea fraude, robo de información, suplantación de identidad, entre otros. Para Violat (2020) las motivaciones más relevantes desde la cibercriminología son:

- **Por diversión**. El interés es llegar un poco más lejos de lo que un usuario "estándar" de la red o de tecnología pueda llegar.
- **Por beneficio económico**. Se utiliza la pericia o los conocimientos para poder obtener un lucro. Aquí se encuadran los casos de estafa o de *Phishing* cuyo objetivo es obtener una ganancia económica.

- **Por sentimientos de ira, rabia, venganza o indignación**. Por ejemplo, un trabajador despedido que, por cuenta propia o con ayuda de terceros realiza un ataque al sistema de la compañía.
- **Por incitación sexual**. Se trata de un ciberdelincuente que utiliza los medios técnicos oportunos para conseguir imágenes o grabaciones sexualizadas, incluyendo pedofilia o sexting.
- **Por cuestiones políticas**. Con el objetivo de derrocar un gobierno o de llamar la atención de la sociedad. Un ejemplo sería el *hacktivismo*[2].

2.1.2. Tipos de Ciberdelitos

Téllez Valdés (2008) clasifica a los delitos según el uso del medio tecnológico, donde éste puede ser utilizado *instrumento* para cometer el hecho delictivo o como *fin u objetivo*. El dispositivo actúa instrumento para la comisión de un delito cuando, por ejemplo, una persona amenaza o acosa a otra u otras y lo realiza a través de esta tecnología, y actúa como fin u objetivo cuando el blanco del delito es la propia tecnología, por ejemplo, cuando un malware o software malicioso como un virus, afecta y altera el normal funcionamiento del dispositivo o los datos y la información que almacena.

En este sentido, se refuerza la idea de que "el cibercrimen no representa un tipo de criminalidad específica en tanto que nuclea a un conjunto de delitos que adoptan esta definición por el lugar que ocupa la tecnología, más que por la naturaleza criminal del acto mismo. La definición de delitos informáticos es instrumental" (Secretaría de Innovación Tecnológica, 2022, p.2).

En Argentina, la Ley 26.388 promulgada el 24 de junio de 2008, introduce modificaciones en el Código Penal para incorporar a los delitos informáticos, considerando como tales a:

- ofrecimiento, distribución y tenencia de imágenes relacionadas con pornografía infantil (Art. 128);
- violación de secretos y privacidad: violación de correspondencia electrónica (Art. 153), acceso ilegítimo a un sistema informático (Art. 153 bis), publicación

[2] También denominado ciberactivismo, se trata de la utilización de herramientas digitales con fines políticos; incluye desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, sabotajes virtuales.

abusiva de correspondencia (Art. 155), revelación de secretos (Art. 157), delitos relacionados con protección de datos personales (Art. 157 bis);

- defraudación informática (Art. 173, inc. 16);
- daño informático (Arts. 183 y 184);
- interrupción de comunicaciones electrónicas (Art. 197);
- destrucción, alteración o inutilización de medios de prueba (Art. 255);
- *grooming* o delitos contra la integridad sexual de menores (Art. 131).

Un informe presentado por la Secretaría de Innovación Tecnológica (2022) reseña que durante la pandemia del COVID-19, en Argentina, se produjo un incremento de denuncias sobre diferentes modalidades delictivas sucedidas en internet. Sin embargo, la tipología de ciberdelitos que enumera no son otra cosa que nuevas modalidades de delitos ya existentes, que adquirieron en este periodo excepcional una mayor sofisticación y complejidad en las técnicas de comisión de estos ilícitos, así como la aparición de asociaciones ilícitas y de bandas con cierto grado de organización, que toman al cibercrimen como emprendimiento delictivo. Las modalidades más frecuentes pueden agruparse en tres tipos: fraudes y estafas en línea; ataques de *ransomware* a organizaciones; y blanqueo ilícito de capitales por internet.

Fraudes y estafas en línea. Un fraude es la adquisición indebida de bienes ajenos por medio del engaño. El fraude económico suele ser entendido como estafa cuando el objetivo del engaño es producir a la víctima un perjuicio de tipo patrimonial –financiero o material– con un fin puramente lucrativo en beneficio del autor. En esta modalidad se encuentra el *Phishing*, que puede traducirse como "pesca de contraseñas". Se trata de un fraude de ingeniería social[3] aplicado para "pescar" datos personales de una víctima. Es utilizado como una técnica para cometer el robo de identidad, entendido como la obtención no autorizada de datos personales para realizar luego una suplantación o usurpación de identidad en un hecho ilícito posterior.

En los casos de *phishing*, el estafador se puede hacer pasar por un representante de una institución bancaria, un organismo público, una tarjeta de crédito o una ONG, entre otras, y envía mensajes fraudulentos a través de correo electrónico, SMS, redes sociales,

[3] La ingeniería social es un proceso por el que se intenta obtener información de un usuario mediante métodos y herramientas no técnicas, como por ejemplo, la comunicación para ganarse la confianza de una persona y así obtener sus datos, generalmente para la comisión de una estafa posterior.

WhatsApp, entre otros, con la excusa de un supuesto problema de seguridad, actualización de datos, aprovechamiento de una oferta o promoción, la caducidad de un servicio o producto o la urgencia por una necesidad de la potencial víctima, y con el propósito de obtener datos personales (como nombre y apellido, DNI, número de tarjeta de crédito, credenciales de acceso a servicios y aplicaciones).

El fraude más común en Argentina es el phishing bancario, donde la víctima recibe un correo electrónico, supuestamente de una institución bancaria que le solicita que valide su usuario y contraseña de acceso a *homebanking*. El cuerpo del mensaje contiene un enlace que deriva a un sitio web falso creado por el estafador (muy similar en aspecto al sitio oficial del banco para el que dice operar) para que la víctima coloque sus credenciales de acceso a *homebanking* que luego el estafador "pescará" e intentará utilizar para hacer transferencias bancarias a una cuenta determinada.

Durante la pandemia y también después, se ampliaron las modalidades de phishing hacia otro tipo de estafas vinculadas a problemáticas de actualidad, como los turnos de vacunación COVID, tratando de explotar diferentes motivaciones en las potenciales víctimas, tales como la curiosidad, el temor o la necesidad. Una de las más habituales fue el "fraude de turno de asignación de vacunación", donde el *phisher* establecía una comunicación fraudulenta por WhatsApp haciéndose pasar por un organismo de Salud determinado, que le informaba la fecha, hora y lugar donde debía asistir para la aplicación de la dosis de la vacuna contra el COVID-19. El fraude consistía en que la víctima debía confirmar el supuesto turno mediante el envío del código numérico de seis dígitos, que le había llegado a su casilla de mensajes de texto del móvil, y que en realidad es un código de seguridad que proporciona WhatsApp cuando se solicita la utilización de cuenta de esta aplicación en otro dispositivo. Una vez que la víctima proporciona este código al estafador, éste lo utiliza para iniciar una sesión de WhatsApp en otro dispositivo, es decir, utiliza los datos de la víctima y el doble factor de autenticación para hacerse pasar por ella. Luego de apoderarse de la cuenta, la estafa posterior consiste en enviar mensajes a los contactos de la víctima solicitándoles dinero por un problema personal.

Otra modalidad de estafa son los "secuestros virtuales", donde la víctima recibe una llamada, generalmente durante la noche, en la que el supuesto secuestrador le dice que liberará a un familiar tras el pago de un rescate. También se pueden mencionar los fraudes de compraventa en redes sociales, especialmente a través de Instagram o Facebook Marketplace, espacios en los que los usuarios puedan comprar y vender productos y

servicios de forma directa. Para atraer a las víctimas, los estafadores ofrecen productos a bajo precio y muestran imágenes ficticias de clientes satisfechos, que están acompañados de comentarios positivos por las transacciones realizadas, todas tomadas de forma pública de la web. Los pagos deben ser siempre en efectivo o con depósito bancario. La persona realiza el pago pero nunca recibe el producto.

Ataques de *ransomware* a organizaciones. El *ransomware* (conjunción de "*ransom*" -rescate- y software) es un programa malicioso, un *malware* que encripta determinados archivos de un dispositivo o sistema o el acceso a los mismos. El "secuestrador" de los datos solicita un "rescate", generalmente un pago en criptomonedas, para liberar la información. Entre los ataques mediante la explotación de vulnerabilidades de los sistemas se encuentran los denominados "de fuerza bruta" que se produce cuando un atacante intenta ingresar a un sistema informático probando diferentes combinaciones de caracteres hasta que logra descubrir la contraseña buscada. De esa forma obtiene las credenciales de acceso para ingresar a la cuenta de un legítimo usuario.

Los blancos principales son las grandes empresas, debido a su potencial capacidad para pagar las sumas millonarias demandadas. Otro objetivo de los ataques de *ransomware* son las Infraestructuras Críticas de Información (ICI), que consisten sistemas y redes informáticas que hacen a la operatividad y suministro de servicios esenciales para las personas. Algunas de ellas pueden ser las pertenecientes al sector bancario, al energético, a la provisión de combustible, a los medios de transporte, al gas, etc..

Blanqueo ilícito de capitales por internet. Consiste en legitimar fondos provenientes de actividades ilegales, también conocido como "lavado de dinero". Es un delito difícil de descubrir por el uso de testaferros para la realización de operaciones ejecutadas por debajo del umbral permitido por las autoridades de control financiero, establecidas por el Grupo de Acción Financiera Internacional (GAFI). La nueva economía digital ofrece una serie de servicios económico-financieros mediados por TIC, tales como la compraventa de bienes y servicios, el desarrollo de pagos electrónico, las transferencias de fondos en línea y el uso de prestaciones bancarias en forma electrónica, entre otros. En esta línea, en los últimos años se produjo en Argentina el surgimiento de bancos digitales, que tienen existencia únicamente en el ciberespacio, es decir, sin sedes físicas. A diferencia de los bancos tradicionales, donde la apertura de una cuenta bancaria es de forma personalizada mediante acreditación de identidad, en la versión en línea se permite comenzar a operar mediante métodos digitales de identificación que están en la web. Esto

facilita la sustitución de identidad, y también la apertura de cuentas para legitimar fondos ilícitos provenientes de fraudes y estafas en línea.

