FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho y Ciencias Políticas

"Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020"

Tesis para optar el título profesional de:

Abogado

Autores:

Jany Giovana Bernal Gallardo
Bertho Arturo Menacho Ortega

Asesor:

Mag. Alfredo Enrique Pérez Bejarano

Lima - Perú

2021

DEDICATORIA

A mis padres, Juana Elena Gallardo Miguel e Ildefonso Severiano Bernal Rejano por ser los principales promotores de mis sueños y brindarme su amor y paciencia incondicional.

A mi hermana, Kelli Elena Bernal Gallardo y a mi prima hermana, Leila Amaya Gallardo por su apoyo incondicional para culminar la primera meta profesional en mi formación académica.

A mis tíos, Máxima Gallardo Miguel y Adler Amaya Huaytalla, quienes fallecieron durante la pandemia, me quedo con sus enseñanzas y sé que les gustaría que la familia vuelva a sonreír, amar y seguir adelante.

Al titular de mi afectividad, Bertho Arturo Menacho Ortega, por ser mi inspiración y compañero de vida.

A todas las personas que me apoyaron y han colaborado que el trabajo se realice con éxito.

Jany Giovana Bernal Gallardo

A mis padres, Bertho Delgado Menacho Cano y Santos Ortega Vega por ser mis ejemplos de superación e inculcarme siempre la importancia de la familia.

A mis hermanos, Jorge Rodrigo Menacho Ortega y Luis Alberto Suyón Ortega por enseñarme que no existe mayor confianza, amor y lealtad que la profesada entre los integrantes de tu propia sangre.

A mis familiares fallecidos que durante su estancia en este espacio terrenal me permitieron comprender la importancia de vivir plenamente cada día de mi vida.

A la titular de mi afectividad, Jany Giovana Bernal Gallardo, por ser mi complemento perfecto y mi estabilidad emocional a lo largo de mi vida.

A todas las personas que, en algún pasaje de mi vida, me brindaron su apoyo o fueron mi ejemplo de superación profesional.

Bertho Arturo Menacho Ortega

AGRADECIMIENTO

A Dios por brindarnos la vida y permitirnos aprender a convertir las dificultades en oportunidades, así como por la posibilidad de ayudar a otras personas a intentar ser mejores cada día.

A nuestro destacado asesor, el Mag. Alfredo Enrique Pérez Bejarano por su orientación, confianza y respaldo durante la elaboración de la tesis.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente estudio tuvo como objetivo evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de los delitos informáticos desde los roles fiscal, judicial y policial. El propósito de la investigación fue básico con enfoque mixto, diseño no experimental, alcance exploratorio y método sociológico.

Los principales resultados fueron el elevado archivamiento de las investigaciones fiscales, las mínimas sentencias condenatorias emitidas, la desconfianza social en la administración de justicia y las deficiencias logísticas en tecnología, infraestructura y recursos humanos técnicos especializados.

Las limitaciones fueron divididas en dos vertientes, la primera vinculada a los autores en donde se destacaron la limitación teórica, la viabilidad de las fuentes, los recursos económicos y la limitación temporal, mientras que la segunda se relaciona a la investigación, entre ellas, el contexto de la población, los recursos humanos y la ubicación geográfica. Ahora bien, las implicancias o implicaciones se dividieron en prácticas, teóricas y metodológicas, exponiendo la importancia de la investigación.

Finalmente, se concluyó que nuestra administración de justicia, conformada por el Ministerio Público, Poder Judicial y Policía Nacional del Perú, no resulta apropiada para procesar la comisión de los delitos informáticos y delitos tradicionales cometidos en medios tecnológicos.

Palabras clave: Delitos informáticos, tecnología, ciberespacio y Sistema de Justicia.

ABSTRACT

This current study was aimed to evaluate whether the Justice Administration System in Peru is qualified to process the commission of cybercrimes from the prosecutor, judicial and police role. The research was conducted with a mixed approach that included a non-experimental design, exploratory scope, and sociological methods.

The main findings from the research were the excessive prosecutor cases that had to be filed, minimal convictions issued, as well as social mistrust in the administration of justice. There were also logistical deficiencies in technology, infrastructure, and specialized technical human resources.

Limitations were divided into two aspects, the first aspect is linked to the authors where the theoretical limitation, the viability of the sources, the economic resources and the temporal limitation stood out. The second is related to the research, which includes, the context of population, human resources and geographic location. Also, the implications or implications were divided into practical, theoretical and methodological, exposing the importance of the research.

Finally, it was concluded that our administration of justice, made up of the Public Ministry, the Judiciary and the National Police of Peru, is not appropriate to prosecute the commission of computer crimes and traditional crimes committed by technological means.

Keywords: Cybercrime, technology, cyberspace, and Justice System.

CAPÍTULO 1. INTRODUCCIÓN

1.1. Realidad problemática

1.1.1. Presentación y descripción del problema

El presente trabajo se enmarca en la línea de investigación de Tecnologías Emergentes, teniendo como sub línea de investigación a las Nuevas Tecnologías. Asimismo, pretende estudiar la situación actual del Sistema de Justicia del Perú, desde sus tres principales órganos, estos son, la Fiscalía, el Juzgado y la Policía Nacional del Perú, dado que el tratamiento de esta clase de delitos, así como el entorno en el que se cometen, exige que las autoridades cuenten con un nivel cognoscitivo de especialización superior, el cual no puede ser suplantado por capacitaciones tradicionales impartidas mediante la Escuela de Capacitación del Ministerio Público y la Academia de la Magistratura, respectivamente, tal y como desarrollaremos más adelante.

La relevancia de este trabajo está relacionada con la capacidad de respuesta con la que contamos actualmente en nuestro Sistema de Justicia. De un lado, los persecutores del delito, quienes son los llamados a ejercer la acción penal pública ante el conocimiento de una posible noticia criminal de parte o difundida por los medios de comunicación. De otro lado, los órganos jurisdiccionales que imparten justica en nuestro país. Ambos cuentan con diversas herramientas jurídicas útiles para la atención de delitos cometidos en una circunscripción geográfica física. Sin embargo, aún son precarios e incipientes los conocimientos especializados en materia de ciberdelincuencia, por lo que resultaría inapropiado el procesamiento de delitos informáticos y no se estaría administrando justicia correctamente.

En la misma línea, es inaceptable que solo tengamos Fiscalías Especializadas en Corrupción de Funcionarios, Criminalidad Organizada, Materia Ambiental, entre otros, y hasta la fecha no hayamos incorporado una Fiscalía Especializada en Ciberdelincuencia, sabiendo que su complejidad no termina con un par de cursos de capacitación que pueden ser dictados a los operadores de justicia, sino que es insustituible la creación de Fiscalías que tengan un correlato igualmente especializado en el Órgano Jurisdiccional que imparte justicia en nuestro país.

El aporte de este trabajo de investigación es uno de los primeros que propugna la incorporación de Fiscalías y Juzgados Especializados en Ciberdelincuencia, con lo que se conseguiría una mayor seguridad jurídica de las partes intervinientes, se generaría

confianza y satisfacción en las presuntas víctimas y se reforzaría el nivel de especialización en las entidades de la administración de justicia.

1.1.1.1. La evolución tecnológica

La evolución tecnológica permitió que el ser humano pueda satisfacer sus múltiples necesidades a lo largo de la historia, en la medida que la ciencia realizaba grandes aportes a la humanidad y contribuía de forma holística en los distintos campos de la demanda social, también se intensificaba la lucha contra la delincuencia cibernética. Un mundo totalmente desconocido empezaba a cobrar sus primeras víctimas en una circunscripción delictiva diferente, esto es «El Ciberespacio».

El intento fallido de nuestras autoridades al combatir con delincuentes altamente calificados y especializados, no solo en el campo tecnológico, pues su impacto incluye aspectos como el económico, político y social, propició que estos sujetos actúen en el anonimato, asumiendo un rol específico en las organizaciones criminales que en la mayoría de los casos trascienden las fronteras de nuestro país, alcanzando espacios inubicables en todo el mundo.

A lo largo de la historia, hemos evidenciado cómo avanzó y evolucionó la ciencia a nivel mundial, con la aparición de «la internet», en el año de 1969, fecha en la que se estableció la primera «red sin nodos centrales», conocida como ARPANET, esto es la agencia «Advanced Research Projects Agency» conocida por sus siglas ARPA, la cual fue creada en el año 1958 por el departamento de defensa norteamericano con el objetivo de poner en práctica las creaciones tecnológicas al campo de la milicia, en respuesta a la creación rusa del satélite soviético «Sputnik» (Aranda, 2004).

1.1.1.2. El Convenio de Budapest

El Convenio Internacional sobre Ciberseguridad es considerado un tratado multilateral adoptado por el Consejo de Europa, el 23 de noviembre de 2001 en la ciudad de Budapest – Hungría, en dicho instrumento mundial se establecieron las reglas de cooperación internacional para afrontar a las nuevas amenazas en la era digital, mediante la armonización de la legislación nacional y las técnicas investigativas (EFE News Service, 2019).

Es a partir de la Resolución Legislativa N° 30913, aprobado con fecha 12 de febrero de 2019 que a su vez, aprobó el Convenio sobre la Ciberdelincuencia, el mismo que fue ratificado mediante el Decreto Supremo N° 010-2019-RE y entró en vigencia el 01

de diciembre de 2019. Al realizar la suscripción de este Convenio nuestro país asumió el compromiso de confrontar efectivamente a la ciberdelincuencia. En ese sentido, pasaremos a detallar si contamos con los órganos especializados para esta nueva forma de criminalidad.

1.1.1.3. Las Fiscalías y Juzgados no Especializados en Ciberdelincuencia

De un lado, la conceptualización de fiscal en palabras del Ministerio Público Fiscalía de la Nación del Perú (2020) lo describe como el previsor y persecutor del delito, así también señala que es el defensor de la legalidad en salvaguarda de los intereses públicos tutelados por la ley. Asimismo, son considerados los representantes de la sociedad y los comisionados a velar por la recta y efectiva administración de justicia.

Actualmente, existen delitos que se cometen en espacios delictivos cibernéticos, esto es, «El Ciberespacio», en la descripción realizada por El Centro Curtis E. LeMay para el Desarrollo y la Educación de la Doctrina (2011), en adelante [Centro Curtis E. LeMay], lo considera como el dominio concebido por el hombre y como tal dependiente a la atención ininterrumpida de su creador para su persistencia, la cual comprende tres aspectos sustanciales, la especificidad, el alcance global y el énfasis en el espectro electromagnético. A su vez, existen los dominios brindados por la naturaleza, tales como el aire, la tierra, el mar y el espacio. Dicho Centro agrega que los nodos del ciberespacio permanecen en su espectro físico en todos los dominios.

Asimismo, el Centro Curtis E. LeMay (2011) incluye como parte de su descripción sobre el ciberespacio que "(…) las actividades en el ciberespacio pueden permitir la libertad de acción para actividades en los otros dominios, y las actividades en los otros dominios pueden crear efectos en y a través del ciberespacio" (párr. 6). Ante ello, se puede extraer que el ciberespacio contiene dos dominios esencialmente distintos, pero que dependen el uno del otro para surtir efectos.

Ahora bien, proyectemos imaginariamente la situación de los fiscales en el Perú. Empezaremos por reconocer la falta de recursos humanos y logísticos para cubrir la demanda de esta nueva clase de delitos en todo el país. Siguiendo la misma lógica, nuestros persecutores de delitos no cuentan con conocimientos especializados vinculados al complejo universo de la ciberdelincuencia. Distinto es el caso de los titulares de la acción penal que cuentan con las siguientes fiscalías especializadas:

Tabla 1

Distribución de las Fiscalías Especializadas en el Perú

Fiscalías Especializadas
Fiscalía Especializada en Corrupción de Funcionarios
Fiscalía Especializada en Criminalidad Organizada
Fiscalía Especializada en Lavado de Activos y Pérdida de Dominio
Fiscalía Especializada en Materia Ambiental
Fiscalía Especializada en Tráfico Ilícito de Drogas
Fiscalía Especializada en Trata de Personas
Fiscalía Especializada en Delitos Tributarios
Fiscalía Especializada en Delitos Aduaneros y contra la Propiedad Intelectual

Fuente: Elaboración propia a partir de los datos que ofrece la página web del Ministerio Público Fiscalía de la Nación, 2020, p. 1.

Queda claro que, en estos últimos casos, existen similares condiciones o mínimamente se hace el esfuerzo para conseguirlo, entre los sujetos que cometen el delito y aquellos que lo persiguen, dado que, para esta clase de delincuentes, contamos con fiscales especializados para combatir estas modalidades delictivas. Sin embargo, no corremos con el mismo grado de preparación y especialización en los casos de ciberdelincuencia (MPFN, 2020).

1.1.1.4. La Escuela de Capacitación del Ministerio Público y la Academia de la Magistratura

El Ministerio Público por medio de la Resolución de la Fiscalía de la Nación N° 714-2003-MP-FN emitida el 14 de mayo de 2003, crea e implementa la Escuela del Ministerio Público denominada «Dr. Gonzalo Ortiz de Zevallos Roedel», con el propósito de promover servicios eficientes, oportunos y accesibles a través de los procesos de capacitación e investigación especializada (MPFN, 2003).

Además, mediante la Resolución de la Fiscalía de la Nación N° 1234-2004-MP-FN emitida el 07 de setiembre de 2004, se aprueba el Reglamento de Organización y Funciones de la Escuela del Ministerio Público antes descrita, cuya función se concentraba en la formulación, aprobación y ejecución de políticas, planes, programas y directivas de capacitación, docencia e investigación en el campo fiscal, forense y administrativo (MPFN, 2004).

A su vez, el Poder Judicial a través de la Ley Orgánica de la Academia de las Magistratura - Ley N° 26335, creó la Academia de la Magistratura, en adelante AMAG, con el propósito de formar académicamente a los aspirantes a cargos de magistrados del Poder Judicial o Ministerio Público, así como la capacitación académica para los ascensos, la actualización y el perfeccionamiento de los mismos (AMAG, 1994).

Adicionalmente, esta Academia cuenta con un Programa de Actualización y Perfeccionamiento, denominado PAP, el cual se fundamenta en actualizar y perfeccionar de manera permanente y descentralizada a los magistrados y auxiliares del Poder Judicial y Ministerio Público a nivel nacional e internacional (AMAG, 2020).

Igualmente, el Texto Único Ordenado de la Ley Orgánica del Poder Judicial consagra en sus artículos 26 y 46 la distribución de los Órganos Jurisdiccionales del Poder Judicial, así como los Juzgados Especializados, los cuales se distribuyen de la siguiente manera:

Tabla 2

Distribución de Órganos Jurisdiccionales en el Perú

Órganos Jurisdiccionales	Juzgados Especializados y Mixtos	Juzgado Especializado o Mixto en lo Penal
La Corte Suprema de Justicia de la República		
Las Cortes Superiores de Justicia, en los respectivos Distritos Judiciales		
Los Juzgados Especializados y Mixtos	Juzgados Civiles, Juzgados Penales, Juzgados de Trabajo, Juzgados Agrarios, Juzgados de Familia y, Juzgados de Tránsito y Seguridad Vial	Juzgados especializados en Delitos Aduaneros, Tributarios, de Propiedad Intelectual, Ambientales, Flagrancia, Omisión a la Asistencia Familiar y Conducción en estado de ebriedad, Corrupción de Funcionarios
Los Juzgados de Paz Letrados		
Los Juzgados de Paz		

Fuente: Elaboración propia a partir de los datos que ofrece el Texto Único Ordenado de la Ley Orgánica del Poder Judicial, 2012, pp. 35 y 43.