Por otra parte, el *Convenio de Budapest* o *Convenio sobre Ciberdelincuencia* firmado en Budapest, Hungría, el 23 de noviembre de 2001 – y al que Argentina adhiere mediante la Ley 27.411/2017 – propone una clasificación de los delitos informáticos en cuatro grupos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos. Ejemplos: el robo de identidades, la conexión a redes no autorizadas y la utilización de *spyware*[4] y de *keylogger*[5].

2. Delitos informáticos:

- Falsificación mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: como la copia y distribución de programas informáticos, o piratería informática.

---

[4] Tipo de software que se instala en el sistema sin que el usuario lo sepa. Suele venir oculto junto a otros programas que se instalan de manera consciente, lo que lo hace muy difícil de detectar. Una vez en el sistema, recopila información para enviarla a terceros.

[5] Software malicioso que, sin permiso o conocimiento, registra todas las teclas que se pulsan para operar una computadora o celular. De este modo, es posible detectar las cosntraseñas.

Dentro de la tipología de ciberdelitos contra la integridad sexual se encuadra también el *grooming*, incorporado como Artículo 31 del Código Penal (Ley 11.179/1984) a través de la Ley 26.904/2013. Este articulo prevé que:

> Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

El grooming puede concebirse como una nueva modalidad de ciberdelito, posible gracias al desarrollo de internet, pero en realidad se trata de una forma "evolucionada" de un delito ya existente, mediante la cual los pedófilos se valen de la tecnología para contactar y abusar de sus víctimas. "Incluso ha mutado la relación víctima-victimario, ya que desaparece el contacto físico, lo que no implica la ausencia de abuso" (Esteban, 2019, p.21).

2.2. El Proceso Penal

Para analizar las características particulares que adquiere la investigación procesal penal en cibercrimen es necesario presentar, en primer lugar, las características generales de un proceso penal, cuyo objetivo último es la averiguación de la verdad material. Es decir "aquella verdad que pueda acreditarse a partir de las pruebas producidas en la etapa de juicio" (Finocchiaro, 2015, p.1).

Vélez Mariconde (citado en Cafferata Nores et al (2003) define al proceso penal como:

> (…) una serie gradual, progresiva y concatenada de actos disciplinados en abstracto por el derecho procesal y cumplidos por órganos públicos y por particulares obligados o autorizados a intervenir, mediante los cuales se procura investigar la verdad sobre la acusación de un delito y actuar concretamente la ley penal sustantiva. (p.172).

El proceso penal atraviesa diferentes estadios o etapas, que pueden diferenciarse entre sí por los sujetos que las componen, la diversidad de objetivos y los diferentes actos procesales que las integran. Binder (2009) describe cinco etapas bien diferenciadas:

1. Fase de investigación, preparación o instrucción, cuyo objetivos es la preparación de la acusación o del juicio.
2. Fase crítica o del control del resultado de esa investigación.
3. Fase plena, central, que es el juicio propiamente dicho.
4. Fase de control de esa sentencia de juicio, manifestada a través de la existencia de distintos medios de impugnación.
5. Fase de ejecución, donde se ejecuta la sentencia que ha quedado firme.

En palabras de Cafferata Nores et al (2003) el proceso penal se desarrolla de la siguiente manera:

> (…) frente a la hipótesis de la comisión de un delito, el Estado, a través de sus órganos persecutorios, impulsa su investigación en procura de verificar la existencia de la infracción que se presume cometida y lograr el eventual examen posterior de los jueces sobre su punibilidad (actividad acusatoria o de persecución penal). Superados afirmativamente estos interrogantes a través de un juicio imparcial en el que se respete la dignidad del acusado y se garantice su defensa, se impone al culpable una sanción (actividad jurisdiccional). (pp.36-37).

El proceso penal en la provincia de Córdoba, contexto de este trabajo, se encuentra dividido en dos etapas principales, siendo la primera de ellas la Investigación Penal Preparatoria, dirigida por el Fiscal, la que tiene por objetivo la reunión de prueba que permita acusar al sospechoso de un hecho delictivo o, por el contrario, desestimar dicha acusación. Este trabajo de investigación se circunscribe a esta primera etapa del proceso penal, siendo la segunda el Juicio propiamente dicho, que no se contempla dentro del marco de este trabajo.

2.2.1. La Investigación Penal Preparatoria

De acuerdo con el Código Procesal Penal de la provincia de Córdoba, la investigación penal preparatoria tiene como finalidad "impedir que el delito cometido produzca consecuencias ulteriores y reunir las pruebas útiles para dar base a la acusación o determinar el sobreseimiento" (Art. 302). En su Artículo 303 se determina que la investigación penal tendrá por objeto:

1) Comprobar si existe un hecho delictuoso, mediante todas las diligencias conducentes al descubrimiento de la verdad.

2) Establecer las circunstancias que califiquen el hecho, lo agraven, atenúen o justifiquen, o influyan en la punibilidad.

3) Individualizar a sus autores, cómplices e instigadores.

4) Verificar la edad, educación, costumbres, condiciones de vida, medios de subsistencia y antecedentes del imputado; el estado y desarrollo de sus facultades mentales, las condiciones en que actuó, los motivos que hubieran podido determinarlo a delinquir y las demás circunstancias que revelen su mayor o menor peligrosidad.

5) Comprobar la extensión del daño causado por el delito, aunque no se hubiera ejercido la acción resarcitoria.

La investigación preparatoria se inicia a través de la denuncia de un hecho delictivo, que de acuerdo con el Artículo 314: "Toda persona que tenga noticia de un delito perseguible de oficio podrá denunciarlo al Fiscal de Instrucción o a la Policía Judicial". Esta denuncia podrá ser escrita o verbal, y se presentada personalmente o por mandatario especial con un poder (Art. 315). Cuando la denuncia se formule ante el Fiscal de Instrucción, éste deberá actuar de inmediato (Art. 319).

El Fiscal de Instrucción tiene a su cargo todo el proceso de investigación penal preparatoria (Art. 301) y le compete reunir los elementos que servirán de base a sus requerimientos. Estos podrán fundamentarse en los actos practicados por la Policía Judicial dentro de sus facultades legales (Art. 328), practicará y hará practicar todos los actos que considere necesarios y útiles para la investigación, salvo aquéllos que la ley atribuya a otro órgano judicial (Art. 329), proveerá a la defensa del imputado (Art. 331), podrá citar, privar y acordar la libertad al imputado (Art. 332). Según el Artículo 334 el Fiscal de Instrucción también dispondrá, por decreto fundado, el archivo de las actuaciones cuando: 1) No se pueda proceder; 2) El hecho contenido en ellas no encuadre en una figura penal; 3) Resulte evidente que el hecho no se cometió, o 4) No se hubiere podido individualizar al autor o partícipe del hecho o si fuere manifiesta la imposibilidad de reunir elementos de convicción que permitan acreditar el hecho.

Por otra parte, La Policía Judicial "por orden de autoridad competente o, en casos de urgencia, por denuncia o iniciativa propia, deberá investigar los delitos de acción

pública, impedir que los cometidos sean llevados a consecuencias ulteriores, individualizar a los culpables y reunir las pruebas útiles para dar base a la acusación o determinar el sobreseimiento" (Art. 321). Además, el Artículo 324 establece que la Policía Judicial tendrá las siguientes atribuciones:

1) Recibir denuncias.

2) Cuidar que el cuerpo, instrumentos, efectos y rastros del delito sean conservados, mediante los resguardos correspondientes, hasta que llegue al lugar el Fiscal de Instrucción.

3) Si hubiere peligro de que cualquier demora comprometa el éxito de la investigación, hacer constar el estado de las personas, cosas y lugares, mediante inspecciones, planos, fotografías, exámenes técnicos y demás operaciones que aconseje la policía científica.

4) Proceder a los allanamientos previstos en el artículo 206 (sin orden judicial), a las requisas urgentes con arreglo al artículo 209 (respetando el pudor de las personas) y a los secuestros impostergables.

5) Si fuera indispensable, ordenar la clausura del local en que se suponga, por vehementes indicios, que se ha cometido un delito grave, o proceder conforme al artículo 274[6].

6) Interrogar sumariamente a los testigos presumiblemente útiles para descubrir la verdad.

7) Citar y aprehender al presunto culpable en los casos y forma que este Código autoriza.

8) Recibir declaración del imputado, sólo si éste lo pidiera, en las formas y con las garantías que establecen los artículos 258[7] y ss.

---

[6] "Artículo 274.- Arresto. Cuando en el primer momento de la investigación de un hecho en que hubieran intervenido varias personas no fuere posible individualizar a los responsables y a los testigos, y no pueda dejarse de proceder sin peligro para la investigación, se podrá disponer que los presentes no se alejen del lugar ni se comuniquen entre sí, antes de prestar declaración, y aún ordenar el arresto, si fuere necesario". (Código Procesal Penal de la provincia de Córdoba).

[7] "Artículo 258.- Asistencia del Defensor. A la declaración del imputado deberá asistir su defensor, bajo pena de nulidad". (Código Procesal Penal de la provincia de Córdoba).

9) Usar de la fuerza pública en la medida de la necesidad.

De acuerdo con el Artículo 337:

> (…) la investigación fiscal deberá practicarse en el término de tres (3) meses a contar desde la declaración del imputado. Si resultase insuficiente, el Fiscal podrá solicitar prórroga al Juez de Control, quien podrá acordarla por otro tanto, según las causas de la demora y la naturaleza de la investigación. Sin embargo, en los casos de suma gravedad y de muy difícil investigación, la prórroga podrá concederse hasta doce (12) meses más.

2.3. La Investigación Penal Preparatoria en la Cibercriminalidad

Como se planteó en la introducción de este trabajo, la investigación criminal en ciberdelitos adquiere un matiz diferente en conceptos tales como "evidencia" y "lugar del hecho". Por un lado, la "evidencia digital" es "todo dato que esté almacenado o sea transmitido mediante la utilización de computadoras (en sentido amplio) que soporta o bien rechaza una teoría acerca de cómo ocurrió un delito o bien aborda los elementos críticos de este, como ser la intención (dolo) o su coartada" (Cenci, 2022, pp.7-8). Es decir que la evidencia digital se asimila en gran medida a cualquier elemento de prueba susceptible de ser secuestrado en un procedimiento judicial.

Está conformada por los datos y la información que transmite, recibe y/o almacena un dispositivo informático, y por lo tanto posee características propias, entre las que Esteban (2019) reseña las siguientes:

- Se trata de una evidencia *inmaterial*, conformada por impulsos eléctricos procesados por un dispositivo;
- Es una evidencia *frágil*, porque puede ser dañada o perdida fácilmente, lo que obliga a generar constantemente mejoras en los sistemas para su almacenamiento;
- Es una evidencia *volátil*, ya que algunos datos son de naturaleza transitoria y se eliminan automáticamente del dispositivo que los aloja;
- Se trata de una evidencia *ocultable*, porque puede ser almacenada en otros dispositivos como pendrives, discos externos, etc.

Es por ello por lo que resulta de suma importancia contar con profesionales y herramientas especiales, con capacidades para adquirir, preservar y analizar la evidencia en tiempo y forma, ya que la manipulación inadecuada de los sistemas involucrados en un delito, así como la dilatación del tiempo transcurrido entre la comisión del delito y la adquisición de la evidencia, pueden destruirla o alterarla significativamente, imposibilitando el avance de la investigación. Al respecto, Cenci (2022) señala que:

> (…) la obtención de prueba digital – ya sea mediante su preconstitución de parte o mediante pericia ordenada judicialmente – y su ulterior preservación y conservación, debe realizarse en las formas (…) que permitan, en primer lugar, confirmar la integridad e inalterabilidad de la prueba digital obtenida, y en segundo orden, facultará el control de las partes tanto en la etapa preliminar, como durante la etapa de juicio oral, garantizando de esta forma el debido proceso. (p.4).

El proceso de obtención de la evidencia digital es complejo e implica, entre otras acciones, realizar el "espejo" o clon del dispositivo con el fin de preservar el original para que no sea contaminado mediante su análisis, ya sea en sede policial o judicial; y la autenticación de dicha evidencia (imagen forense) mediante el cálculo de firmas digitales que garantizan la integridad y autenticidad de la evidencia digital recolectada (Cenci, 2022).

Este proceso requiere necesariamente de la asistencia de un experto en informática forense para evitar que una manipulación indebida contamine la prueba. Pero también se hace necesaria la capacitación de todos los actores que intervienen en la etapa de investigación preparatoria en casos de cibercrimen. Temperini (2018) cita las conclusiones del Congreso Internacional de Derecho Penal del año 2014, en las se afirmó que:

> (…) los Estados han de asumir la obligación de proveer a las fuerzas policiales de los medios técnicos, las capacidades y la formación especializada en el uso de las TIC, no solo para luchar de manera eficaz contra las formas sofisticadas de cibercrimen, sino también para obtener y manejar correctamente la prueba electrónica en general. Se promoverá el desarrollo de guías de buenas prácticas en el uso de las TIC con fines de investigación criminal. (p.67).

Por otra parte, hay que tener en cuenta que, tal como afirma Arocena Alonso (2016):

> Bien es cierto que la policía constituye el primer eslabón de la cadena y que, por tanto, su actuación para perseguir los delitos informáticos precisa de conocimientos técnicos y de no cometer fallos para que el proceso no fracase. No obstante, no podemos olvidarnos del resto de la cadena que también ha de hacer su trabajo de forma efectiva y eficaz. Esto se consigue pasando por una especialización suficiente por parte, también, de la Fiscalía y de los propios Jueces y Magistrados. (p.28).

Pero esta capacitación debe contemplar también que las medidas de investigación que impliquen el uso de las TIC representan una intromisión significativa en el derecho a la privacidad (como el acceso al contenido de las comunicaciones, la interceptación y el acceso de datos en tiempo real, o la utilización de técnicas de investigación remota) y por lo tanto solo podrán aplicarse previa autorización judicial, cuando exista una sospecha razonable de la comisión de un delito que pueda calificarse como grave y de que el destinatario de la medida está vinculado con ese hecho delictivo (Tenperini, 2018).

El otro concepto clave es el de "lugar del hecho", porque no existe un lugar físico sino un entorno virtual. En este sentido, juegan un rol importante las empresas proveedoras de servicios a las que la Justicia puede solicitar información de dos tipos: las solicitudes tradicionales, en las cuales el asunto objeto de investigación no pone en juego el daño físico y/o psíquico, o la muerte de una persona, y las solicitudes de emergencia, que se realizan cuando existe un riesgo para una persona, siendo la emergencia aún mayor cuando la víctima es menor de edad.

En este proceso se pueden producir demoras en el aporte de la información, que dependen de diferentes factores, como por ejemplo: la ubicación de la sede de la empresa proveedora del servicio, si desea o no brindar colaboración, si ya ha firmado algún acuerdo de confidencialidad, etc.

Con relación al material solicitado en una investigación, Esteban (2019) describe los siguientes:

- **Preservación**: se solicita resguardar el contenido asociado a un usuario, independientemente que el mismo lo borre o lo altere. No necesariamente se requiere una orden o autorización judicial, sino que se solicita que la información

se preserve hasta tanto la justicia interviniente en la investigación determine que utilizará dicho material o no.

- **Registro**: incluye los datos básicos de suscripción, con los cuales se arma un perfil, no es contenido. Para solicitar que se registren datos como direcciones IP, fechas, zona horaria de las interacciones que ha tenido la cuenta o perfil investigado, etc. no se requiere autorización judicial.
- **Contenido**: se refiere a todo aquello asociado al perfil o la cuenta, siempre que esté disponible de acuerdo con la política de privacidad, preservación o destrucción de la empresa prestadora del servicio. Considerando que la mayoría de estas empresas tiene su sede en el exterior (principalmente en Estados Unidos) para este tipo de solicitudes son necesarios los Tratados de Asistencia Legal Mutua (*Mutual Assistance Legal Treats*) que son acuerdos de cooperación entre dos o más países para compartir información relacionada con una investigación criminal.

Además hay que tener en cuenta que hasta el momento no existe en Argentina una normativa que obligue a los proveedores de servicios de internet (ISP) a guardar las direcciones IP asignadas a sus clientes por algún plazo determinado. En consecuencia, es posible que al realizar una investigación penal sobre algún hecho (y teniendo identificada la dirección IP del autor del delito) aun contando con la autorización judicial correspondiente no se pueda lograr identificar a la persona que la tenía asignada en un momento determinado (Temperini, 2018).

Otro aspecto que se presenta como problemático en este campo de investigación es la cooperación entre las distintas instancias (policía, fiscalía, peritos técnicos, etc.). En este sentido, Arce et al (2011) señalan que:

> La realidad muestra que las solicitudes de cooperación de las áreas Judiciales a las técnicas, y en particular la "Informática Forense" se realizan horas antes del abordaje o con un día de anticipación, sin brindar más datos que el pedido. Por lo que "No se conoce la causa, lugar a abordar, ni elementos a buscar". Esta falta de información se traduce en dificultades a la hora de tomar decisiones, por ejemplo de que elementos llevar al lugar, a causa de no poder proyectar con que posible escenario nos encontraremos (Domicilio particular, empresas, organismos públicos) y ni siquiera elementos o información a buscar). (p.6).

3. METODOLOGÍA

3.1. Diseño de la Investigación

La metodología empleada para el alcance del objetivo general y los objetivos específicos de este trabajo de investigación es descriptiva la cual, según Hernández Sampieri et al (2010) intenta identificar características que se encuentran involucradas en un acontecimiento, específicamente en este caso en el análisis de los principales obstáculos que enfrenta la investigación de cibercrimen en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, provincia de. Córdoba, Argentina. Para construir una descripción de las características, perfiles de personas y grupos resulta fundamental llevar adelante la recolección conjunta de datos, los cuales se integran a los marcos conceptuales para comprender los fenómenos estudiados (Hernández Sampieri et al, 2010). La articulación entre el marco teórico y el trabajo de campo establece un diseño analítico-empírico que permite describir la situación estudiada con mayor profundidad.

Siguiendo a estos autores, el diseño de investigación es no experimental porque se observan los fenómenos en su contexto natural, para después analizarlos sin intervenir ni manipular deliberadamente las variables. En este caso, a partir de encuestas se toman las respuestas proporcionadas por los participantes en este estudio, constituido por grupos ya formados en su propio contexto; es decir que "*no se genera ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación*" (Hernández Sampieri et al, 2010, p.80).

Por otra parte, se define como transversal o transeccional porque se realiza durante un periodo único. La totalidad de las encuestas se realizaron a lo largo de una semana y el resultado fue recopilado en el mismo periodo, sin considerar su evolución en el tiempo. Para Hernández Sampieri et al (2010) el propósito de los estudios transeccionales es "*describir variables y analizar su incidencia e interrelación en un momento dado. Es como ´tomar una fotografía´ de algo que sucede*" (p.154).