Estos Juzgados Especializados y Mixtos, son dependientes de la Corte Superior de Justicia y operan por cada provincia en determinados asuntos, los cuales pueden ser civiles, penales, laborales, familiares, aduaneros y tributarios, entre otros, todos ellos tienen la misma jerarquía y buscan atender casos específicos que requieren una atención especializada (Ley Orgánica del Poder Judicial, 2012).

Consideramos que es insuficiente tanto las capacitaciones que brinda la Escuela del Ministerio Público, así como la Academia de la Magistratura. Pues el nivel de especialización que exige la atención de esta clase de delitos cometidos en espacios cibernéticos, reviste una mayor complejidad para investigarlos y sancionarlos.

Ante ello, podemos advertir que en el Perú es necesaria la implementación de «Fiscalías y Juzgados Especializados en Ciberdelincuencia» como correlato la una de la otra, se reconoce la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia, pero resultaría insuficiente intentar suplir el trabajo de un Fiscalía Especializada con u órgano consultor. Adicionalmente, no es menos importante elogiar y reconocer el loable trabajo que realizan nuestros jueces, pese a todas las limitaciones en infraestructura, logística, especialización, entre otros factores que afectan el rendimiento de su trabajo.

Sin perjuicio de ello, es inaceptable que el Ministerio Público haya apostado por la incorporación de una Unidad Fiscal Especializada que no realice las actuaciones inherentes a la investigación, persecución y sustentación del caso en juicio. La situación se agrava cuando el Poder Judicial pretende mantener la idea de que no necesitan ningún cambio para la atención de los delitos informáticos y aquellos cometidos mediante medios tecnológicos.

Seguidamente, al haber mostrado la grave situación que atraviesa nuestro país en la lucha constante contra la ciberdelincuencia. Es igual de importante, comentar que para una adecuada implementación de una Fiscalía Especializada en Ciberdelincuencia, es necesaria la incorporación de Juzgados igualmente especializados para una adecuada impartición de justicia, es momento de apostar por la adquisición de la tecnología vanguardista, esta adopción implica necesariamente la especialización de jueces y fiscales, quienes investidos del poder delegado por el Estado, ejercerán cabalmente sus funciones con las herramientas jurídicas y tecnológicas necesarias para confrontar con eficiencia y eficacia a la ciberdelincuencia.

1.1.1.5. La centralización de la División de Investigación de Delitos de Alta Tecnología

De forma semejante, contamos con efectivos policiales altamente capacitados en la División de Investigación de Delitos de Alta Tecnología, en adelante DIVINDAT conocidos como «Ciberpolicías». Desde el año 2005 se vienen gestando diversas estrategias para combatir a los delincuentes que operan en el mundo digital. Según Montoya, quien es citado por la DIVINDAT (2006), manifiesta que "no se trata de cualquier trabajo policial. Hablamos de un 'patrullaje virtual en el ciberespacio' que demanda estar en las mismas o en mejores condiciones tecnológicas que los delincuentes informáticos" (párr. 3).

No obstante, dicha División se encuentra saturada con incontables investigaciones en curso. Claramente, se debe a la centralización de recursos y capital humano. A continuación, se mostrará el detalle de las denuncias recibidas por delitos informáticos desde el año 2015 hasta el 2020, revisar el **(Anexo 1)**:

Tabla 3

Denuncias recibidas en la DIVINDAT por delitos informáticos

Año de interposición	Abuso de mecanismos y dispositivos informáticos	Contra la fe pública-suplantación de identidad	Contra la indemnidad y libertad sexual-proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Contra datos y sistemas informáticos	Contra el patrimonio-fraude informático	Contra la intimidad y el secreto de las comunicaciones	Denuncias recibidas
Año 2015	6	114	-	47	414	-	**581**
Año 2016	4	134	-	47	610	-	**795**
Año 2017	5	132	29	104	1219	-	**1489**
Año 2018	1	227	94	126	1928	3	**2379**
Año 2019	2	247	49	159	2097	2	**2556**
Año 2020	6	428	88	129	1951	6	**2608**

Fuente: Elaboración propia a partir de los datos proporcionados por la Oficina de trámite documentario de la DIVINDAT con fecha 31 de octubre de 2020.

Es así que se puede evidenciar un incremento de las denuncias recibidas en esos años. Para poder realizar una correcta investigación en sede policial, es indispensable que tanto las fiscalías como los juzgados cuenten con los conocimientos de especialización necesarios que permitan coadyuvar en la lucha contra la ciberdelincuencia.

1.1.2. Antecedentes de investigación

1.1.2.1. Antecedentes internacionales

El Convenio del Consejo de Europa sobre Ciberdelincuencia, conocido como el Convenio de Budapest, es el primer acuerdo internacional que desarrolla una serie de presupuestos normativos para combatir a la delincuencia, cuya comisión es realizada en «El Ciberespacio». Actualmente, el Portal del Consejo de Europa (2020) cuenta con el Cuadro de firmas y ratificaciones del Tratado n.° 185 del Convenio sobre Ciberdelincuencia, en el cual se informa que un total de 65 países han ratificado y adherido el mencionado Convenio, para más detalle observar el **(Anexo 2)**.

En rigor, Posada (2019) sostiene en la entrevista practicada por LP Pasión por el Derecho, que en Colombia se ha realizado una serie de procesos de capacitación y especialización en Cibercrimen a los fiscales, pese a ello aún persiste el problema en cuanto a la atención de los casos vinculados a la ciberdelincuencia, dado que los operadores que previamente habían sido capacitados están en constante rotación de un despacho a otro, con lo cual resulta insuficiente la medida adoptada.

Los problemas más comunes están estrictamente relacionados con la cadena de custodia, envío y almacenamiento de información, dado que el procedimiento exige la intervención de peritos y expertos en la materia. Cabe resaltar que el Cibercrimen no utiliza para su desarrollo a los procesos ordinarios, aquellos en los que el uso de la documentación simple es usual, pues para la atención de los delitos cometidos en «El Ciberespacio» es necesaria la participación de colaboradores expertos.

Coincidentemente empleando las palabras de Cortes (2015), señala que en Colombia la implementación de Fiscalías Especializadas en Ciberdelincuencia es un proceso a largo plazo que permitirá la consolidación de una estructura adecuada en la persecución, investigación y castigos relacionados a ciberdelitos. En caso de la Policía Judicial de Colombia no es suficiente contar con herramientas, personal y con una estructura normativa en ciberdelincuencia, sino es necesario la previsión orgánica en el Estado y en los distintos órganos vinculados a la ciberdelincuencia que busquen mitigar toda clase de impunidad.

Cabe mencionar que, respecto a la Fiscalía de la Nación y Jueces de la República, pese a la constante preparación de los fiscales, así como las capacitaciones de juzgamiento recibidas no han permitido reducir los índices de impunidad en ciberdelincuencia,

motivo por el cual, es necesaria la implementación de Fiscalías Especializadas en Ciberdelincuencia y contar con el apoyo de personal facilitador en el acceso a herramientas suficientes para el tratamiento de estos casos.

A decir verdad, en algunos países como España se implementó la Fiscalía General del Estado con el objetivo de combatir a la ciberdelincuencia, esta clase de fiscalías tiene un alto nivel de especialización para la atención de este tipo de casos, en palabras de Mesa (2017) se describe que:

> En el año 2011, mediante la Instrucción 2/2011113, de 11 de octubre, la Fiscalía General del Estado crea la figura del Fiscal de Sala de Criminalidad Informática, de esta forma se pretende coordinar y potenciar la armonización de las actuaciones en esta materia mediante la difusión de las oportunas Instrucciones buscando la "unidad de actuación especializada" en todas las jurisdicciones territoriales del Ministerio Público, al considerar que la delincuencia relacionada con las TIC está en constante aumento y la investigación y enjuiciamiento de las mismas no son tarea fácil, lo que hace necesario reforzar la unidad de actuación del Ministerio Fiscal también en esta materia completando la especialización del Ministerio Público. (p. 83)

Al respecto, las amenazas tendientes a afectar el bien jurídico tutelado por la norma, están evolucionando constantemente, por lo que las instituciones que pretenden confrontarlas tienen que avanzar en el mismo sentido y con la misma eficiencia, de ese modo la balanza se encuentra equilibrada según las nuevas exigencias y necesidades del mundo real (Mesa, 2017, p. 83).

Como lo hacen notar Prieto y Vargas (2020) cuando describen que en Ecuador no cuentan con una fiscalía especializada en delitos informáticos. Por lo general, este tipo de casos se tramita en la Unidad de Patrimonio Ciudadano y los otros delitos son tramitados previa identificación del bien jurídico tutelado. Sin embargo, debido a las limitaciones en cuanto al personal especializado en la materia, la mayoría de las investigaciones se tornan engorrosas, mientras más complejos sean los delitos. Por lo que, se requiere de la creación de un Organismo Especializado en Ciberdelincuencia.

Teniendo en cuenta a Marchal (2016), quien menciona que en Ecuador la delincuencia cibernética posiciona en una situación de vulnerabilidad y serios problemas a la Administración de Justicia al momento de investigar un delito, así también se debe considerar que los sucesos de la vida real, transforman a la legislación en anticuada e

insuficiente, esto debido al constante avance tecnológico, lo que debería obligar a los cuerpos de seguridad a contrarrestar de forma oportuna a la ciberdelincuencia.

Asimismo, un factor que resta a la lucha contra este tipo de ilícitos penales es la escasa preparación de los jueces sobre el alcance de las nuevas tecnologías, siendo indispensable una formación y preparación pormenorizada sobre la información relevante, no con eso se logrará que los jueces se conviertan en peritos, por el contrario, contarán con los conocimientos mínimos para poder enfrentarlos.

Sobre la creación de una Fiscalía de Ciberdelito en la provincia de Salta, considerada la cuarta en Argentina, el Ministerio Público Fiscal de la Provincia de Salta (2020), mediante la conferencia rendida por el procurador general de la provincia, Abel Cornejo, refirió que había rasgos de una incontrolable orfandad en cuanto al aspecto de la investigación criminal en los casos de ciberdelitos. A su vez, con la creación de esta, se incorporarán colaboradores especializados en informática con conocimientos plenos en cibercriminalidad, con ello se conseguirá la resolución y búsqueda de evidencia para esclarecer los hechos y alcanzar la verdad.

Como dicen Jackson y Scrollini (2020), en Uruguay no han implementado Fiscalías o Juzgados Especializados en Ciberdelincuencia para cubrir la labor de persecución de los delitos informáticos. No obstante, en el año 2016, la Resolución 578/2016 emitida por la Fiscalía General de la Nación propuso la creación de un grupo para desarrollar el trabajo de elaboración de un protocolo para la actuación del Estado frente a los delitos informáticos.

De acuerdo con Vásquez (2019), menciona que México enfrenta actualmente una dificultad de alcance mundial, esto es, la escasez de entidades especializadas que coadyuven en la investigación y persecución de los delitos cibernéticos. A ello, debe sumarse la carente capacitación con la que cuentan actualmente para formalizar actividades exhaustivas y en coordinación con otras entidades.

En último término, los ataques cibernéticos en España no tienen frontera y su evolución es imparable, las tecnologías modernas son utilizadas para cometer delitos en el ciberespacio contra diferentes receptores, entre ellos gobiernos, corporaciones e individuos, situación que hace una década era inimaginable, ahora forma parte de nuestra vida diaria, esta nueva clase de delitos no conocen fronteras y generan múltiples daños en todo el mundo.

Los ciberdelincuentes incrementan su agilidad y aprovechan al máximo los aparatos y plataformas tecnológicas, mejorando cada vez más sus ataques hasta el grado de cooperar entre sí de manera nunca antes registrada. Las organizaciones delictivas operan a escala mundial, mientras que la policía debe mantenerse a la altura con el objetivo de comprender y contrarrestar cualquier posibilidad delictiva en contra de la sociedad (Organización Internacional de Policía Criminal - Interpol, 2021).

1.1.2.2. Antecedentes Nacionales

Según Díaz (2019) manifiesta que en el Perú los ciberdelitos muestran un aumento del 70 % por cada año, los ciudadanos que a su vez ocupan la situación de cibernautas suelen demostrar demasiada confianza al momento de efectuar transacciones en la banca por internet. Lamentablemente, en la mayoría de los casos, las personas suelen ser precavidos después de haberse convertido en víctimas. El navegar en el ciberespacio implica mucha responsabilidad, ya que la comisión de un delito informático puede realizarse en cualquier parte del mundo.

De acuerdo con Flores (2018), actualmente nuestro país afronta una mayor cantidad de ataques cibernéticos y como resultado, se encuentra posicionado en el quinto lugar en Latinoamérica, estos ataques afectan a diversos sectores económicos, entre ellos, el más importante es el sector financiero.

Nuestro país se adhirió recientemente al Convenio de Budapest, a través de la Resolución Legislativa N° 30913, publicada el 13 de febrero de 2019, en la que consta 4 declaraciones y 3 reservas. De acuerdo con Morachimo (2019) quien comenta que podría confundirse la incorporación del Perú a este Convenio, pues desde su aprobación en el 2001 y su fecha de adhesión han transcurrido 18 años, esto es, un tiempo bastante extenso. Sin embargo, en la región sur del Continente Americano lo hicieron Argentina y Paraguay en el año 2018, Chile en el año 2017, mientras que México y Colombia se encuentran realizando su tramitación.

Ante ello, se observa que a pesar de existir una brecha considerablemente amplía en cuanto a tiempo, nuestra realidad social no es ajena a las realidades de los países vecinos. Las incorporaciones más trascendentales según La Ley (2019), ha sido la confrontación de los delitos informáticos y aquellos delitos que para su comisión sea indispensable la utilización del Internet. Esto es posible con la mejora de las técnicas de investigación y el incremento de la cooperación internacional. De esa forma, los

Estados suscribientes deben cumplir diversas reglas para reforzar los temas de investigación, procesamiento y sanción de múltiples delitos cuyo espacio de comisión es «El Ciberespacio».

Comparada con la postura anterior, una de las finalidades del Convenio es la protección de la sociedad frente a la grave situación de desprotección en la que se encuentra a causa de la «ciberdelincuencia», con la particularidad de adoptar una legislación adecuada a nuestra realidad actual y con el compromiso de mejorar los aspectos vinculados a la cooperación internacional (Presidencia del Consejo de Ministros, 2019).