3.2. Enfoque de la Investigación

Esta investigación tiene un enfoque cuantitativo, que de acuerdo con Hernández Sampieri et al (2010) "*se basa en la medición numérica y el análisis estadístico, con el fin establecer pautas de comportamiento*" (p.4). Es decir que permite medir las variables

en un determinado contexto para luego analizar las mediciones obtenidas utilizando métodos estadísticos y extraer conclusiones.

De acuerdo con estos autores, una característica de este tipo de enfoque es que se pueden generalizar los resultados encontrados en un grupo (muestra) a un universo o población mayor debido a que la objetividad de los resultados permite que el estudio puede replicarse fácilmente.

3.3. Muestra

Para recabar información primaria se conformó una muestra de 20 representantes claves que pertenecen o tienen competencia en la Unidad Judicial N° 3 de la ciudad de Río Cuarto, provincia de. Córdoba, Argentina, incluyendo: miembros del Ministerio Público Fiscal (funcionarios, secretarios, prosecretarios, ayudantes fiscales y fiscales); representantes de áreas jurisdiccionales (Cámaras del Crimen, Juzgado de Control de Garantías); policías de investigaciones y técnicos informáticos del Poder Judicial.

La selección de informantes clave obedece a criterios prácticos, de factibilidad y de conveniencia en relación con su voluntad y disponibilidad para participar del estudio, pero tratando de incluir la perspectiva de diferentes actores involucrados en el proceso de investigación penal preparatoria sobre los principales obstáculos que enfrenta la investigación de cibercrimen en esta Unidad Judicial desde.

3.4. Instrumento de Recolección de Datos

El instrumento de recolección de datos diseñado para este trabajo es un cuestionario estructurado (ver Anexo I) que presenta preguntas cerradas, de opción única, dicotómica o múltiple, y de escala de Likert de 5 anclajes (siendo 1 sin gravedad y 5 muy grave). El cuestionario está conformado por 14 preguntas organizadas en 6 grandes bloques:

- **Parte I: Información Demográfica**: las preguntas están orientadas a definir el perfil de los encuestados, incluyendo rol en el sistema de justicia, experiencia en el cargo y conocimiento de los conceptos de “cibercrimen” y “delitos informáticos” en el contexto legal.
- **Parte II: Percepción del Cibercrimen y su Investigación**: en este bloque se incluyen preguntas vinculadas con la percepción personal sobre la gravead el delito cibernético en general, sobre la legislación vigente en torno

al cibercrimen, y los desafíos que enfrenta la investigación de cibercrimen en la provincia de Córdoba.

- **Parte III: Proceso de Investigación y Resultados**: aquí se indaga la experiencia en investigaciones de cibercrimen, cuántas denuncias de cibercrimen han sido registradas en esta unidad en el último año, cuántas de estas denuncias resultaron en la imputación de los presuntos autores, y cuáles son los principales obstáculos que se presentan para llegar a una imputación en este tipo de delitos.
- **Parte IV: Recursos y Capacitación**: en este bloque las preguntas están orientadas a la capacitación específica recibida en investigaciones de cibercrimen y los recursos técnicos para investigar cibercrimen de manera efectiva.
- **Parte V: Colaboración y Coordinación**: se indaga sobre la comunicación entre las unidades de policía, fiscalía y peritos informáticos en casos de cibercrimen.
- **Parte VI: Sugerencias y Conclusiones**: medidas o mejoras que podrían ayudar a mejorar la tasa de imputación en casos de cibercrimen en la provincia de Córdoba.

Los cuestionarios se entregaron a los participantes en mano y se recibieron en el momento. En todos los casos, hubo una comunicación personal previa para explicar los alcances de su participación y garantizar la confidencialidad de la información proporcionada.

3.5. Procedimientos para el Análisis de los Datos

Los datos fueron tabulados en una hoja de cálculo del software Microsoft Excel para facilitar el procesamiento estadístico de la información, así como la elaboración de gráficos para una mejor visualización de los datos más significativos. La presentación de los resultados se organiza de acuerdo con las secciones del cuestionario, cruzando la información con el marco teórico y orientados a los objetivos propuestos y las hipótesis planteadas para el presente trabajo.

4. RESULTADOS

4.1. Información Demográfica

Sobre un total de 20 personas encuestadas, 4 son funcionarios de áreas jurisdiccionales; 7 son funcionarios del del Ministerio Público Fiscal; 1 es Miembro del Equipo de Policía Judicial; 6 son policías de investigaciones; y 2 son técnicos informáticos del Poder Judicial. Todos ellos corresponden a la ciudad de Río Cuarto, donde tiene competencia, entre otras, la U.J.3. La antigüedad promedio en los cargo es de 8 años, lo que demuestra que se trata de personal con experiencia, siendo mayor en el caso de los funcionarios jurisdiccionales y en los del Ministerio Público Fiscal (10 años en cada uno). Todos los encuestados manifestaron tener conocimiento de los conceptos de "cibercrimen" y "delitos informáticos" desde el aspecto legal. En la Tabla 4 se presenta el resumen del perfil de los encuestados.

Tabla 4. Perfil de los encuestados.

Cargo	Antigüedad en el cargo (AÑOS)	Conocimiento de los conceptos de "cibercrimen" y "delitos informáticos"
Funcionario jurisdiccional 1	2	SI
Funcionario jurisdiccional 2	5	SI
Funcionario jurisdiccional 3	14	SI
Funcionario jurisdiccional 4	18	SI
PROMEDIO DE ANTIGÜEDAD	**10**	
Funcionario MPF 1	8	SI
Funcionario MPF 2	16	SI
Funcionario MPF 3	18	SI
Funcionario MPF 4	4	SI
Funcionario MPF 5	7	SI
Funcionario MPF 6	10	SI
Funcionario MPF 7	6	SI
PROMEDIO DE ANTIGÜEDAD	**10**	
Técnico Informático PJ 1	11	SI
Técnico Informático PJ 2	6	SI
PROMEDIO DE ANTIGÜEDAD	**9**	
Miembro Equipo de Policía Judicial	5	SI
PROMEDIO DE ANTIGÜEDAD	**5**	
Policía 1	11	SI
Policía 2	8	SI
Policía 3	2	SI
Policía 4	9	SI
Policía 5	7	SI
Policía 6	5	SI
PROMEDIO DE ANTIGÜEDAD	**7**	
PROMEDIO GENERAL DE ANTIGÜEDAD	**8**	

A los efectos de esta investigación no se consideraron otras variables sociodemográficas por no ser pertinentes al estudio que se desea realizar.

4.2. Percepción del Cibercrimen y su Investigación

Frente a la pregunta sobre cuán grave considera el delito cibernético en general (siendo 1 sin gravedad y 5 muy grave), para la totalidad de los encuestados se observa que solo el 10% lo considera "muy grave" y los restantes grados de gravedad menor se reparten de forma equitativa con un 30% cada uno, aunque ninguno optó por el nivel 1 = sin gravedad (ver Figura 2).

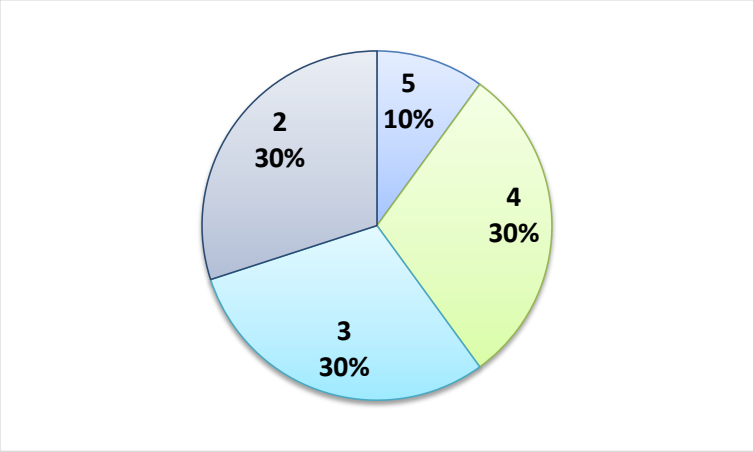
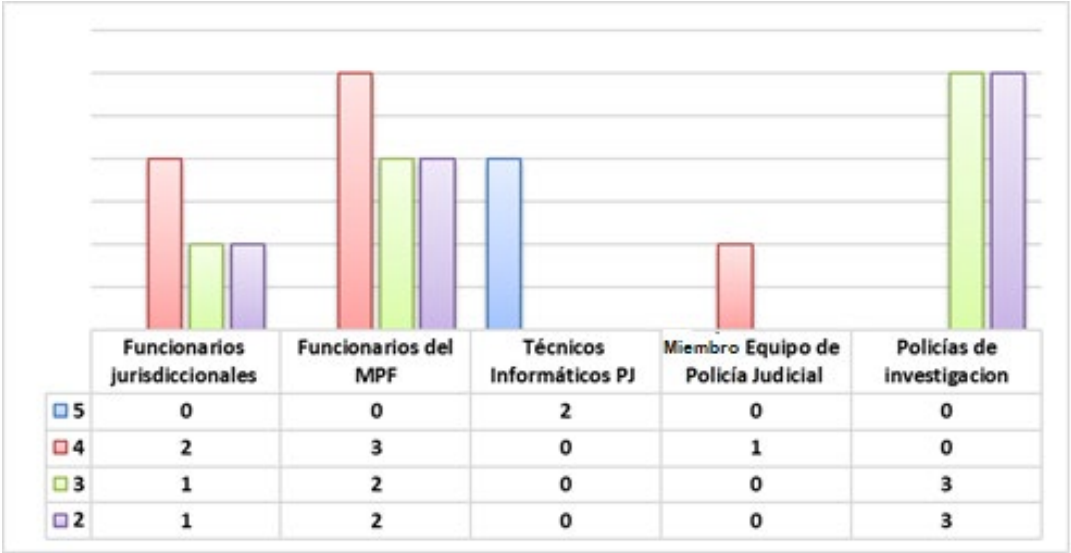


Figura 2. Percepción sobre la gravedad del ciberdelito. N = 20.

El desagregado de la valoración de la gravedad por cargo muestra que solo los Técnicos Informáticos del Poder Judicial son los que consideran que son "muy graves", lo que permite inferir que esto se debe al mayor conocimiento de los expertos sobre el tema. El 43% de los funcionarios del Ministerio Público Fiscal, el 50% de los funcionarios jurisdiccionales y el Miembro del Equipo de Policía Judicial los consideran "graves". Resulta significativo que la totalidad de los policías de investigación le atribuyen los menores niveles de gravedad (Figura 3).



	Funcionarios jurisdiccionales	Funcionarios del MPF	Técnicos Informáticos PJ	Miembro Equipo de Policía Judicial	Policías de investigacion
5	0	0	2	0	0
4	2	3	0	1	0
3	1	2	0	0	3
2	1	2	0	0	3

Figura 3. Percepción sobre la gravedad del ciberdelito. Desagregado por cargo.

Entre los desafíos que los encuestados consideran que enfrenta la investigación de cibercrimen en Córdoba, el 35% señala la falta de recursos técnicos, el 33% la falta de conocimiento especializado, el 18% la falta de legislación adecuada y el 14% la dificultad para rastrear las actividades en línea (Figura 4).

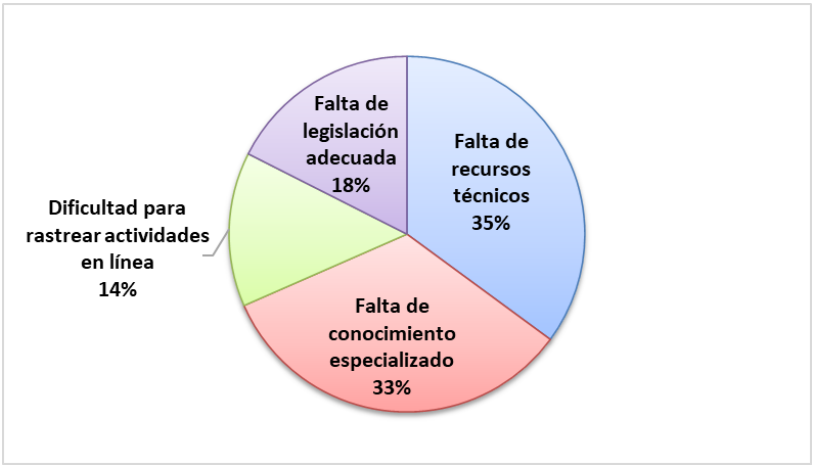


Figura 4. Percepción sobre los desafíos que enfrenta la investigación de cibercrimen en Córdoba. N = 20.

Cabe destacar que la falta de recursos técnicos y la falta de conocimiento especializado son los dos desafíos que aparecen señalados en todos los perfiles encuestados. Esto confirma las apreciaciones de diferentes autores analizados en el marco teórico, como Borzi Cirilli (2018), Justo (2017) o Temperini (2018).

4.3. Proceso de Investigación y Resultados

Del total de 20 encuestados, el 75% manifestó que en el último año se han registrado en su dependencia menos de 100 denuncias de cibercrimen, y el 15% que se han realizado

entre 100 y 500. Cabe señalar que estos últimos corresponden a 3 funcionarios del Ministerio Público Fiscal. Por otra parte, el Miembro del Equipo de Policía Judicial y 1 de los Técnicos Informáticos del Poder Judicial no responden esta pregunta (ver Figura 5).

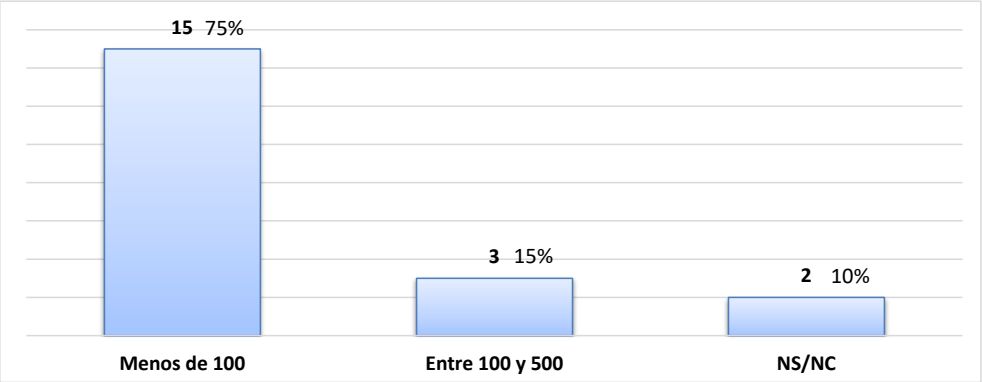


Figura 5. Percepción sobre la cantidad de denuncias de cibercrimen registradas en el último año en la UJ N° 3. N = 20.

En relación con la cantidad de denuncias que resultaron en la imputación de los presuntos autores, 12 encuestados responde que menos del 10% y 7 entre el 10% y el 25%. En este ultimo caso, los encuestados son funcionarios jurisdiccionales o del Ministerio Público Fiscal (Figura 6).

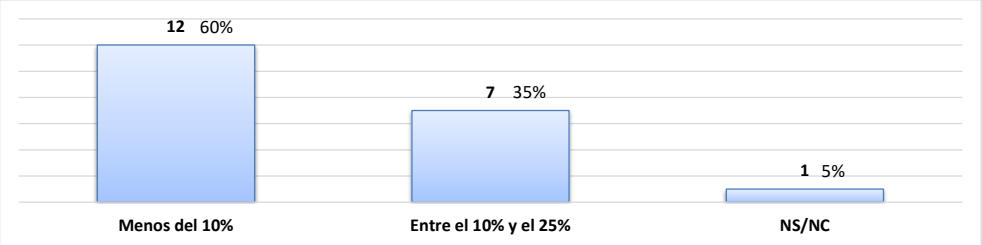


Figura 6. Percepción sobre la cantidad de denuncias de cibercrimen que resultaron en la imputación de los presuntos autores en la UJ N° 3. N = 20.

En conjunto, el 95% de los encuestados manifiesta que las denuncias de cibercrimen en las distintas dependencias a sus cargos, todas de la ciudad de Río Cuarto –incluyendo las tramitadas en la U.J.3- tienen muy bajos resultados en cuanto a la resolución en la imputación de los presuntos autores. Por lo tanto, es pertinente indagar acerca de cuáles consideran que son los principales obstáculos para llegar a una imputación en casos de cibercrimen en este contexto. La opción elegida con mayor frecuencia es la dificultad para identificar a los perpetradores, seguida de la falta de evidencia digital sólida, los desafíos técnicos para rastrear actividades en línea, y en última lugar, la falta de colaboración internacional (ver Figura 7).

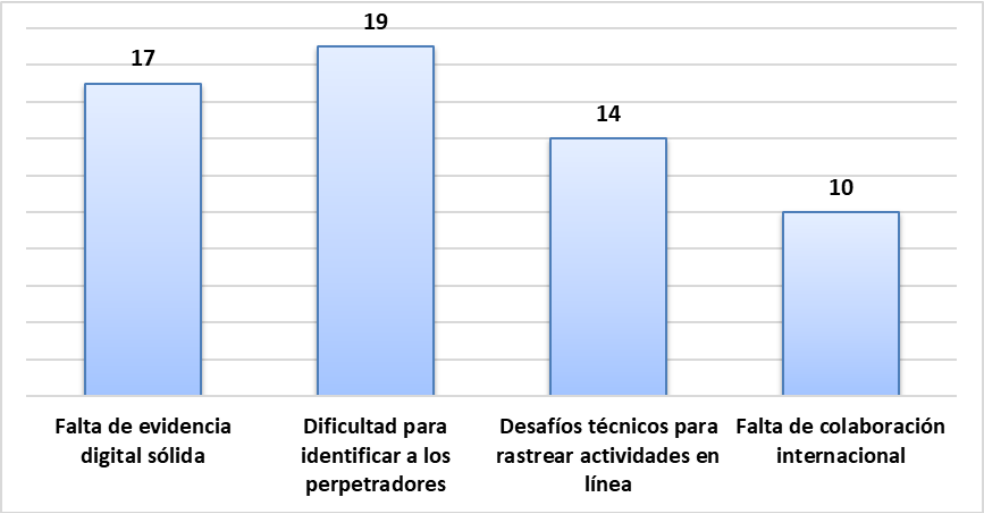


Figura 7. Percepción sobre principales obstáculos para llegar a una imputación en casos de cibercrimen en la UJ N° 3. N = 20.

Nota: la suma excede a N porque los encuestados podían marcar más de una opción.

La percepción de los encuestados coincide nuevamente con las aportaciones de los autores analizados en el marco teórico, que se vinculan con las características específicas que tiene el ciberdelito en cuanto al anonimato de los perpetradores (Temperini, 2018; Violat, 2020); las dificultades que surgen en la obtención y preservación de la evidencia digital (Borzi Cirilli, 2018; Cenci, 2022; Esteban, 2019; Téllez Valdés, 2008; Temperini, 2018), la ocurrencia de estos delitos en un "lugar" o ámbito deslocalizado como el ciberespacio (Miró Llinares, 2012), y las dificultades derivadas del carácter trasnacional de estos delitos, no solo porque pueden abarcar jurisdicciones de distintos países, sino también porque el Poder Judicial depende de empresas telefónicas o proveedoras de servicios de internet que, o bien no proporcionan datos de sus usurarios o bien porque sus sedes centrales se encuentran en el exterior, principalmente en Estados Unidos, lo que ocasiona importantes demoras o trabas para el desarrollo del proceso penal (Esteban, 2019; Justo, 2017; Téllez Valdés, 2008; Temperini, 2018).