El legislador nacional ocupó como principal punto de atención los aspectos relacionados a la penalización de los delitos cometidos a través de nuevas tecnologías. El detalle radica en que las Instituciones Públicas de nuestra Administración de Justicia, entre ellas, la Policía Nacional del Perú ha logrado la especialización de sus divisiones y con ello enfrentar esta clase de delitos. Contrariamente, el Ministerio Público y el Poder Judicial han quedado desfasados, por lo que necesitan modernizarse y especializar a sus operadores jurídicos en actos de investigación y persecución en tanto que el tratamiento de estos ilícitos penales dista de los delitos tradicionales (Elías, 2014).

Aunado a esto, García (2019) sostiene que existe un consenso poblacional en relación al incremento global de los ciberataques, considerando que los ciberdelincuentes cuentan con aparatos sofisticados tal y como se ha podido evidenciar en los delitos consumados hasta el momento. En respuesta a ello, el Estado debería tomar conciencia de los posibles daños, entre ellos irreparables en los que podrían incurrir las empresas en nuestro país. Al parecer, este incidente no fue considerado entre los puntos de agenda cuya atención requiere inmediatez.

Mientras tanto, uno de los inconvenientes que se presenta en la realidad, está ligado a la incorrecta adecuación del hecho presuntamente delictivo con el tipo penal, dado que es imposible pensar que estos casos realmente sucedan en la práctica. No obstante, el problema medular es la falta de especialización de fiscales para la persecución de estos delitos (Herrera, 2018).

Sin perjuicio de lo anterior, un referente en el campo jurídico como lo es LP Pasión por el Derecho (2020) describe que no basta con la modificación de la Ley de los

Delitos Informáticos, pues el factor humano termina siendo decisorio para lograr un avance integral, es importante integrar a los operadores de justicia, conformado por los fiscales y los jueces.

A su vez, para lograr coadyuvar a los efectivos policiales, resulta justificada la creación de Fiscalías y Juzgados Especializados en Ciberdelincuencia. Adicionalmente, agrega que los legisladores tienen pendiente uno de los retos más complejos de nuestra era, esto es, la regulación adecuada del tratamiento y sanción de los delitos cibernéticos, así como la ideación y materialización de la estructura de un sistema de justicia óptimo.

En esa misma línea de pensamiento, Tenorio (2018) explica sobre la necesaria implementación de Fiscalías y Juzgados Especializados en Ciberdelincuencia, no es suficiente sin el apoyo de un personal altamente calificado en la atención, control y resolución de los casos de ciberdelincuencia. Más aún si consideramos que este es un tema poco abordado en nuestra legislación, el mismo que requiere de mecanismos de cooperación adecuada, en otras palabras, el trabajo en conjunto tanto de los órganos nacionales como internacionales a fin de evitar futuras contingencias y garantizar un debido proceso.

1.1.3. Marco Teórico

En este apartado de la investigación, corresponde definir las variables, así como delimitar las dimensiones de manera suficiente. Para ello, es necesario incluir lo propuesto por Baena (2014) en su obra titulada «Metodología de la Investigación», en lo referido a las variables:

> Reciben el nombre de variable independiente (x) la característica o propiedad que se supone la causa del fenómeno estudiado que no se puede controlar y variable dependiente (y) aquella cuyas modalidades o valores están en relación con los cambios de la variable independiente, pero que sí es factible de controlarse científicamente. (p. 53)

Asimismo, nuestra referente comenta que "los indicadores constituyen las dimensiones menores de las variables y se componen de elementos concretos en los cuales se expresa la realidad que se quiere conocer. Pueden existir también medidas menores conocidas como índices y subíndices" (p. 53). **(Anexo 3).** Siendo así, se comenzará con el desarrollo de la variable independiente «Sistema de Justicia del Perú», luego con la

variable dependiente «Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia» y las dimensiones correspondientes.

Incorporación de los delitos informáticos en la normativa nacional

A lo largo de la historia del Perú se han propuesto una serie de Proyectos de Ley en los que se pretendía regular a los delitos informáticos, entre los más destacables podemos ubicar el Proyecto de Ley Nro. 05071 de Jorge Muñiz Ziches de fecha 18 de agosto de 1999 **(Anexo 4)**, el Proyecto de Ley Nro. 05132 de Susana Díaz Díaz de fecha 31 de agosto de 1999 **(Anexo 5)** y el Proyecto de Ley Nro. 05326 de Anastacio Vega Asencio de fecha 18 de octubre de 1999 **(Anexo 6)**. Estos dieron origen a la incorporación de los delitos informáticos en el Código Penal, mediante la Ley Nro. 27309 para que años más tarde se modifiquen algunos artículos de dicho ordenamiento jurídico por medio de la Ley Nro. 28251. Conforme transcurrieron los años se añadieron la Ley de delitos informáticos Nro. 30096 y al año siguiente se incorporó su modificatoria mediante la Ley Nro. 30171.

Las Fiscalías y Juzgados Especializados en Ciberdelincuencia

En palabras de Morachimo (2019), adherirse al Convenio de Budapest resulta insuficiente para castigar los delitos informáticos, pues debemos considerar que en nuestro país desde el año 2000 no contamos con evidencia sólida sobre los resultados de los marcos normativos aplicables. En esa línea de análisis, las cifras reportadas por la Policía Nacional del Perú y el Ministerio Público, muestran inconsistencias y excluyen términos de vital importancia en cuanto a la modalidad del delito o el progreso de las denuncias interpuestas. Considerando todo eso, es un punto de agenda pendiente de evaluación, la necesidad de aumentar los recursos actuales de la Policía Informática y la oportunidad de crear Fiscalías y Juzgados Especializados.

Al respecto, Guerrero (2018) comenta que existen actores en la sociedad que asumen diferentes roles, para el caso objeto de análisis, el Gobierno es el encargado de adoptar medidas para contrarrestar a la ciberdelincuencia, es así que la creación de Fiscalías y Juzgados Especializados en delitos informáticos, es indispensable para cumplir el propósito planteado, considerando que para una adecuada actuación por parte de las autoridades es necesario contar con personal altamente capacitado.

Adicionalmente, durante las capacitaciones realizadas tanto a la Policía, Fiscalía y Juzgados sobre la Ciberdelincuencia, fue minúsculo el avance en más de 20 años, no es

suficiente con la creación de la DIVINDAT, pues al no contar con Fiscalías y Juzgados Especializados en nuestro país, los resultados continúan siendo infructuosos. Esto configura una gran deuda a la sociedad, porque estamos exigiendo que desarrollen habilidades sumamente especializadas y no estamos otorgándole la preparación correspondiente (Elías, 2020). **(Anexo 7)**

En el caso de la legislación nacional, se cuenta con el derecho a la iniciativa legislativa tanto en el Congreso de la República como en el Poder Ejecutivo, según lo dispuesto en la Constitución Política del Perú en su artículo 107, en razón de ello, el 02 de agosto de 2019, se emitió el Proyecto de Ley N° 4643/2019-CR cuyo encabezado planteaba que esta ley declaraba de interés nacional y necesidad pública la creación de la Fiscalía Especializada en delitos informáticos.

Por consiguiente, el referido Proyecto de Ley, expresó que la especialización con medios técnicos y fiscales con formación especializada es primordial para que los persecutores del delito logren resultados eficientes, tales como la identificación plena de los responsables de la comisión del delito. Por ello, propone que se incorpore una Fiscalía Especializada en delitos informáticos como novena Fiscalía Especializada en el Perú (Proyecto de Ley, 2019).

A decir verdad, para julio del año 2020 la mayor cantidad de fiscalías clasificadas acorde a la especialidad penal fue equivalente a 0.14 % para el caso de las Fiscalías Supremas, 9.64 % correspondiente a las Fiscalías Superiores y 30.72 % a favor de las Fiscalías Provinciales. En términos objetivos, estas cifras nos indican que la mayor concentración de atenciones se ubica en la especialidad del Derecho Penal (Boletín Estadístico del Ministerio Público, 2020).

Según cifras obtenidas del Boletín Estadístico del Ministerio Público (2020) iniciando por enero hasta julio de 2019 y culminando por enero hasta julio de 2020, se registraron 299.852 delitos en materia Penal, en las Fiscalías Provinciales Penales y Mixtas a Nivel Nacional.

Tabla 4

Delitos registrados en Fiscalías Provinciales Penales y Mixtas según tipo de delito genérico a nivel nacional, enero - julio 2019 y enero - julio 2020

Delitos Genéricos	2019 Enero - Julio	2020 Enero - Julio

	N° Delitos	%	N° Delitos	%	% de Variación
Contra la Vida, el Cuerpo y la Salud	240,055	38.94	122,915	41.00	48.80
Contra el Patrimonio	186,961	30.33	82,396	27.48	55.93
Contra la Seguridad Pública	46,186	7.49	25,831	8.61	44.07
Contra la Administración Publica	35,602	5.78	20,887	6.97	41.33
Contra la Libertad	33,505	5.44	17,693	5.90	47.19
Contra la Familia	42,791	6.94	13,885	4.63	67.55
Contra la Fe Pública	13,488	2.19	5,900	1.97	56.26
Delitos Ambientales	4,552	0.74	2,846	0.95	37.48
Ley Nº 30096, Ley de Delitos Informáticos	3,908	0.63	2,644	0.88	32.34
Contra la Tranquilidad Pública	1,930	0.31	883	0.29	54.25
Otros Delitos Genéricos	7,459	1.21	3,972	1.32	46.75
Total	616,437	100.00	299,852	100.00	51.36

Fuente: Elaboración propia a partir de los datos que ofrece el Boletín N° 7 del Ministerio Público Fiscalía de la Nación, 2020, p. 40.

De lo expuesto en la tabla, podemos apreciar que los delitos informáticos reportados en el 2020 representan un total de 2644, cifra inferior a la reportada en el año 2019. No obstante, sigue siendo una cantidad muy aproximada a la reportada en los delitos ambientales, dado que la diferencia solo es de 202 casos reportados. Lo cual permite asumir que al ser una carga muy similar y teniendo en cuenta que para los casos ambientales tienen una Fiscalía Especializada en Delitos Ambientales, sería igualmente conveniente que, para la atención de casos de delitos informáticos, también se cuente con una Fiscalía Especializada en Ciberdelincuencia.

Tabla 5

Delitos Informáticos registrados en Fiscalías Provinciales Penales y Mixtas según tipo de delito sub genérico a nivel nacional, enero - julio 2019 y enero - julio 2020

Delitos Sub Genéricos	**2019**	**2020**
	Enero - Julio	**Enero - Julio**

	N° Delitos	%	N° Delitos	%	% de Variación
Delitos Informáticos Contra el Patrimonio	1,515	38.77	1,099	41.57	-27.46
Delitos Informáticos Contra la Fe Publica	138	3.53	109	4.12	-21.01
Delitos Contra Datos y Sistemas Informáticos	134	3.43	79	2.99	-41.04
Delitos Informáticos Contra la Intimidad y el Secreto de las Comunicaciones	27	0.69	39	1.48	-44.44
Delitos Informáticos Contra la Indemnidad y Libertad Sexuales	55	1.41	25	0.95	-54.55
Disposiciones Comunes	19	0.49	15	0.57	-21.05
Sin Especificar Delito Sub Genérico	2,020	51.68	1,278	48.32	-36.73
Total	3,908	100.00	2,644	100.00	-32.34

Fuente: Elaboración propia a partir de los datos que ofrece el Boletín N° 7 del Ministerio Público Fiscalía de la Nación, 2020, p. 48.

A su vez, se advierte de la información extraída que los delitos sub genéricos han cobrado mayor presencia en los reportes de los años 2019 y 2020, desde enero a julio, respectivamente, para una ayuda visual revisar **(Anexo 8)**. Especialmente, los delitos informáticos contra el patrimonio y la fe pública. Asimismo, el reporte muestra una cantidad considerable de delitos sin especificación para ambos años, lo cual intensifica la necesidad de implementar una Fiscalía Especializada en Ciberdelincuencia.

Sistema de Justicia del Perú

En la actualidad no corremos con la fortuna de tener un Juzgado Especializado en Ciberdelincuencia, a diferencia de otros delitos que revisten cierta complejidad y necesitan conocimientos técnicos y especializados, tales como los Juzgados Especializados en Delitos Aduaneros, Tributarios o de Propiedad Intelectual, por mencionar algunos ejemplos.

El Ministerio de Justicia y Derechos Humanos (2020), en adelante MINJUS, en su «Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú», refirió que de la información obtenida arrojó indicadores que refuerzan la necesidad de afianzar las capacidades y conocimientos de las Fiscalías y Juzgados en la atención de los delitos informáticos.

A su vez, menciona que las Fiscalías deben incorporar componentes viables para fortalecer las debilidades presentadas durante la atención de este tipo de delitos, considerando que el trabajo es realizado conjuntamente con la Policía Nacional del Perú y el Poder Judicial, al ser quienes interfieren en la persecución, identificación y sanción de estos delitos.

Existen posiciones desde dos ópticas distintas, de un lado aquellas que no apuestan por la incorporación de Fiscalías y Juzgados Especializados en Ciberdelincuencia y de otro lado, contamos con los que sí consideran pertinente su incorporación en el Sistema de Justicia, para registrar todas las denuncias y evitar inexactitudes en el conteo de los casos denunciados, con lo que se lograría no solo formalizar las investigaciones preparatorias y sustentarlas en juicio, sino que a través de programas de sensibilización y concientización se conseguiría resultados óptimos en la sociedad.

Tabla 6

Personas con sentencia condenatoria registrada según delitos informáticos y contra el patrimonio relativo a delito informático a nivel nacional, durante el periodo 2016 - 2020

Delito	Años					Total
	2016	2017	2018	2019	2020	
DELITOS INFORMÁTICOS (LEY 30096 Y 30171)						
Acceso Ilícito - Art. 2 - Ley Nº 30096		2	1	4		7
Atentado a la Integridad de Datos Informáticos - Art. 3 - Ley Nº 30096			4	1	1	6
Atentado a la integridad de sistemas informáticos - Art. 4 - Ley N° 30096		1	1			2
Fraude Informático - Art. 8 - Ley N° 30096	21	9	94	118	30	272
Interceptación de datos informáticos - Art. 7 - Ley N° 30096	1	2	2	3	1	9
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos - Art. 5 - Ley N° 30096	8	11	34	23	11	87
Suplantación de Identidad - Art. 9 - Ley N° 30096	3		6			9
Total	**33**	**25**	**142**	**149**	**43**	**392**
TITULO V DELITOS CONTRA EL PATRIMONIO (ARTÍCULO 185 AL 208)						
Delitos Informáticos (Artículo 207-A al 207-D)	4	36	3	3	2	48
Alteración, daño o destrucción de base de datos Art. 207-B				3	2	5
Delito Informático - Art. 207-C Agravantes		1	2			3

Delito Informático Art. 207		34				34
Tráfico ilegal de datos - Art. 207-D (Ley Nº 30076)	1					1
Uso o ingreso indebido a una base de datos Art. 207-A	3	1	1			5
Total	**37**	**61**	**145**	**152**	**45**	**440**

Fuente: Elaboración propia a partir de los datos proporcionados por la Sub Gerencia de Estadística – Gerencia de Planificación del Poder Judicial de fecha 29 de octubre de 2020.