4.4. Recursos y Capacitación

Por las características propias de este tipo de delitos, la capacitación del personal y los recursos técnicos con los que cuenta son cruciales para llevar adelante la investigación penal probatoria en casos de cibercrimen. En relación con la capacitación, el 65% de los encuestados considera que fue "Suficiente. Sirve para conocer el tema" y el 35% que fue "Escasa. No alcanza para estar al tanto del tema". Cabe señalar que ninguno de los encuestados consideró los extremos, es decir, ni "Nula" ni "Excelente" (Figura 8).

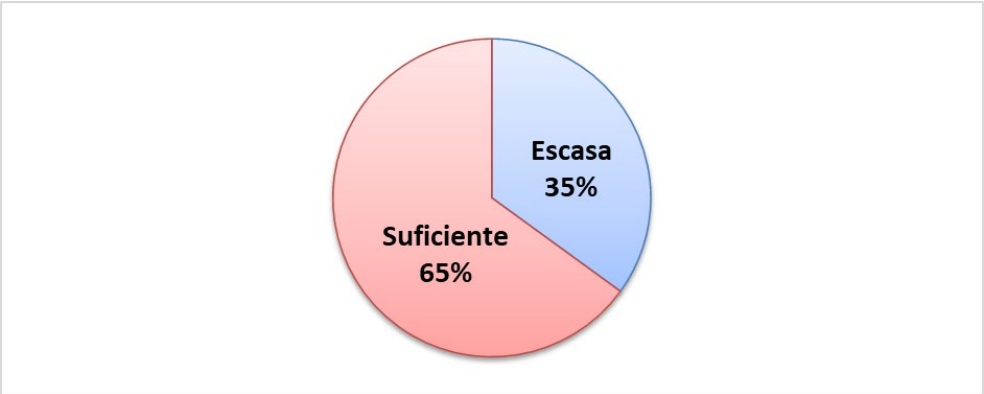


Figura 8. Percepción sobre la capacitación recibida en cibercrimen en la UJ N° 3. N = 20.

En este punto resulta de interés hacer un desagregado por perfil de los encuestados. Así, en la Tabla 5 se observa que entre los funcionarios jurisdiccionales y los del Ministerio Público Fiscal es mayor la percepción sobre haber recibido una capacitación suficiente, así como entre el grupo de policías de investigación.

Tabla 5. Percepción sobre la capacitación recibida en cibercrimen. Desagregado por cargo.

Capacitación	**Suficiente**		**Escasa**	
Cargo	**Total**	**%**	**Total**	**%**
Funcionarios Jurisdiccionales	3	75%	1	25%
Funcionarios MPF	5	71%	2	29%
Técnicos Informáticos	1	50%	1	50%
Miembro del Equipo de Policía Judicial	0	0%	1	100%
Policías de Investigación	4	67%	2	33%
	13	**65%**	**7**	**35%**

En relación con la percepción de los encuestados sobre si son suficientes los recursos técnicos con los que cuenta la Unidad Judicial N° 3 para investigar cibercrimen de manera efectiva, todos manifestaron que no. Este dato representa un problema importante dada la evolución y sofisticación de este tipo de delitos, que requieren no solo de personal capacitado en esta área, sino también de los recursos que permitan una investigación efectiva.

4.5. Colaboración y Coordinación

La coordinación y colaboración entre los distintos actores que intervienen en la investigación penal probatoria son factores importantes para llegar a un resultado efectivo. En este sentido, el 55% de los encuestados considera que es suficiente y el 45% que es poca (Figura 9).

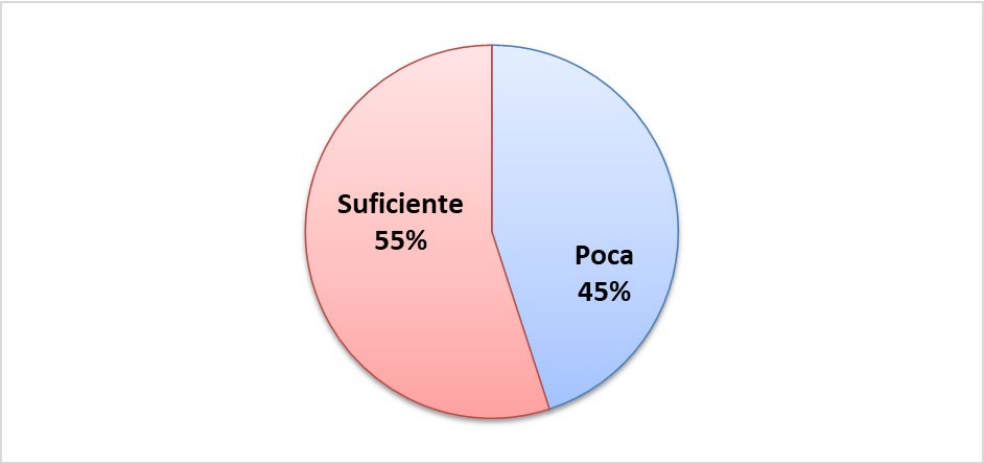


Figura 9. Percepción sobre la comunicación entre las unidades de policía, fiscalía y peritos informáticos en casos de cibercrimen. N = 20.

Aquí nuevamente resulta de interés observar esta percepción en el desagregado según el perfil de los encuestados. En la Tabla 6 se observa que entre los funcionarios jurisdiccionales y los del Ministerio Público Fiscal es mayor la percepción sobre un nivel de colaboración y coordinación suficiente; sin embargo, es significativo que el 67 % de los policías perciba que existe poca colaboración y coordinación, lo que entorpece desde el inicio la investigación por ser ellos los primeros eslabones del proceso (ver Tabla 6).

Tabla 6. Percepción sobre la colaboración con otras dependencias. Desagregado por cargo.

Coordinación/Colaboración	**Suficiente**		**Poca**	
Cargo	**Total**	**%**	**Total**	**%**
Funcionarios Jurisdiccionales	3	75%	1	25%
Funcionarios MPF	5	71%	2	29%
Técnicos Informáticos	1	50%	1	50%
Miembro del Equipo de Policía Judicial	0	0%	1	100%
Policías de Investigación	2	33%	4	67%
	11	**55%**	**9**	**45%**

Se comprueba lo señalado por Arce et al (2011) en que la falta de información se traduce en dificultades a la hora de tomar decisiones y proyectar un posible escenario.

4.6. Sugerencias y Conclusiones

El último punto del cuestionario es una pregunta abierta en la que se pide a los encuestados que formulen o planteen qué medidas consideran que podrían ayudar a mejorar la tasa de imputación en casos de cibercrimen en Córdoba. En el grupo de funcionarios jurisdiccionales se destacan dos aspectos a mejorar: por un lado, el normativo, y por otro, el referido a la formación. En palabras de los encuestados:

Es fundamental atacar el problema desde dos aspectos. El primero legislativo, mejorando y actualizando las normas vigentes a fin de dar cabida a las nuevas modalidades delictivas asociadas al ciberespacio y por otra parte mejorar los recursos técnicos y humanos con que se cuenta, fundamentalmente en sedes del interior como Río Cuarto. (Funcionario Jurisdiccional 1).

Los tribunales y su personal deberían contar con la formación suficiente para poder trabajar con tipos delictivos tan dinámicos como estos ante los que nos encontramos. Dotar de recursos humanos a sedes como Rio Cuarto que son ciudades grandes pero no capitales, es muy necesario para que la investigación se pueda llevar a cabo in situ y no deba ir a Córdoba (Funcionario Jurisdiccional 2).

Se debe trabajar en una reforma al sistema normativo penal en su conjunto, ya que actualmente hay tipos delictivos superpuestas, legislados por el propio código penal y luego también y de forma superpuesta, por leyes especiales. Esto es muy notorio en el tema cibercrimen, toda vez que aquí nos encontramos con modalidades delictivas que son preexistentes a las nuevas tecnologías, y por ende ya se encontraban legisladas desde hace décadas, pero que actualmente encontraron en las nuevas TIC, formas novedosas para que los criminales las lleven adelante (Funcionario Jurisdiccional 3).

Es responsabilidad de cada miembro del poder judicial, así como de la policía y organismos de investigación, mantenerse formado y actualizado respecto a esa dinámica tan cambiante que es la cibercriminalidad. Igualmente sería deseable que el estado invierta más en ciberseguridad y en dotar a los órganos de investigación de mayor personal y equipamiento técnico. El aumento de las penas para ciertos delitos de tipo informático, fundamentalmente aquellos en los que haya ataques a la intimidad de las personas, es otro elemento que debe incorporarse. (Funcionario Jurisdiccional 4).

Entre los funcionarios del Ministerio Público Fiscal aparece también la necesidad de actualizar la normativa nacional y procesal a nivel provincial:

> *Actualizar de forma urgente la normativa nacional de fondo y procesal a nivel provincial para dar cobertura a las nuevas modalidades delictivas asociadas con las nuevas tecnologías.* (Funcionario del MPF 3).
>
> *Actualizar la legislación. Crear organismos que contribuyan a la investigación de este tipo de causas. Aumentar las penas para estos delitos a fin de que se pueda detener con prisión preventiva a los autores.* (Funcionario del MPF 5).
>
> (…) *adecuación del marco normativo a las nuevas tecnologías y a los delitos que de ella se puedan derivar.* (Funcionario del MPF 6).