Según la tabla anterior, las cifras de los periodos consignados resultan alarmantes y nos llevaría a pensar que la Administración de Justicia estaría condenando excepcionalmente, dicho de otro modo, no es que se busque la condena en todos los casos, sino un correlato de casos resueltos durante un periodo específico. Esta información se secunda con la extraída de los boletines antes consignados en cuanto a las cifras arrojadas. En tal sentido, al no contar con Fiscalías se estarían practicando investigaciones defectuosas y en consecuencia el archivo de los casos; y a falta de Juzgados Especializados, la impartición de justicia estaría siendo un inconveniente al no tener entre sus filas a jueces con conocimientos técnicos y especializados que les permita valorar los medios probatorios y resolver la causa con claridad.

Unidad Fiscal Especializada en Ciberdelincuencia

En América del Sur hasta el 30 de diciembre de 2020, teníamos como uno de nuestros más cercanos referentes al país de Argentina por haber incorporado Fiscalías Especializadas en Ciberdelincuencia en dos de sus principales Estados. No obstante, recientemente en el Perú se incorporó una Unidad Fiscal Especializada en Ciberdelincuencia, en adelante UFEC, la cual cuenta con competencia a nivel nacional e inició su funcionamiento el día 15 de febrero de 2021, con lo que logramos cumplir el primer paso de una enorme deuda pendiente con la sociedad.

Uno de los principales inconvenientes que debemos enfrentar es el ámbito de competencia, pues en la Resolución de la Nación N.° 1503-2020-MP-FN se consideró que la UFEC sería un órgano informativo y consultor, incumpliendo las expectativas de muchos ciudadanos que a estas alturas esperaban un órgano que asuma la encargatura permanente en la dirección de la investigación, recolección de elementos probatorios, trabajo en coordinación nacional e internacional y representación de la sociedad en la audiencia de juzgamiento y demás etapas procesales en instancias nacionales y extranjeras, así como todo aquel acto necesario para el esclarecimiento de los hechos y de los presuntos responsables.

La Unidad Fiscal Especializada en Ciberdelincuencia de Argentina, en adelante UFECI, se incorporó a dicho país con la finalidad de robustecer la capacidad de respuesta del organismo, teniendo como puntos principales la detección, persecución y represión de la criminalidad organizada (Ministerio Público Fiscal, 2021). Distinto es el caso de la UFEC, dado que se pretende recargar a los fiscales comunes con delitos informáticos mediante consultorías e informes técnicos que al final generan sobresaturación de casos en vez de aligerar la carga.

Presupuesto público para la implementación de las Fiscalías y los Juzgados Especializados en Ciberdelincuencia

Es de conocimiento público que las entidades del país dependen del presupuesto público destinado por el Ministerio de Economía y Finanzas (2021) cuyo propósito es "otorgar un mayor bienestar a la ciudadanía mediante la asignación eficiente y eficaz de los recursos públicos, acorde con la disponibilidad de los fondos públicos" (párr. 1).

Por ello, la implementación de las Fiscalías y los Juzgados Especializados en Ciberdelincuencia estará supeditado a la presentación de la solicitud de la Comisión de Presupuesto del Congreso y que esta sea considerada una prioridad para el próximo presupuesto público. En palabras sencillas, seguirá una temática similar a la creación de fiscalías en el Distrito Fiscal de Lima, con motivo de la Implementación del Código Procesal Penal, correspondiente al Primer Tramo.

Dicho lo anterior, la secuencia sería que la Secretaría Técnica del Equipo Técnico de Implementación del Nuevo Código Procesal Penal informará si la Dirección General de Presupuesto Público del Ministerio de Economía y Finanzas, en adelante MEF, autorizó el presupuesto para la ejecución del proyecto en tramos y delimitación de los montos (Fiscalía de la Nación, 2020). Una suerte similar tendrá que atravesar el Poder Judicial para lograr el nivel de especialización.

1.1.4. Definición de términos básicos

En este espacio, corresponde definir la aproximación más acertada de las palabras técnicas, complejas o interesantes de la investigación, las cuales fueron empleadas por destacados autores o simplemente incluidas por los coautores. Estos términos se esclarecen con el propósito que los lectores tengan mayor comprensión durante la exteriorización de su apetito de conocimiento.

Allanamiento: De acuerdo con lo señalado por el Dr. Cornejo, debe entenderse como:

> En el desarrollo de una investigación penal es una medida de restricción de derechos que implica el ingreso del Ministerio Público y sus representantes a un determinado inmueble con la finalidad de buscar e identificar pruebas. Por lo general, es autorizado por un juez penal. Sin embargo, es posible que el fiscal efectúe este allanamiento sin una orden judicial (…). (2020, 3min8seg)

Tratado Internacional: Según la Organización de los Estados Americanos (1969), menciona que es "un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos y cualquiera que sea su denominación particular" (p. 2).

Acuerdo Internacional: El Derecho Internacional (2018), refiere que "es el compromiso alcanzado por dos o más sujetos (usualmente Estados y/u organizaciones internacionales) a través de un proceso de concertación, que está llamado a producir efectos en el ámbito internacional" (párr.1).

Ratificación de los Tratados Internacionales: Tal como precisa la Organización de los Estados Americanos (1969) "es el acto internacional así denominado por el cual un Estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado" (p. 2).

Declaraciones de un Convenio: De acuerdo con lo señalado por la Organización Mundial de la Propiedad Intelectual (1969), cuando menciona que:

> Se aplica a varios instrumentos internacionales. Sin embargo, las declaraciones no siempre son jurídicamente vinculantes. A menudo se elige este término deliberadamente para indicar que las partes no tienen la intención de crear obligaciones vinculantes, sino que simplemente quieren declarar ciertas intenciones (…). (p. 4)

Reservas de un Tratado: Tal como aborda la Organización de los Estados Americanos (1969), cuando señala que:

> Es una declaración unilateral, cualquiera que sea su enunciado o denominación, hecha por un Estado al firmar, ratificar, aceptar o aprobar un tratado o al adherirse a él, con objeto de excluir o modificar los efectos jurídicos de ciertas disposiciones del tratado en su aplicación a ese Estado. (p. 3)

Delito informático: Conforme lo describe el Diccionario Panhispánico del Español Jurídico (2020) cuando menciona que "es la Infracción penal cometida utilizando un medio o un instrumento informático" (p. 1).

Ciberdelito: La presente definición es abordada por A favor de tic (2017), describiendo que "es un crimen que se comete a través de las plataformas digitales (…)" (párr. 1).

Robo de identidad o phishing: En lo expuesto por la página A favor de tic (2017) cuando sostiene que "consiste en obtener datos de otra persona para utilizarlos como si fueran propios. Generalmente con el objetivo de realizar trámites legales, bancarios o de seguros y compras (…)" (p. 2).

Secuestro de información o ransomware: En información recabada de A favor de tic (2017) lo define como el supuesto que "bloquea el acceso de las personas a cierta información de sus dispositivos y pide un pago a cambio de su liberación. Si no se cubre el rescate, la información contenida en los aparatos es destruida (p. 2).

Vishing: En palabras del Cardozo (2019) sostiene que "el 'Vishing' es un tipo de estafa informática que se realiza a través de llamadas telefónicas y que busca obtener información bancaria de las personas. Su nombre proviene de la conjunción de las palabras inglesas: 'voice' y 'phishing'" (p. 1).

Cibercrimen: Tal como indica Kaspersky (2019), cuando describe que:

> Es una actividad delictiva que afecta o abusa de una computadora, una red informática o un dispositivo en red. La mayor parte del cibercrimen, pero no todo, lo perpetran cibercriminales o hackers que desean ganar dinero. El cibercrimen lo cometen personas u organizaciones. Algunos cibercriminales están organizados en grupos, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas. Otros son hackers novatos. En raras ocasiones, el cibercrimen tiene como objetivo dañar las computadoras por motivos distintos a la obtención de dinero. Estos pueden ser políticos o personales. (p. 1)

Cadena de custodia: Bajo la definición del Ministerio Público Fiscalía de la Nación (2017), sostiene que "es una serie de recaudos destinados a asegurar el origen, la identidad e integridad de la evidencia, evitando que se pierda, destruya o altere" (p. 40).

El Ciberespacio: En palabras de Álvarez (2018), quién sostiene que "cabe entender ese espacio no físico donde se interconectan e interrelacionan las redes de comunicación e información que Internet une" (p. 1).

La Ciberdelincuencia: Según la convergencia de posturas entre Domínguez y Cornejo (2020), quienes señalan que:

> La ciberdelincuencia engloba a todo delito en el que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC. Se trata por tanto de comportamientos delictivos dirigidos a tres objetivos: los dispositivos informáticos, los datos y la información informatizada. Podemos clasificar estos delitos del siguiente modo:
>
> a) Delitos de daños, sabotaje informático y ataques de denegación de servicios. Ejemplo de estos delitos son los ataques por virus o el espionaje a sistemas informáticos de los Estados o empresas.
>
> b) Delitos de acceso sin autorización a datos, programas o sistemas informáticos.
>
> c) Delitos de descubrimiento y revelación de secretos, cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos. (p. 3)

El agente encubierto: Con relación a la idea de Proaño (2018), quien refiere que:

> El agente encubierto, infiltrado o clandestino, se involucra de manera directa con la organización delictual, a descubrir toda la información que sea posible, sobre personas involucradas (activas y pasivas), así como la posible infracción a cometer o que ha sido cometida. (p. 3)

Wireshark: En palabras de Zeas (2011) desarrolla el concepto como:

> Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para múltiples plataformas. Conocido originalmente como Ethereal, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. (p. 31)

Skimming: Según la idea de Rico (2013) manifiesta que "(…) el uso del término Skimming como omnicomprensivo de las situaciones donde se produce el robo de la información de las tarjetas como consecuencia de una utilización legítima del instrumento de pago" (p. 6).

Evidencia digital: El Ministerio Público Fiscalía de la Nación (2017), sostiene que debe ser entendida como la "información o datos, almacenado o transmitido en un medio informático, que puede ser utilizado como evidencia" (p. 43).

1.2. Formulación del problema

1.2.1. Formulación del problema general

1.2.1.1. PG: ¿El Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos?

1.2.2. Formulación de problemas específicos

1.2.2.1. PE$_1$: ¿De qué forma atienden las Fiscalías Provinciales no Especializadas en Ciberdelincuencia en el Sistema de Administración de Justicia del Perú, 2020?

1.2.2.2. PE$_2$: ¿De qué manera atienden los Juzgados no Especializados los casos de Ciberdelincuencia en el Sistema de Administración de Justicia del Perú, 2020?

1.3. Objetivos

1.3.1. Objetivo general

1.3.1.1. OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.

1.3.2. Objetivos específicos

1.3.2.1. OE$_1$: Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

1.3.2.2. OE$_2$: Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

1.4. Hipótesis

1.4.1. Hipótesis general

1.4.1.1. HG: El Sistema de Justicia del Perú resulta inapropiado para procesar los delitos informáticos, en la medida que carece de Fiscalías y Juzgados Especializados en Ciberdelincuencia.

1.4.2. Hipótesis específicas

1.4.2.1. HE$_1$: La ausencia de las Fiscalías Especializadas en Ciberdelincuencia incide negativamente en los actos de investigación fiscal, imposibilitando una representación idónea y generando un estado de indefensión de las víctimas y de la sociedad.

1.4.2.2. HE$_2$: La inexistencia de los Juzgados Especializados en Ciberdelincuencia inciden negativamente al valorar y resolver con base a los medios probatorios aportados por las partes, afectando la predictibilidad de las resoluciones judiciales y el equilibrio del Sistema de Justicia del Perú.

CAPÍTULO 2. METODOLOGÍA

2.1. Tipo de investigación

En este apartado de la investigación es fundamental establecer los criterios adoptados para la metodología empleada, en principio se debe resaltar el nivel investigativo que se persigue profundizar, esto es, el nivel exploratorio, según Fernández, Urteaga y Verona (2015) comentan que "se enfoca en descubrir información sobre un objeto de estudio desconocido" (p. 17). Asimismo, como lo hace notar Vera (2021) cuando menciona que:

> Los estudios exploratorios se presentan como el primer nivel, son los más superficiales, pero no por ello carecen de rigor científico, todo lo contrario, son la apertura del campo científico hacia los fenómenos nuevos, poco estudiados, o propios de una población aislada (de forma que el eje central de la investigación ya se ha trabajado, pero no en dicha población). (p. 55)

El método practicado sigue el sendero de Taylor y Bogdan (1994) cuando refieren que "los conceptos sociológicos se emplean para iluminar rasgos de los escenarios o personas estudiados y para que faciliten la comprensión" (p. 159). Seguidamente, se debe desarrollar el nivel de aplicación de la investigación. Para este caso se optó por el propósito básico o puro, en palabras de Martínez y Benítez (2015) quienes mencionan que:

> La investigación básica en las ciencias sociales se lleva a cabo para ampliar el conocimiento de lo social. De esta manera, es puramente investigación teórica destinada a aumentar el conocimiento sobre determinadas conductas o fenómenos. En definitiva, la investigación básica se lleva a cabo con el único propósito de recopilar información y desarrollar el conocimiento existente. (p. 69)

Ahora bien, se debe señalar que se aplicó el enfoque mixto, el cual puede ser entendido como "los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta" (Hernández, 2014, p. 534). En esa misma línea, "la investigación mixta es un nuevo enfoque e implica combinar los métodos cuantitativo y cualitativo en un mismo estudio" (Hernández, Fernández y Baptista, 2010, p. 31).

Para el abordaje de las entrevistas se empleó el enfoque mixto, pero en su sub enfoque cualitativo, el cual se define como los "(…) predecesores de los estudios cuantitativos, y se caracterizan por no utilizar la estadística para poder completarse; mientras que los estudios cuantitativos requieren necesariamente de la estadística" (Supo, 2015, p. 36). Adicionalmente, según Hernández, Fernández y Baptista, máximos exponentes sobre la investigación y la metodología a nivel mundial, postulan lo siguiente sobre la investigación cualitativa "utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación" (2010, p. 7). En esa misma línea, Hernández y Mendoza (2018) agregan que:

> Con el enfoque cualitativo también se estudian fenómenos de manera sistemática. Sin embargo, en lugar de comenzar con una teoría y luego "voltear" al mundo empírico para confirmar si esta es apoyada por los datos y resultados, el investigador comienza el proceso examinando los hechos en sí y revisado los estudios previos, ambas acciones de manera simultánea, a fin de generar una teoría que sea consistente con lo que está observando que ocurre. (p. 7)

Para el caso del análisis documental de los reportes, se aplicó el sub enfoque cuantitativo, dado que en palabras de Hernández (2014) refiere que "los planteamientos cuantitativos se derivan de la literatura y corresponden a una extensa gama de propósitos de investigación, como: describir tendencias y patrones, evaluar variaciones, identificar diferencias, medir resultados y probar teorías" (p. 36).

En lo correspondiente al diseño no experimental se debe precisar que "en ella no hay manipulación de las variables" (Ramírez, 2004, p. 47). En esa misma línea de pensamiento, Altuna postula que "este tipo de investigación se centra en el estudio y comprensión de fenómenos, explorando desde un ambiente natural de los participantes para relacionarlos con los contextos donde se desarrollen" (2018, p. 10).

Al respecto, Villanueva (2011) suscribe que estos diseños "se dividen en transeccionales o transversales y longitudinales, ambos son relevantes y necesarios; cada uno tiene un valor propio" (p. 52).

2.2. Población y muestra (materiales, instrumentos y métodos)

A continuación, es pertinente explicar cómo está conformada nuestra población, no sin antes definirla para lograr un mejor entendimiento. De acuerdo con Arias (2020) en su obra titulada «Técnicas e instrumentos de investigación científica», propone que:

> En esta técnica se puede tener como población de estudio a sujetos, infraestructuras, equipos, herramientas e incluso material audiovisual. Se debe tener cuidado con el tipo de población que se elige porque con esta técnica el investigador no puede extender el tiempo de estudio a las personas. (p. 13)

Asimismo, Hernández et al, refiere que la aproximación más cercana de población se entiende como "el conjunto de todos los casos que concuerdan con determinadas especificaciones" (2010, p. 174). Con ese mismo criterio, Altuna (2018) revela que es "un grupo de personas, seres vivos, objetos, casos, situaciones, etc. [sic] sobre los cuales el investigador está interesado en estudiar para comprobar una hipótesis planteada al respecto de ellos" (p. 35).

Adicionalmente, la población puede estar compuesta por un grupo finito o infinito, para tener clara tal afirmación Arias (2020) en su obra denominada «Proyecto de Tesis Guía para la elaboración» destaca que:

> Existe la población finita que es cuando se conoce la cantidad de sujetos que integran la población y la población infinita que es cuando no se tiene el dato exacto acerca de la cantidad de sujetos de la población, o también se denomina población infinita cuando existen más de cien mil sujetos que conforman la población. (p. 59)

En ese orden de propuestas, corresponde abordar conceptualmente a la muestra utilizada en la investigación. Dicho esto, extraemos lo postulado por Hernández y Mendoza (2018) cuando sostienen que "la muestra es un subgrupo considerado como una parte representativa de la población o el universo, los datos recolectados serán obtenidos de la muestra, la población se perfila desde la situación problemática de la investigación" (p. 61).

Agregado a ello, Arias afirma que "no existe una cantidad establecida que debe tener la muestra, sin embargo, es importante que se sepa delimitar correctamente según los objetivos que se desea alcanzar en el estudio y la situación problemática planteada" (2020, p. 61).

A su vez, la muestra tiene dos vertientes, la primera considera como objeto de estudio de quien se producen datos e información para el análisis del estudio, mientras que la unidad de muestreo son los sujetos u objetos que se utilizan para obtener la información

(Arias, 2020, p. 62). Habiendo esclarecido el panorama, se procedió a elaborar una tabla detallada, la cual se muestra a continuación:

Tabla 7

Conexión del problema general con la unidad de análisis y la unidad de muestreo

Problema general	Muestra	
	Unidad de análisis	**Unidades de muestreo**
¿El Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos?	Las Fiscalías y Juzgados Especializados en Ciberdelincuencia en el Sistema de Justicia del Perú durante el año 2020.	UM_1: Especialistas en ciberdelincuencia a nivel nacional e internacional. UM_2: Base de datos de los casos en sede fiscal y judicial.

Fuente: Elaboración propia a partir de la información obtenida en la obra Proyecto de Tesis Guía para la elaboración, Arias, 2020, p. 62.

Cabe indicar que se eligió el muestreo no probabilístico por conveniencia, entre los postulados que mejor la definen ubicamos a Hernández et al. (2010), cuando plantean que:

> Son válidas en cuanto a que un determinado diseño de investigación así las requiere; sin embargo, los resultados se aplican nada más a la muestra en sí o a muestras similares en tiempo y lugar (transferencia de resultados), pero esto último con suma precaución. No son generalizables a una población, ni interesa tal extrapolación. (p. 401)

En respaldo a ello, Arias (2020) expone que:

> Este tipo de muestreo se utiliza cuando se desea elegir a una población teniendo en cuenta sus características en común o por un juicio tendencioso por parte del investigador, además, en este caso no se utiliza algún método de muestreo estadístico, y no todos los miembros de la población tienen la misma oportunidad de ser seleccionados, se utiliza también cuando la población es muy pequeña. (p. 60)

Habiendo esclarecido el panorama investigativo, se debe señalar que se definió como universo o población finita a un grupo de abogados especialistas internacionales y nacionales, así como un efectivo policial de la DIVINDAT; y otro de objetos, esto es, información documental recabada del Ministerio Público y Poder Judicial, los cuales serán analizados con sus respectivos sub enfoques. De esa forma, se buscará responder

si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos, a propósito del estado de las investigaciones y las resoluciones condenatorias emitidas.

En efecto, la muestra estuvo conformada por 11 abogados especialistas en ciberdelincuencia, entre ellos 3 nacionales y 8 internacionales, así como un efectivo policial especialista de la DIVINDAT, todos ellos con amplia trayectoria académica y profesional, así como un respetable reconocimiento en sus países. Asimismo, el reporte de los delitos informáticos atendidos en los 33 de los 34 distritos fiscales a nivel nacional, iniciados a partir del año 2015 y el reporte de los casos en los que se emitió condena derivada por el Poder Judicial. De eso se desprende, que el método específico de la investigación sea el sociológico, dado que la regulación nacional e internacional deja abierta la posibilidad que el Perú pueda incorporar Fiscalías y Juzgados Especializados en Ciberdelincuencia, de acuerdo al fenómeno que enfrenta nuestra actual realidad social.

2.3. Operacionalización de variables

OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.

Tabla 8

Operacionalización de las variables dependiente e independiente

Variables	Definición conceptual	Dimensión	Indicadores
	Las Fiscalías Especializadas en Ciberdelincuencia: Es el titular de la acción penal pública, defensor de la legalidad de los derechos ciudadanos, persecutor del delito y encargado de representar	Fiscalía Especializada en Ciberdelincuencia	Ciberdelincuencia Delitos informáticos Proceso Judicial

V_D: Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia.	a la sociedad en juicio en los casos de ciberdelincuencia. **Los Juzgados Especializadas en Ciberdelincuencia:** Es aquel órgano jurisdiccional especializado en ciberdelincuencia que imparte justica en una determinada circunscripción geográfica.	Juzgado Especializado en Ciberdelincuencia	Unidad Fiscal Especializada en Ciberdelincuencia
V_I: El Sistema de Justicia del Perú, 2020.	Es el aparato del Estado puesto al servicio de la administración de justicia, directa o indirectamente a través del Poder Judicial, el Ministerio Público y otras entidades públicas.	Administración de Justicia	Ministerio Público Poder Judicial División de Investigación de Delitos de Alta Tecnología

Fuente: Elaboración propia.

2.4. Técnicas e instrumentos de recolección y análisis de datos

Para lograr recolectar estructuralmente la información recogida se emplearon una serie de procedimientos orientados a las ideas discursivas de Arias (2020), sobre las técnicas de análisis de documentos y entrevistas, dado que es una de las opiniones más acertada y cercana a lo referido por Altuna (2018) sobre la técnica de análisis documental cuando señala que "se refiere al procedimiento para la recolección de información contenida en libros o documentos entendidos como ese conjunto de fuentes que contienen información de hechos, sucesos, acontecimientos, sean naturales o sociales" (p. 41).

Al haberse realizado la precisión anterior se procede a comentar el detalle de las técnicas e instrumentos practicados. De un lado, se procedió con la aplicación del instrumento de recolección de datos de análisis de documentos, la estrategia elaborada para la búsqueda fue solicitar información documental a través del acceso a la información pública dirigido al Ministerio Público Fiscalía de la Nación. Luego, se realizó el descarte de la unidad de muestreo por el orden de actualidad, estableciéndose el orden ascendente de la información, esto es, desde el año 2015 hasta el 2020.

Los documentos analizados fueron entregados de forma completa. Es decir, se consideró en el reporte la cantidad de casos resueltos en las Fiscalías Provinciales por denuncias relacionadas a la Ley N° 30096 – Ley de Delitos informáticos a nivel nacional cuyo

periodo elegido fue desde el 01 de enero de 2015 hasta el 30 de noviembre de 2020. Sin embargo, con el ánimo de delimitar la información y mostrar ordenadores visuales atractivos y sencillos de entender se incorporaron figuras con el estado de las investigaciones por distrito fiscal. La cantidad de reportes revisados se alinearon con el objetivo general y los objetivos específicos de investigación.

Cabe resaltar que durante el desarrollo del trabajo no se consideró necesario el análisis de forma física porque no se encontraron documentos históricos y todos fueron obtenidos mediante el correo electrónico remitido por la entidad antes descrita. De acuerdo a la obtención y el análisis virtual de la información se creyó pertinente la incorporación de la siguiente tabla pormenorizada:

Tabla 9

Análisis virtual de documentos

Análisis de documentos	
Criterios	**Análisis virtual**
Materiales	2 laptops con acceso a internet, dos cuentas de correo Gmail y memorias de almacenamiento interno de 1 terabyte.
Sistematización	Documentos sistematizados por el Sistema de Gestión Fiscal (SGF) y el Sistema de Información de Apoyo al Trabajo Fiscal (SIAFT).
Costo	Costo de internet y energía eléctrica.
Acceso a la información	El acceso fue mediante una Solicitud de Acceso a la Información Pública (SAIP).
Resultados de la investigación	Información proveniente de la Oficina de Control de Productividad Fiscal, adscrita al Ministerio Público Fiscalía de la Nación, por lo que resulta Confiable.

Fuente: Elaboración propia a partir de la información obtenida en la obra Métodos de investigación online herramientas digitales para recolectar datos, Arias, 2020, p. 27.

De otro lado, al haber realizado la búsqueda de información virtual se pretendió profundizar la investigación aplicando la técnica de la entrevista y siguiendo lo planteado por Altuna (2018) cuando refiere que:

> Es el contacto interpersonal que tiene por objeto recopilar testimonios orales referidos a determinados conocimientos o experiencias del experto. La entrevista es una técnica muy útil para las investigaciones de índole jurídico, dado el valor especializado que brinda respaldo para la contrastación de las hipótesis planteadas por el investigador. (p. 41)

Ante ello, se optó por realizar las entrevistas a 8 abogados especialistas internacionales y 3 abogados especialistas nacionales, así como a 1 efectivo policial de la DIVINDAT - PNP. El instrumento de recolección de datos fue el cuestionario o guía de entrevista,

en el caso de las 8 entrevistas internacionales se conformó por 4 preguntas relacionadas al objetivo general, 5 preguntas vinculadas al objetivo específico 1 y 4 preguntas ligadas al objetivo específico 2, haciendo un total de 13 preguntas.

Asimismo, en el caso de las 3 entrevistas nacionales se conformaron por 5 preguntas relacionadas al objetivo general, 4 preguntas en referencia al objetivo específico 1 y 4 preguntas relacionadas al objetivo específico 2, obteniendo un total de 13 preguntas. Agregado a ello, se plantearon 2 preguntas vinculadas al objetivo general, 3 preguntas relacionadas al objetivo específico y 2 preguntas concadenadas al objetivo específico 2. Para mayor detalle de la aplicación de las entrevistas virtuales se muestra la siguiente tabla:

Tabla 10

Entrevista virtual

Entrevistas	
Criterios	**Aplicación virtual**
Población	Abogados especialistas en ciberdelincuencia en el ámbito nacional e internacional y un efectivo policial especialista de la DIVINDAT.
Materiales	Dos laptops con acceso a internet.
Tiempo	Entre 30 a 60 minutos.
Costo	Internet, plataforma Zoom y energía eléctrica.
Lugar	En el país de Perú y departamento de Lima mediante la Plataforma digital de Zoom Meetings.
Entorno	Entrevista personalizada sin participación de sujetos externos.
Rasgos conductuales	Profesionalismo, conocimiento y dominio del tema, así como disposición para absolver las consultas.
Resultados de la investigación	Información pertinente y confiable.

Fuente: Elaboración propia a partir de la información obtenida en la obra Métodos de investigación online herramientas digitales para recolectar datos, Arias, 2020, p. 32.

En consecuencia, al haberse establecido de formar clara y secuencial el método que en palabras de nuestra referente es el camino de la investigación, así como las técnicas que representan el modo en que se recorrió dicho camino, corresponde detallar cómo ha sido el procedimiento de la investigación y qué pasos se siguieron en el desarrollo del mismo. Es fundamental hacer la precisión sobre los modelos utilizados para el cuestionario de entrevista, ya que fueron extraídos y adaptados de otras investigaciones realizadas con anterioridad a esta. Para mejor entendimiento revisar **(Anexos 9, 10 y 11)**.

2.5. Procedimiento

2.5.1. Procedimiento de recolección de datos

En este apartado se dividió la explicación en dos momentos para poder detallar el procedimiento de recolección de datos. Empezaremos por comentar que se consideraron una serie de criterios antes de solicitar la información a la entidad pública, entre los más relevantes se precisó el aspecto temporal desde el año 2015 hasta el 2020. Acto seguido, se delimitaron el estado de la investigación, el delito registrado, el código del caso, el tipo de conclusión, el tipo de fallo y la etapa final. A su vez, se precisó que el aspecto espacial sería en todo el país, considerando para ello el distrito fiscal en la que se siguió cada investigación.

Luego, se realizaron las averiguaciones pertinentes para acceder al formato con la solicitud de acceso a la información pública, se procedió a rellenarlo y enviarlo al correo electrónico que figuraba en la página oficial del Portal de Transparencia del Ministerio Público, para mayor detalle revisar el **(Anexo 12)**. Posteriormente, nos comunicaron que se debía dirigir dicho pedido a un correo distinto, el cual pertenecía a la Presidencia de la Junta de Fiscales Superiores del Distrito Fiscal de Lima Norte, lo cual puede verse reflejado en el **(Anexo 13)**.

Recibida esta aclaración se remitió la solicitud al correo competente para que sea atendido. Como consecuencia del envío nos acusaron la recepción del mismo y nos respondieron con fecha posterior, adjuntando 5 archivos Portable Document Format, en adelante PDF, el primero fue la disposición fiscal en la que se concedió el requerimiento, mientras que los 4 archivos restantes eran los reportes con el detalle de los criterios previamente solicitados, estos últimos representaban un total de 208 páginas, dicha información puede evidenciarse en el **(Anexo 14)**.