En este grupo también se destaca la necesidad de incrementar la cantidad de personal especializado y recursos técnicos para atender este tipo de delitos:

> *Incrementar el personal y los recursos técnicos con los que cuentan, tanto las dependencias judiciales, como los organismos policiales destinados a la investigación de estos delitos. Crear nuevas oficinas dedicadas especialmente a la investigación de estos delitos, ya que las Fiscalías o Unidades judiciales comunes muchas veces no poseen tiempo ni recursos suficientes para estas investigaciones.* (Funcionario del MPF 2).
>
> (…) *mejorar en cantidad de personal y equipos técnicos que coadyuven a la investigación de este tipo de delitos.* (Funcionario del MPF 3).
>
> *Fijar a la ciberdelincuencia como prioridad a la hora de plantear las políticas criminales, tanto a nivel nacional como provincial, dándole los recursos humanos y técnicos que por este estado de prioridad le correspondan* (Funcionario del MPF 4).
>
> *Descomprimir a las Unidades Judiciales comunes de la investigación de estos delitos, ya que al estar tan saturadas de denuncias de hechos delictivos "comunes", es poco el tiempo o la dedicación que se puede poner en investigar este tipo de hechos.* (Funcionario del MPF 7).

Uno de los encuestados del Ministerio Público Fiscal también destaca la necesidad de descentralizar la investigación de ciberdelitos:

> *Deberían existir dependencias especializadas en investigación de ciberdelitos en las sedes más importantes del interior de la provincia de Córdoba, descentralizando esta actividad de la ciudad capital. Igualmente debería aumentar el número de personal especializado en dicha temática en la estructura del poder judicial.* (Funcionario del MPF 1).

Los Técnicos Informáticos y el Miembro del del Equipo de Policía Judicial también se enfocan en la necesidad de capacitación, el incremento de personal y la descentralización:

> (…) *En la sede Rio Cuarto considero que sería importante mejorar la capacitación, aumentar el personal y el equipamiento para que se pueda trabajar acá en la investigación de los ciberdelitos y esto no tenga que irse a Córdoba ya que allá están abarrotados de trabajo con sus propias causas también*. (Técnico Informático 2).

> *Dentro de la tarea que desempeño como coordinador del Cuerpo Operativo de Policía Judicial de Río Cuarto creo que sería importante dotar a la delegación local de personal idóneo en la materia, ya que actualmente todo el trabajo se desarrolla en la ciudad de Córdoba*. (Miembro del del Equipo de Policía Judicial).

En el grupo de policías encuestados aparecen las mismas cuestiones sobre los aspectos que se podrían contribuir a mejorar la tasa de imputación en casos de cibercrimen en la Unidad Judicial N° 3 de Río Cuarto:

> *Mejorar la capacitación, aumentar la cantidad de personal que pueda investigar este tipo de delitos.* (Policía de Investigación 1).

> *Crear un área específica de investigación de causas complejas como las de cibercrimen, dentro de la jurisdicción de Río Cuarto para que pueda encargarse de estos temas.* (Policía de Investigación 2).

Mejorar los equipos con los que cuenta la policía y la justicia para investigar este tipo de delito, así como incorporar personal con conocimientos en informática. (Policía de Investigación 3).

Aumentar la cantidad de personal y recursos con los que cuentan las unidades judiciales y las oficinas técnicas que colaboran en la investigación de estos delitos. (Policía de Investigación 4).

Mejorar las leyes que regulan los delitos más nuevos y que hoy no están regulados, aumentar el personal de investigaciones. (Policía de Investigación 5).

Dar más capacitación al personal que trabaje en investigar estos delitos y aumentar la cantidad de recursos para investigar estos delitos. (Policía de Investigación 6).

El análisis cuantitativo que resume las propuestas de mejora que sugieren los encuestados – y que se vinculan directamente con los obstáculos que se presentan en esta ciudad, donde funciona la Unidad Judicial 3, para llevar adelante de manera exitosa la investigación penal preparatoria – muestra que una de las áreas críticas es la necesidad de incrementar los recursos humanos y técnicos (31%), seguida de la capacitación del personal (25%), y de la descentralización y actualización del marco normativo (22% cada una). (Figura 10).

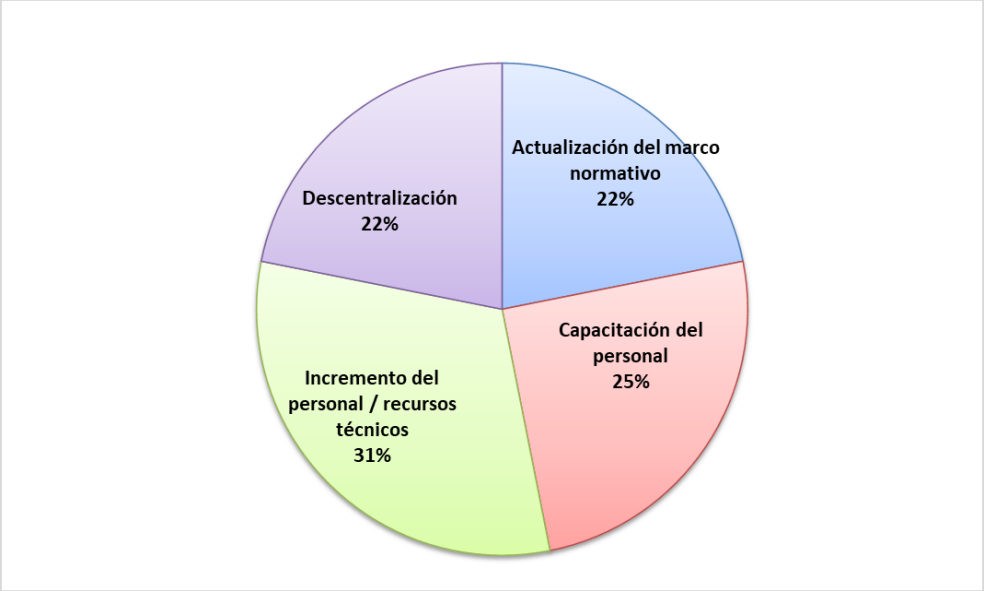


Figura 10. Resumen de las propuestas de mejoras para optimizar la investigación en casos de cibercrimen en la UJ N° 3. N = 20.

5. CONCLUSIONES

El propósito de este trabajo fue analizar cuáles son las causas y obstáculos que enfrentan en la ciudad de Río Cuarto, tomando como unidad de análisis la Unidad Judicial N° 3 de esa ciudad, provincia de Córdoba, Argentina, para la Investigación Penal Probatoria en los casos de cibercrimen. La motivación fue que un relevamiento estadístico realizado a partir de datos consignados en el Libro de Sumarios de correspondiente al periodo 2021-2023 (julio) e esta unidad Judicial arrojó como diagnóstico que a pesar de estar identificados los autores de diferentes tipos de ciberdelitos, solo 2 resultaron imputados.

A partir de estos datos se plantearon como hipótesis que existe una combinación de circunstancias que contribuyen negativamente a la efectiva imputación de los delitos. La primera hipótesis fue que la *escasez de personal* frente al gran volumen de trabajo hace muy difícil que el instructor de la causa pueda dedicarse a instruir un expediente por un hecho de cibercrimen, quedando relegadas estas causas por otros hechos mayor gravedad y urgencia. A pesar de que los encuestados no consideraron a la escasez de personal entre los desafíos y obstáculos que enfrenta la investigación de cibercrimen en esta unidad Judicial, aparece como mejora prioritaria la necesidad de incrementar los recursos humanos y técnicos, lo que permite comprobar la hipótesis planteada.

La segunda hipótesis fue que la *capacitación específica en investigaciones de cibercrimen* es escasa o nula. El 65% de los encuestados considera que la capacitación recibida en cibercrimen en el área de competencia de la UJ N° 3 fue suficiente, sin embargo, la necesidad de capacitación aparece como el segundo aspecto en las propuestas de mejoras para optimizar la investigación en casos de cibercrimen en esta Unidad Judicial. A la luz de estos datos, se afirma que esta hipótesis se comprobó parcialmente, ya que no se puede considerar como escasa o nula, pero tampoco como suficiente ya que es reclamada por los encuestados.

Se comprueba la tercera hipótesis, referida a que la *centralización de recursos investigativos científico/técnicos en la ciudad de Córdoba* atenta contra un diligenciamiento rápido de la instrucción desde una ciudad del interior de la provincia como Rio Cuarto, dado que en varias respuestas se plantea la necesidad de contar con

dependencias especializadas en investigación de ciberdelitos en las sedes más importantes del interior de la provincia de Córdoba, como es el caso de la ciudad de Río Cuarto.

Finalmente, también se comprueba que el *marco normativo* – tanto nacional como provincial – resulta insuficiente para dar respuesta a estas modalidades delictivas. Varios encuestados han referido que las normas vigentes no incluyen a las nuevas modalidades delictivas asociadas al ciberespacio, que evolucionan de manera constante, y por otra parte, hay tipos delictivos legislados por el propio Código Penal pero también y de forma superpuesta, por leyes especiales.

Los hallazgos obtenidos en este trabajo de campo confirman los análisis aportados en el marco teórico sobre las dificultades para la Investigación Penal Preparatoria en casos de cibercrimen, vinculadas con el atraso de la ley frente a los avances e innovaciones de esta modalidad delictiva, la cooperación con diversas empresas proveedoras de servicios de internet que son las poseedoras de información relevante, y con aspectos claves como el "lugar del hecho" (deslocalizado en el ciberespacio) y la obtención y conservación sin contaminación de la "evidencia digital" (inmaterial, frágil, volátil, y en consecuencia, difícil de rastrear).

Pero también dan cuenta de problemas estructurales al interior de las Unidades Judiciales como la escasez de personal o la capacitación y recursos técnicos insuficientes. En este sentido, es necesario reforzar la idea de que es necesario que tanto las fuerzas policiales como todos los actores que intervienen en el proceso deben poseer los medios técnicos, las capacidades y la formación especializada en el uso de herramientas y dispositivos digitales, no solo para luchar de manera eficaz contra las formas sofisticadas de cibercrimen sino también para obtener y manejar correctamente las evidencias digitales.