Asimismo, respecto al reporte brindado por el Poder Judicial se siguió el mismo procedimiento de los párrafos anteriores, solicitándose un archivo Excel detallado con los delitos informáticos atendidos desde el año 2015 hasta el año 2020 por el Poder Judicial mediante sus Juzgados Mixtos o Especializados u otros, considerando los casos archivados, los casos culminados por principio de oportunidad o terminación anticipada, los casos en etapa de juicio oral, los casos sentenciados, los casos con sentencias confirmadas o revocados y se aprovechó el documento para solicitar una entrevista con tres jueces especialistas en cibercriminalidad, revisar el **(Anexo 15)**.

En respuesta a ello, nos adjuntaron 4 archivos PDF, el primero contenía la denegación de la información estadística de los casos culminados por el principio de oportunidad, casos en la etapa oral y casos con sentencias confirmadas o revocadas, así como las entrevistas solicitadas; el segundo contenía la aprobación de un entregable con los datos de las personas con sentencia condenatoria registrada según delitos informáticos y contra el patrimonio relativo a delito informático durante el periodo 2016 al 2020, denegando nuestro pedido que solicitaba el periodo 2015 al 2020.

En relación a los últimos documentos, en uno de ellos constaba la delegación de entrega a la Sub Gerencia de Estadística – Gerencia de Planificación del Poder Judicial, quien finalmente nos deriva la documentación por medio del correo de mesa de partes. Dicho reporte fue objeto de análisis documental en la presente investigación, tal y como se detallará en los siguientes apartados, para mejor entender revisar el **(Anexo 16)**.

En un segundo momento, se aplicó el instrumento de recolección de datos de la entrevista siendo una herramienta infalible para recolectar testimonios de los más acertados exponentes a nivel internacional. Para ello, mientras se extraía información de la experiencia internacional sobre ciberdelincuencia se fueron identificando y listando una base de datos con los posibles entrevistados, revisar **(Anexos 17 y 18)**. A decir verdad, nos dimos con la desafortunada sorpresa de que en el Perú habían contados especialistas en la materia y gran parte de ellos no accedieron, tal y como se explicará más adelante.

Al terminar de redactar los objetivos de la presente investigación se formularon las preguntas siguiendo el criterio de aplicación por espacio geográfico. Dicho de otro modo, 13 preguntas formuladas para los invitados internaciones, 13 para los entrevistados nacionales y 7 preguntas para el efectivo policial de la DIVINDAT, no por ello se perdió la rigurosidad del planteamiento de interrogantes en el cuestionario de entrevista, ya que todas se desprendían de nuestro objetivo general y de los objetivos específicos.

Inicialmente, se contactaron a los ponentes nacionales e internacionales a través de sus redes sociales, entre ellas Facebook, Twitter y LinkedIn. Acto seguido, se formalizó la invitación por medio de las cuentas de correo oficial proporcionadas por ellos y se desarrollaron las entrevistas en la plataforma Zoom, versión licenciada, para mayor detalle revisar los **(Anexos 19 al 30)**. Durante el desarrollo de estas, se solicitó a cada

entrevistado su consentimiento para grabar su imagen, el audio, el vídeo y que el material fílmico obtenido pueda utilizarse para los fines estrictamente académicos.

Para el caso del efectivo policial nos pusimos en contacto mediante el acceso a la información pública, en la respuesta al requerimiento nos contestaron con gentileza y prontitud, brindándonos el número de contacto del sub oficial encomendado, con quien coordinamos la fecha y la hora, así como la plataforma más idónea, teniendo en cuenta el cargo que ocupa y su horario de trabajo.

2.5.2. Procedimiento de tratamiento de análisis de datos

El procedimiento de análisis de los documentos se realizó creando una carpeta exclusiva con la información proporcionada por el Ministerio Público y el Poder Judicial, dentro de esa carpeta se hizo una subdivisión en dos carpetas para colocar en una de ellas la información general sobre el universo y en la otra el contenido de la muestra. Como se comentó anteriormente se eligieron 33 de los 34 distritos fiscales para analizar la información, dicha elección se hizo considerando el estado de las investigaciones proporcionadas en el reporte, el cual fue convertido en una base de datos Excel que se creó y guardó en la carpeta antes descrita.

Los pasos realizados fueron en primer término la conversión del archivo PDF en formato Excel para colocar, ordenar y filtrar las celdas pertinentes. Seguidamente, se procedió a generar una tabla dinámica por cada distrito fiscal, obteniendo un total de 33 pestañas con el detalle del estado de cada caso. Esto permitió que se pueda condensar la información en gráficos dinámicos y que se evidencie los resultados de forma transparente y sencilla. Logrando así una información más compacta y susceptible de analizar.

En seguida, se realizó el análisis externo para determinar de dónde se obtuvieron los documentos y detectar si su procedencia efectivamente era de la Oficina de Control de Productividad Fiscal para el caso de los documentos fiscales y de la Sub Gerencia de Estadística de la Gerencia de Planificación del Poder Judicial para el caso del reporte judicial, lo cual fue comprobado. Su validez fue corroborada con la firma electrónica contenida en cada documento y la corroboración del aplicativo PDF.

En segundo término, se analizó el aspecto interno del documento, esto es, el contenido de cada archivo PDF. Para evaluar si conforme a los datos obtenidos, entre ellos el estado de la investigación, el tipo de conclusión y la etapa final se podría evaluar la

implementación de las Fiscalías y Juzgados Especializados en Ciberdelincuencia en el Sistema de Justicia del Perú. Al obtenerse los primeros resultados que en su mayoría nos indicaban archivamientos desmedidos, se procedió a generar gráficos, los mismos que serán presentados en el apartado de resultados.

Asimismo, en lo correspondiente al procedimiento de análisis de las entrevistas se obtuvo material fílmico de los 12 entrevistados, el cual fue proporcionado mediante la grabación de la plataforma Zoom. En su mayoría, las coordinaciones se realizaron mediante las cuentas de correo electrónico para fijar el horario en que se practicarían las entrevistas con excepción del efectivo policial, el mismo que fue contactado por acceso a la información pública de la DIVINDAT, así como el cuestionario de entrevista que se envió para que las respuestas brindadas sean las pertinentes según el conocimiento y experiencia de cada uno.

La plataforma Zoom fue la herramienta digital elegida para efectuar las entrevistas porque facilita al entrevistador generar un link de invitación prefijando la fecha y la hora, también facilitó reprogramar las reuniones que por motivos excepcionales se presentaron durante el desarrollo de la investigación. Dicho enlace se adjuntaba al correo de invitación para mayor facilidad de los entrevistados. El manejo de la herramienta fue sencillo, didáctico y funcional, uno de los invitados decidió compartir información en diapositivas mediante la opción ventana compartida, lo cual facilitó el desarrollo de la entrevista.

En la base de datos con la información personal de los 12 entrevistados se creyó pertinente consignar los nombres y apellidos completos, una reseña profesional y los datos sociodemográficos de cada uno. En relación a las preguntas formuladas, todas ellas fueron plasmadas acorde a los objetivos de la investigación y se tomó en cuenta preguntas no estructuradas para evitar el condicionamiento de las respuestas y así obtener resultados de la más alta calidad investigativa, fue esencial recabar sus declaraciones para cotejar su experiencia con la nuestra. El material obtenido enriqueció el trabajo de investigación, considerando que todos los entrevistados fueron especialistas en ciberdelincuencia, las respuestas fueron transcritas para su utilización en los próximos apartados de la presente investigación.

2.6. Aspectos éticos

En este último apartado de la metodología conviene señalar que durante el desarrollo de la investigación se respetó una cadena de criterios éticos, entre los más destacables se ubican la redacción académica en cuanto al citado y referenciado de la información, también debe comentarse que los reportes fueron obtenidos a través del conducto regular, eso fue el acceso a la información pública por el Portal de Transparencia de cada entidad. En esa línea, debe explicarse que antes de cada entrevista se solicitó a los participantes que otorguen su consentimiento expreso para ser grabados y utilizar el material fílmico resultante para el desarrollo de la investigación.

Aunado a ello, no todas las entrevistas resultaron provechosas para la investigación y como respuesta inmediata se procedió a descartar aquella que no cumplía con el estándar cualitativo planteado por los coautores. En aras de salvaguardar la integridad de los libros, artículos y demás documentos utilizados que no estaban alojados en una página estable, se consignaron los hipervínculos de acceso público correspondientes, cuya base principal fue el OneDrive de los coautores para evitar posibles caídas del sistema o errores en la búsqueda.

Una de las pautas esenciales en todas las entrevistas fue la presentación formal por parte de los entrevistadores con el ánimo de mostrar profesionalismo no solo en la dicción de las preguntas y el dominio del tema, sino en la vestimenta y el espacio destinado para realizarla. Finalmente, solo se entrevistaron a especialistas en ciberdelincuencia a nivel nacional e internacional aumentando las probabilidades de éxito en los resultados obtenidos.

CAPÍTULO 3. RESULTADOS

En el presente apartado se muestra el análisis e interpretación de los hallazgos obtenidos luego de una minuciosa y exhaustiva búsqueda. Entre ellos, los resultados del análisis documental tanto de Ministerio Público como del Poder Judicial. Asimismo, los resultados del análisis de las entrevistas a los 11 especialistas nacionales e internacionales y a 1 efectivo policial de la División de Investigaciones de Delitos de Alta Tecnología. En adición, se expone los resultados del análisis de la doctrina y la legislación.

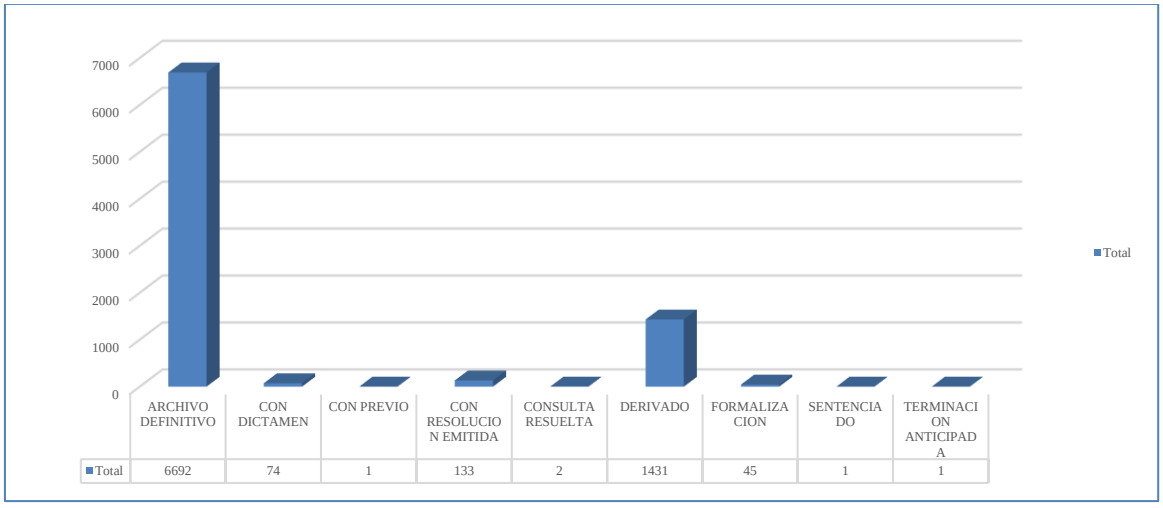
3.1. Resultados del análisis documental

3.1.1. Análisis documental del Ministerio Público

En el análisis de los reportes cursados por la entidad de la Administración de Justicia se consideró necesario distribuirlos teniendo en cuenta 33 de los 34 distritos fiscales, un margen temporal desde el año 2015 hasta el 2020 y la etapa en la que se encuentran cada caso. Para ello, se procedió a elaborar organizadores visuales en forma de figuras con el propósito de interpretar cada uno y con ello evaluar si el Sistema de Administración de Justicia en nuestro país resulta apropiado para procesar la comisión de los delitos informáticos.

Figura 1

Análisis de los casos de los delitos informáticos en Lima desde el año 2015 hasta 2020



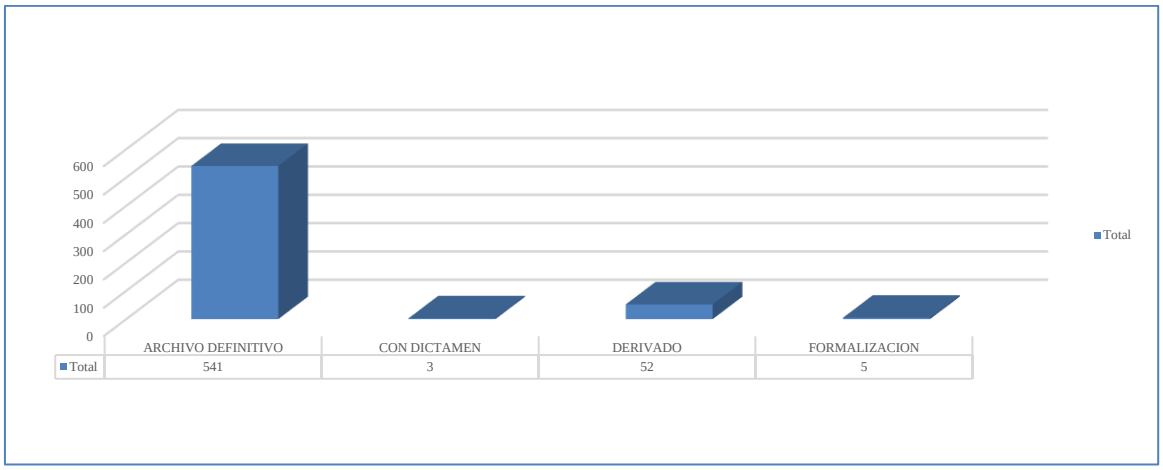
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 8380 casos registrados en el distrito fiscal de Lima desde el año 2015 hasta el 2020, 6692 fueron archivados definitivamente antes de iniciar la etapa preparatoria. Esta última cifra representa un porcentaje superior al 50 %, lo que nos

conduciría a pensar que se estarían cometiendo errores al momento de proponer los actos de investigación en la etapa preparatoria. Es curioso observar que en esos seis años únicamente se hayan formalizado 45 casos y solo uno de ellos llegase a la etapa de juzgamiento.

Figura 2

Análisis de los casos de los delitos informáticos en Lima Sur desde el año 2016 hasta 2020

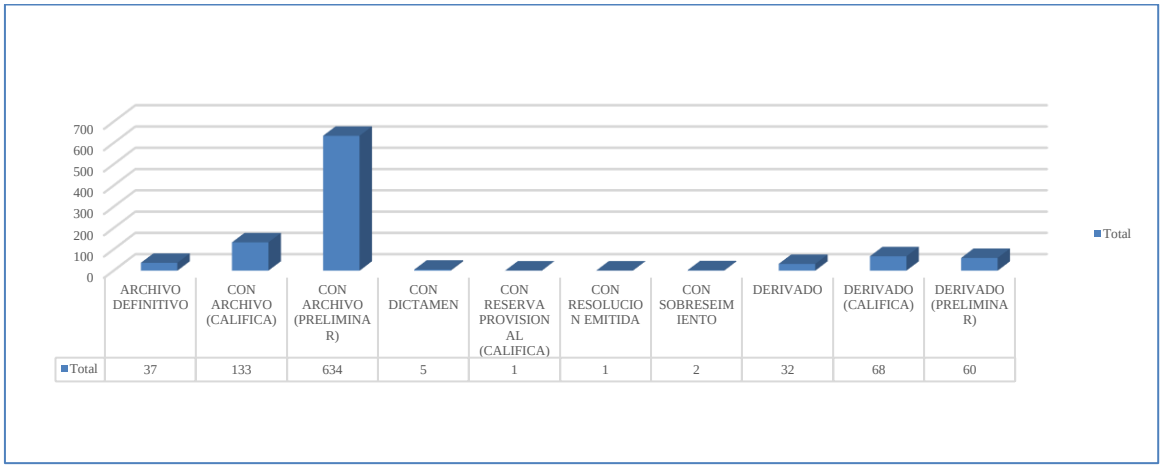


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se apreció que de un total de 601 casos registrados en el distrito fiscal de Lima Sur desde el año 2016 hasta el 2020, 541 se archivaron definitivamente antes de iniciarse la etapa preparatoria y solo 5 fueron formalizados durante cinco años, no habiendo llegado ninguno a la etapa de juzgamiento.

Figura 3

Análisis de los casos de delitos informáticos en Lima Norte desde el año 2015 hasta 2020



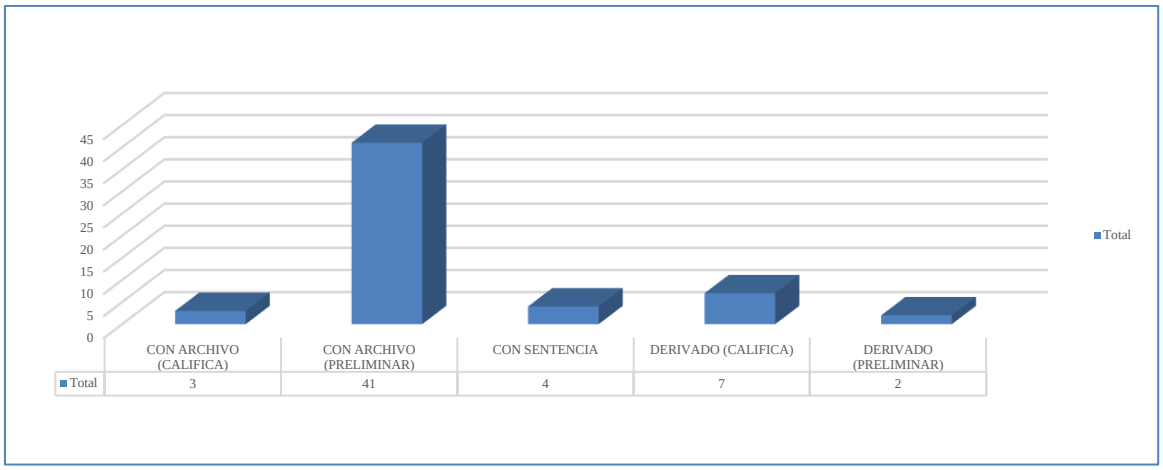
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se observó que, de un total de 973 casos registrados en el distrito fiscal de Lima Norte desde el año 2015 hasta el 2020, 37 fueron archivados definitivamente antes

de la etapa de investigación preparatoria, 133 se archivaron en la etapa de calificación de la denuncia y 634 fueron archivados en la subetapa de diligencias preliminares, 2 casos fueron sobreseídos en la etapa intermedia.

Figura 4

Análisis de los casos de delitos informáticos en Lima Noroeste desde el año 2016 hasta 2020

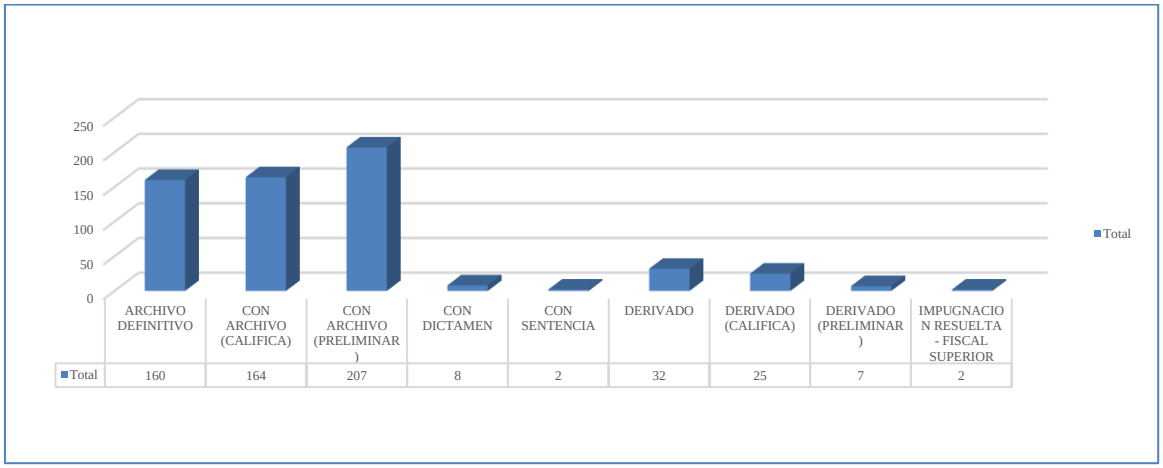


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se advirtió que, de un total de 57 casos registrados en el distrito fiscal de Lima Noroeste desde el año 2016 hasta el 2020, 3 de ellos se archivaron en la etapa de calificación de la denuncia, 41 se archivaron en la subetapa preliminar y solo 4 casos fueron sentenciados.

Figura 5

Análisis de los casos de delitos informáticos en Lima Este desde el año 2016 hasta 2020



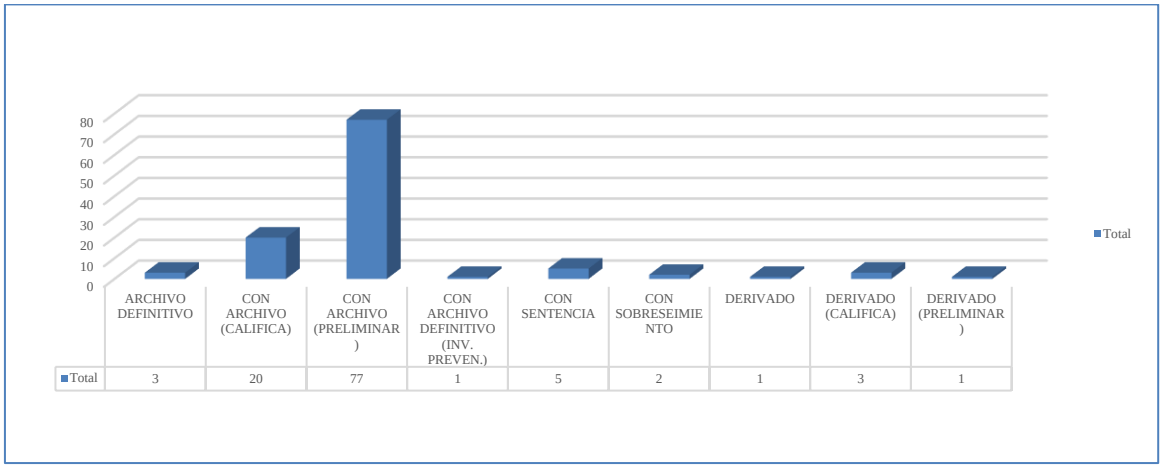
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se infirió que, de un total de 607 casos registrados en el distrito fiscal de Lima Este desde el año 2016 hasta el 2020, 160 se archivaron definitivamente en la etapa

de investigación preparatoria, 164 se archivaron en la etapa de calificación de la denuncia, 207 se archivaron en la subetapa preliminar y solo en dos casos se emitieron sentencias.

Figura 6

Análisis de los casos de delitos informáticos en Santa desde el año 2016 hasta 2020

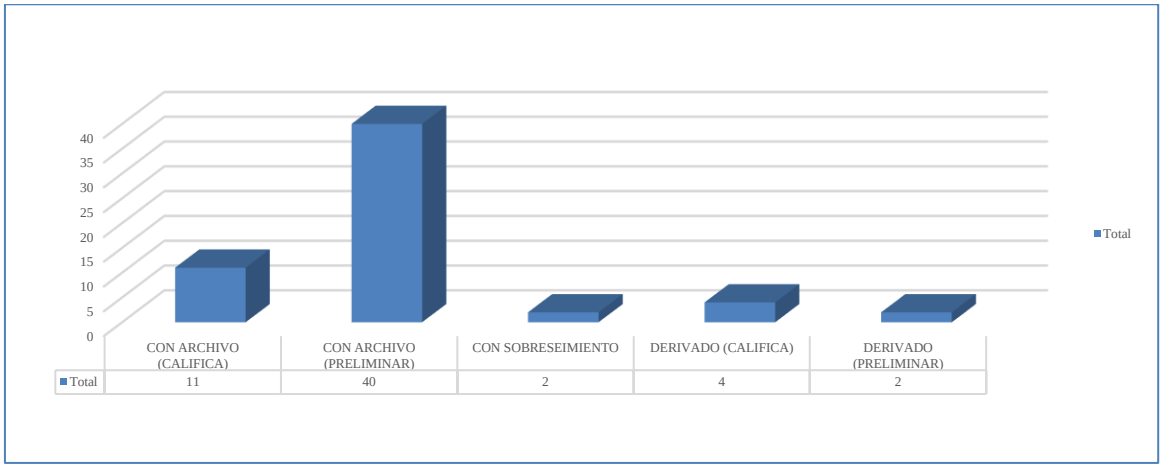


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se presumió que, de un total de 113 casos registrados en el distrito fiscal de Santa desde el año 2016 hasta el 2020, 3 de ellos se archivaron definitivamente en la investigación preparatoria, 20 se archivaron en la etapa de calificación de la denuncia y 77 se archivaron en la subetapa de investigación preliminar. Agregado a ello, 2 casos fueron sobreseídos y solo se sentenciaron 5 casos en 5 años.

Figura 7

Análisis de los casos de delitos informáticos en Ucayali desde el año 2017 hasta 2020



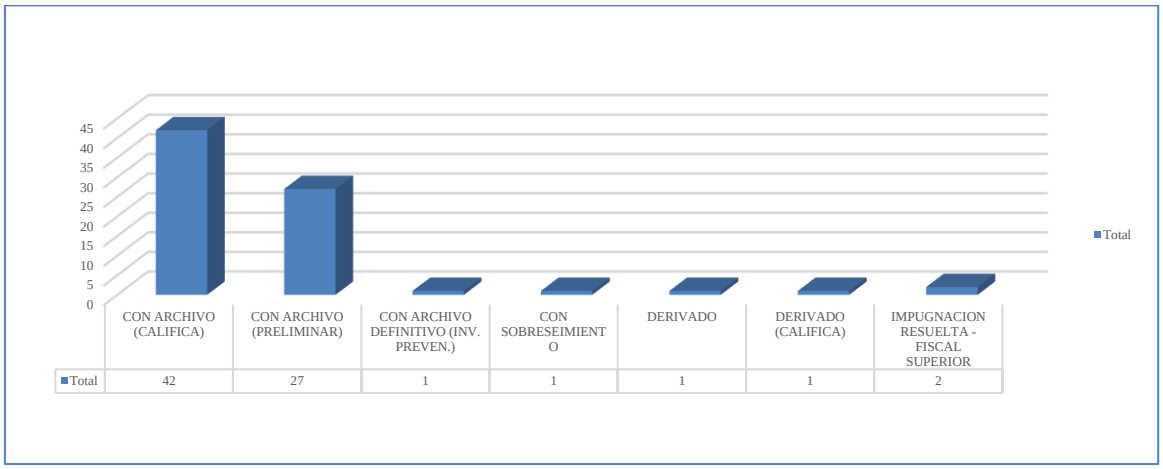
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se obtuvo que, de un total de 59 casos registrados en el distrito fiscal de Ucayali desde el año 2017 hasta el 2020, 11 se archivaron en la etapa de calificación de la

denuncia, 40 se archivaron en la subetapa de investigación preliminar y 2 fueron sobreseídos en la etapa intermedia.

Figura 8

Análisis de los casos de delitos informáticos en Tacna desde el año 2016 hasta 2020

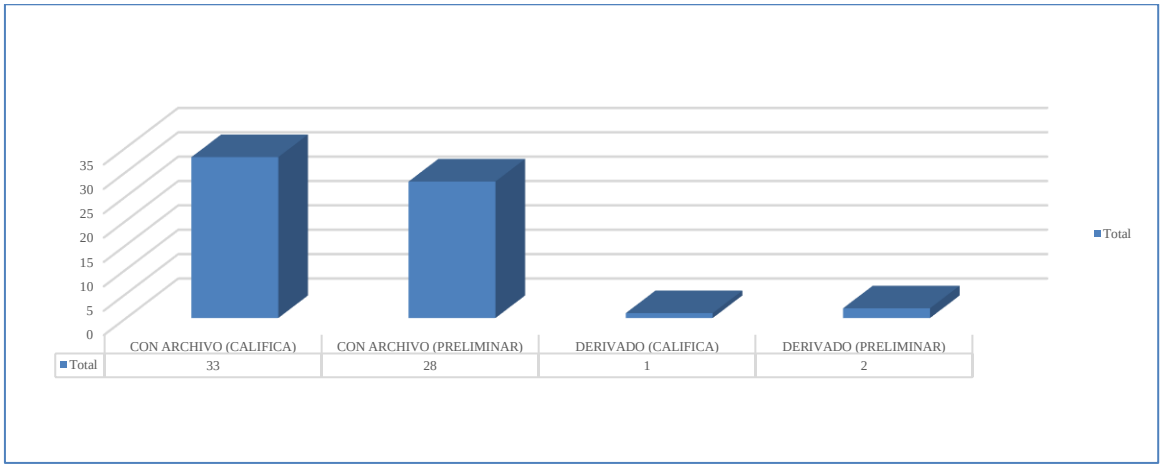


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se agregó que, de un total de 75 casos registrados en el distrito fiscal de Tacna desde el año 2016 hasta el 2020, 42 se archivaron en la etapa de calificación de la denuncia, 27 se archivaron en la subetapa de investigación preliminar, 1 se archivó definitivamente en la investigación preventiva y 1 fue sobreseído, ninguno de ellos fue sentenciado.