Es muy probable que si se replica esta misma investigación en otras Unidades Judiciales se obtengan resultados similares, por lo que resulta recomendable continuar con esta línea de investigación para superar o mitigar los nuevos desafíos que presentan los delitos informáticos. Y en este sentido, como conclusión general de este trabajo se coincide con Marcelo Temperini (2018) cuando afirma que:

> La superación o mitigación de estos desafíos que nos presentan los delitos informáticos involucran aspectos técnicos, jurídicos, socioculturales y políticos que requieren mejorar los niveles de

capacitación de todos los actores intervinientes en el proceso judicial, así como un abordaje serio por parte del Estado (en sus distintos niveles), basado en la previa comprensión y dimensionamiento de la problemática que implica el cibercrimen en Argentina. (p.68).

BIBLIOGRAFÍA

Arce, J., Galli Funes, J. P. & Zabala, D. (2011). *Pautas informativas y procedimentales en ciberdelitos. Experiencia de la Ciudad de Córdoba*. [conferencia. IX Simposio Argentino de Informática y Derecho (SID 2011). Córdoba, 29 de agosto al 2 de septiembre de 2011. http://sedici.unlp.edu.ar/bitstream/handle/10915/134329/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y.

Arocena Alonso, L. (2016). *La odisea procesal de la criminalidad informática* [tesis de grado]. Universidad del País Vasco / Euskal Herriko Unibertsitatea. https://www.pensamientopenal.com.ar/system/files/2016/08/doctrina43936.pdf.

Augé, M. (1993). *Los no lugares. Espacios del anonimato. Antropología de la Sobremodernidad*. Ed. Gedisa.

Binder, A. (2009). *Introducción al Derecho Procesal Penal*. 2ª ed. Ad-Hoc.

Borzi Cirilli, F. (2018). Cibercrimen y evidencia digital: problemática probatoria. En R. A. Parada y J.D. Errecaborde (comp.). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (pp.173-182). Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf.

Cafferata Nores, J., Tarditti, A., & Arocena, G. (2003). *Código Procesal Penal de la Provincia de Córdoba comentado*. Ed. Mediterránea.

Cenci, M. (2022). *Evidencia digital* [trabajo final especialización en Derecho Penal y Ciencias Penales]. Universidad de Comahue. http://rdi.uncoma.edu.ar/bitstream/handle/uncomaid/16652/CENCI%20MATIAS%20-%20TRABAJO%20INTEGRADOR%20ESPECIALIZACION%20EN%20DERECHO%20PENAL-convertido.pdf?sequence=1&isAllowed=y.

Esteban, B. (2019). *Delitos contra la integridad sexual de niños, niñas y adolescentes en Internet: el 'grooming' o acoso sexual de menores en línea* [trabajo final integrador]. Universidad Nacional de Quilmes. https://www.pensamientopenal.com.ar/system/files/2019/06/doctrina47708.pdf.

Finocchiaro, E. (2015). La investigación penal preparatoria y la etapa de control en el sistema acusatorio. *Revista Pensamiento Penal* [en línea], 1-32. https://www.pensamientopenal.com.ar/system/files/2015/09/doctrina42114.pdf.

González García, A., & Campoy Torrente, P. (2018). Ciberacoso y cyberbullying: diferenciación en función de los precipitadores situacionales. *Revista Española De Investigación Criminológica, 16*, 1–31. https://doi.org/10.46381/reic.v16i0.149.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, M. P. (2010). *Metodología de la investigación*. 6ª Edición. McGraw-Hill.

Justo, M. (2017). *Evidencia Digital e Investigación del Cibercrimen. Estado del Arte. Análisis y desafíos técnico forenses*. Jornada de Trabajo "Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal". Asociación por los Derechos Civiles (ADC). https://adc.org.ar/wp-content/uploads/2019/06/032-evidencia-igital-investigacion-de-cibercrimen-y-garantias-del-proceso-penal-jornada-de-trabajo-12-2017.pdf.

Mateos, I. (2013). *Ciberdelincuencia, desarrollo y persecución tecnológica* [trabajo final de grado]. Universidad Politécnica de Madrid. http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf.

Miró Llinares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Secretaría de Innovación Tecnológica (2022). *Delitos informáticos en Argentina: modalidades detectadas durante la pandemia del COVID-19*. https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf.

Téllez Valdés, J. (2008). *Derecho informático*. 4ª ed. - Ed. Mc Graw Hill.

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. En R. A. Parada y J.D. Errecaborde (comp.). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (pp.49-68). Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf.

Violat, M. (2020). El perfil del ciberdelincuente: los patrones del mal. *Derecho de la Red* [en línea]. https://derechodelared.com/perfil-ciberdelincuente/.

Normativa Consultada

Ley 8.123/1992. *Código Procesal Penal de la Provincia de Córdoba*. http://www.saij.gob.ar/8123-local-cordoba-codigo-procesal-penal-provincia-cordoba-lpo0008123-1991-12-05/123456789-0abc-defg-321-8000ovorpyel.

Ley 11.179/1984. *Código Penal* (actualizado). https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/actualizacion#17.

Ley 26.388/2008. *Modificación del Código Penal*. *Incorporación de delitos informáticos*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

Ley 26.904/2013. *Modificación del Código Penal*. *Incorporación de delitos contra la integridad sexual de menores*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm.

Ley 27.411/2017. *Convenio sobre Ciberdelito del Consejo de Europa*. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798.

ANEXOS

Anexo I. Cuestionario

ENCUESTA SOBRE EL CIBERCRIMEN Y LA INVESTIGACIÓN PENAL EN EL SUR DE CÓRDOBA

Se agradece la disposición para participar en esta encuesta. El objetivo de esta investigación es analizar los desafíos y factores que podrían estar contribuyendo a la falta de imputados/detenidos/condenados en casos de cibercrimen en la provincia de Córdoba, a partir de datos estadísticos de acceso público del sistema judicial. Las respuestas aportadas significan un valioso aporte para comprender mejor esta problemática y proponer posibles soluciones en el futuro.

Queremos asegurarle que sus respuestas serán tratadas con confidencialidad y anonimato. Los resultados de esta encuesta serán utilizados exclusivamente con fines de investigación y análisis, y ningún dato personal que pueda identificarlo/a será compartido o divulgado en ningún momento.

PARTE I: INFORMACIÓN DEMOGRÁFICA

1. ¿Cuál es su rol en el sistema de justicia? (Seleccionar una opción)

( ) Policía

( ) Fiscal/Funcionario del MPF

( ) Juez/Funcionario Área Jurisdiccional

( ) Perito Informático

( ) Otro (indicar): _____

2. ¿Cuántos años de experiencia tiene en su rol actual? _____

3. ¿Está familiarizado/a con los conceptos de "cibercrimen" y "delitos informáticos" en el contexto legal?

SI / NO

PARTE II: PERCEPCIÓN DEL CIBERCRIMEN Y SU INVESTIGACIÓN

4. Del 1 al 5, ¿cuán grave considera el delito cibernético en general? (siendo 1 sin gravedad, y 5 muy grave). _____

5. ¿Cómo valora o qué opinión tiene sobre la legislación vigente en torno al cibercrimen?

_____

_____

_____

6. ¿Qué desafíos considera que enfrenta la investigación de cibercrimen en Córdoba? (*Seleccionar todas las que apliquen*)

( ) Falta de recursos técnicos

( ) Falta de conocimiento especializado

( ) Dificultad para rastrear actividades en línea

( ) Falta de legislación adecuada

( ) Otros. Especificar: _____

PARTE III: PROCESO DE INVESTIGACIÓN Y RESULTADOS

7. ¿Ha tenido experiencia en investigaciones de cibercrimen?

SI / NO

8. En caso de haber respondido sí en la anterior pregunta, o aun respondiendo NO pero trabajando con otras personas que sí han realizado este tipo de investigaciones en su oficina: ¿cuántas denuncias de cibercrimen han sido registradas en su unidad en el último año?

( ) Menos de 100

( ) Entre 100 y 500

( ) Entre 500 y 2000

( ) Entre 2000 y 10000

( ) Más de 10000

9. ¿Cuántas de estas denuncias resultaron en la imputación de los presuntos autores?

( ) Ninguna

( ) Menos del 10%

( ) Entre el 10% y el 25%

( ) Entre el 25% y el 50%

( ) Entre el 50% y el 75%

( ) Más del 75%

( ) El 100%

10. ¿Cuáles considera que son los principales obstáculos para llegar a una imputación en casos de cibercrimen? (*Seleccionar todas las que apliquen*)

( ) Falta de evidencia digital sólida

( ) Dificultad para identificar a los perpetradores

( ) Desafíos técnicos para rastrear actividades en línea

( ) Falta de colaboración internacional

( ) Otros. Especificar: _____

PARTE IV: RECURSOS Y CAPACITACIÓN

11. ¿Ha recibido capacitación específica en investigaciones de cibercrimen? Marque la opción que más se acerque a lo que piensa.

( ) Nula, no recibí capacitación al respecto.

( ) Escasa. No alcanza para estar al tanto del tema.

( ) Suficiente. Sirve para conocer el tema.

( ) Excelente. La capacitación fue perfecta.

12. ¿Considera que su unidad cuenta con suficientes recursos técnicos para investigar cibercrimen de manera efectiva?

SI / NO

PARTE V: COLABORACIÓN Y COORDINACIÓN

13. ¿Cómo valora la comunicación entre las unidades de policía, fiscalía y peritos informáticos en casos de cibercrimen?

( ) Nula.

( ) Poca.

( ) Suficiente.

( ) Excelente.

PARTE VI: SUGERENCIAS Y CONCLUSIONES

14. ¿Qué medidas o mejoras considera que podrían ayudar a mejorar la tasa de imputación en casos de cibercrimen en Córdoba?

_____

_____

_____