Figura 9

Análisis de los casos de delitos informáticos en Sullana desde el año 2015 hasta 2020



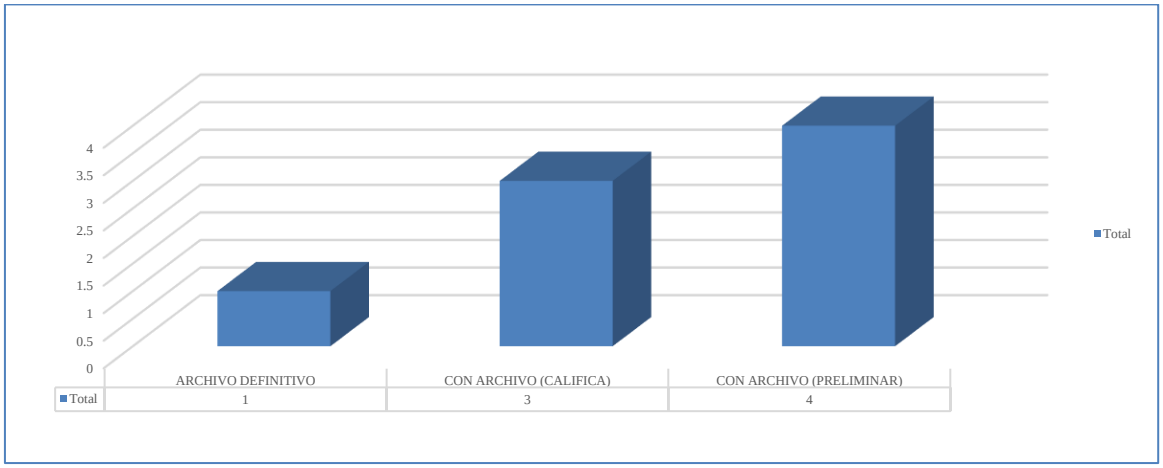
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se evidenció que, de un total de 64 casos registrados en el distrito fiscal de Sullana desde el año 2015 hasta el 2020, 33 fueron archivados en la etapa de calificación

de la denuncia, 28 se archivaron en la subetapa de investigación preliminar y ninguno llegó a la etapa de juzgamiento.

Figura 10

Análisis de los casos de delitos informáticos en Selva Central desde el año 2017 hasta 2020

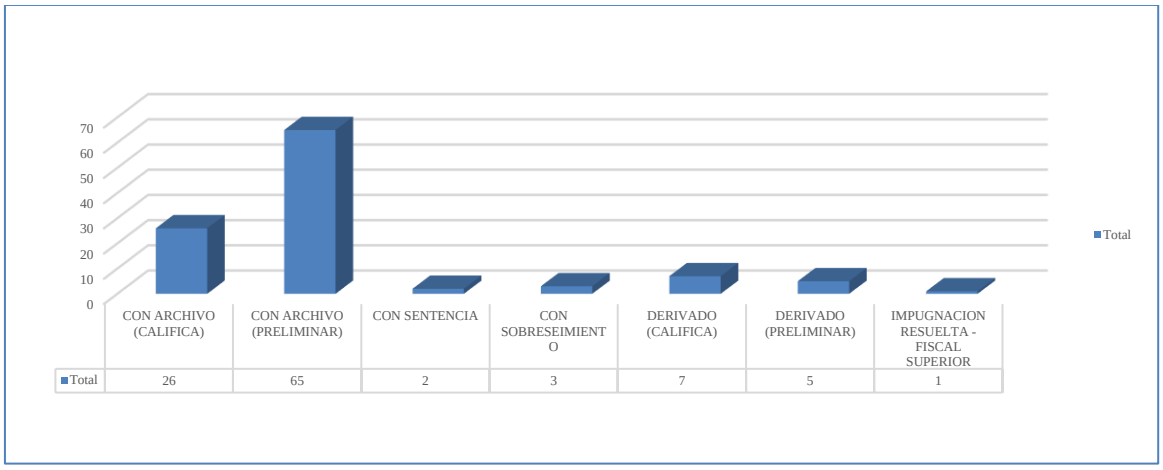


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se desprendió que, de un total de 8 casos registrados en el distrito fiscal de la Selva Central desde el año 2017 hasta el 2020, todos fueron archivados, entre ellos, 1 se archivó definitivamente en la investigación preparatoria, 3 se archivaron en la etapa de la calificación de la denuncia, 1 se archivó en la subetapa de investigación preliminar y ninguno de ellos llegó a la etapa de juzgamiento.

Figura 11

Análisis de los casos de delitos informáticos en San Martín desde el año 2015 hasta 2020



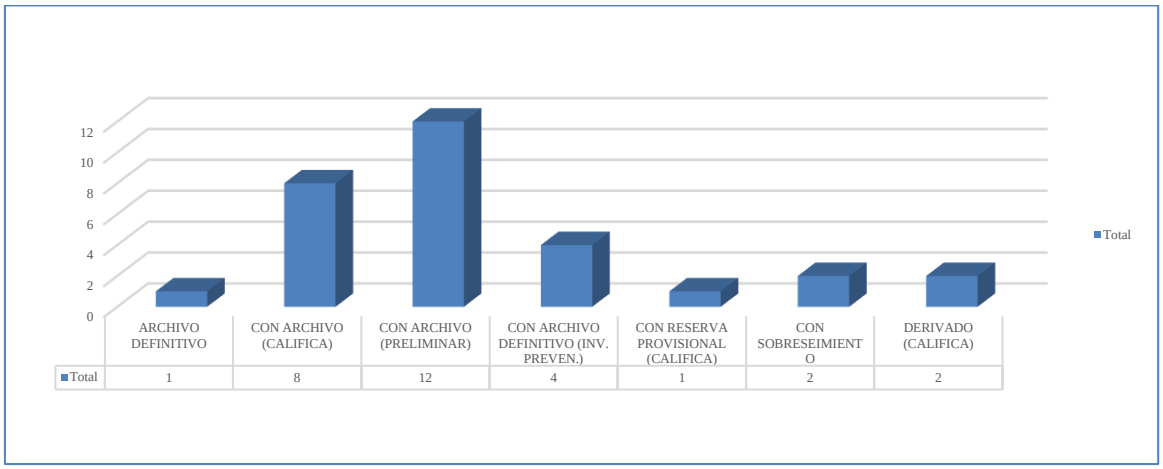
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se extrajo que, de un total de 109 casos registrados en el distrito fiscal de la San Martín desde el año 2015 hasta el 2020, 26 se archivaron en la etapa de calificación

de la denuncia, 65 se archivaron en la subetapa de investigación preliminar, 3 fueron sobreseídos en la etapa intermedia y solos en 2 se emitieron sentencias.

Figura 12

Análisis de los casos de delitos informáticos en Puno desde el año 2016 hasta 2020

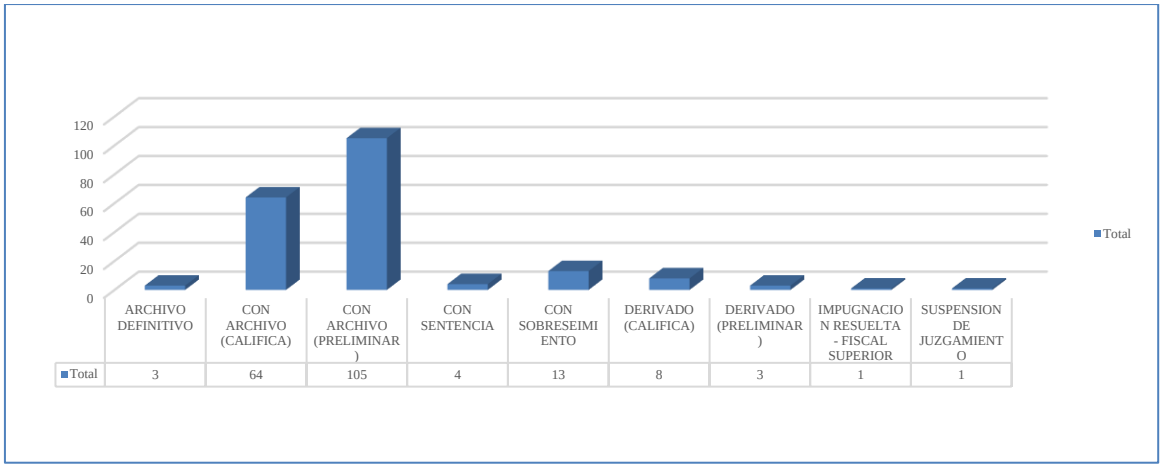


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se registró que, de un total de 30 casos registrados en el distrito fiscal de Puno desde el año 2016 hasta el 2020, 1 se archivó definitivamente en la investigación preparatoria, 8 se archivaron en la etapa de la calificación de la denuncia y 12 se archivaron en la subetapa preliminar. Ninguno de ellos llegó a la etapa de juzgamiento.

Figura 13

Análisis de los casos de delitos informáticos en Piura desde el año 2015 hasta 2020



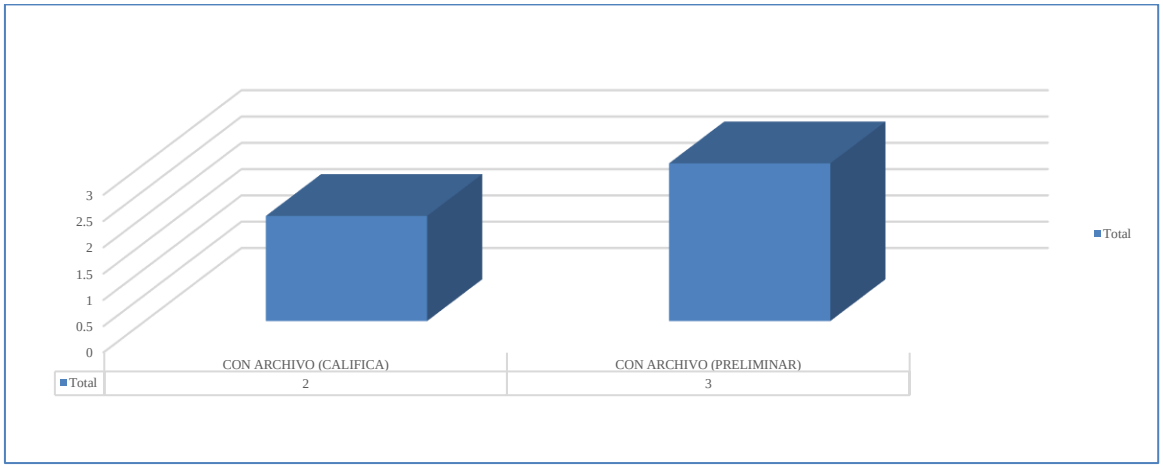
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se indicó que, de un total de 202 casos registrados en el distrito fiscal de Piura desde el año 2015 hasta el 2020, 3 fueron archivados definitivamente en la investigación preparatoria, 64 fueron archivados en la etapa de calificación de la denuncia,

105 se archivaron en la subetapa preliminar y 13 fueron sobreseídos en la etapa intermedia. Durante 6 años, solo en 4 casos se emitieron sentencias.

Figura 14

Análisis de los casos de delitos informáticos en Pasco desde el año 2018 hasta 2019

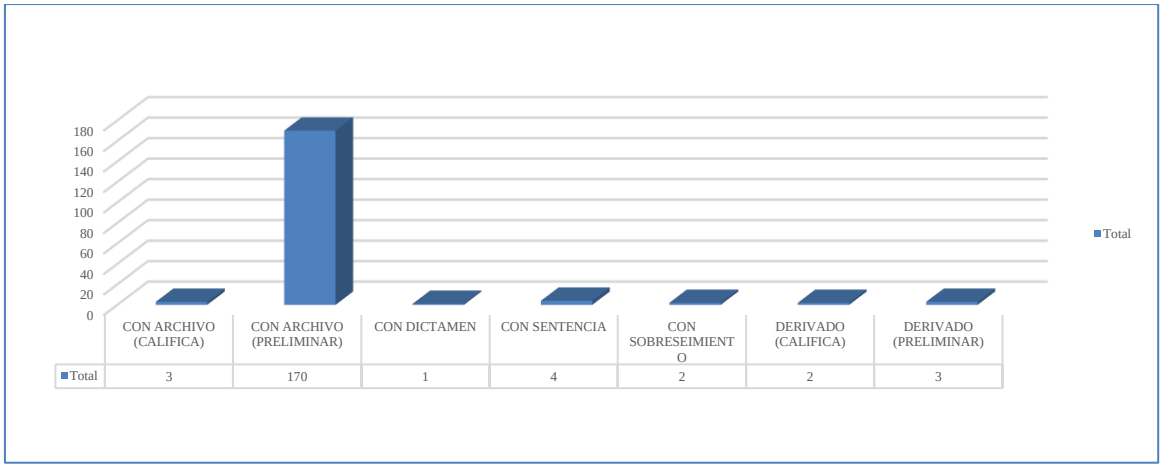


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se entendió que, de un total de 5 casos registrados en el distrito fiscal de Pasco desde el año 2018 hasta el 2019, 2 fueron archivados en la etapa de calificación de la denuncia y 3 fueron archivados en la subetapa preliminar. Ninguno de ellos llegó a la etapa de juzgamiento.

Figura 15

Análisis de los casos de delitos informáticos en Moquegua desde el año 2016 hasta 2020

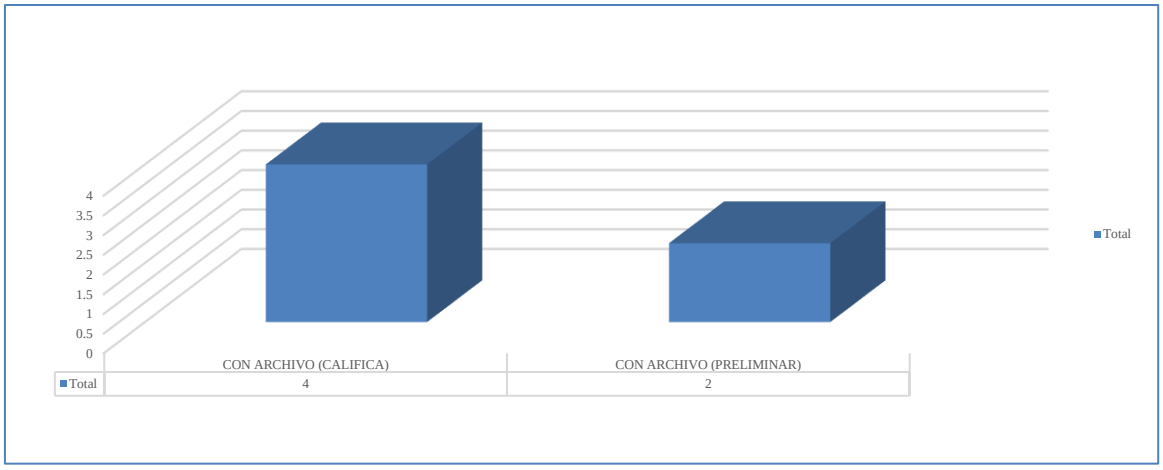


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se indujo que, de un total de 185 casos registrados en el distrito fiscal de Moquegua desde el año 2016 hasta el 2020, 3 se archivaron en la etapa de calificación de la denuncia, 170 fueron archivados en la subetapa de investigación preliminar, 2 fueron sobreseídos en etapa intermedia y solo 4 de ellos fueron sentenciados.

Figura 16

Análisis de los casos de delitos informáticos en Madre de Dios desde el año 2015 hasta 2019

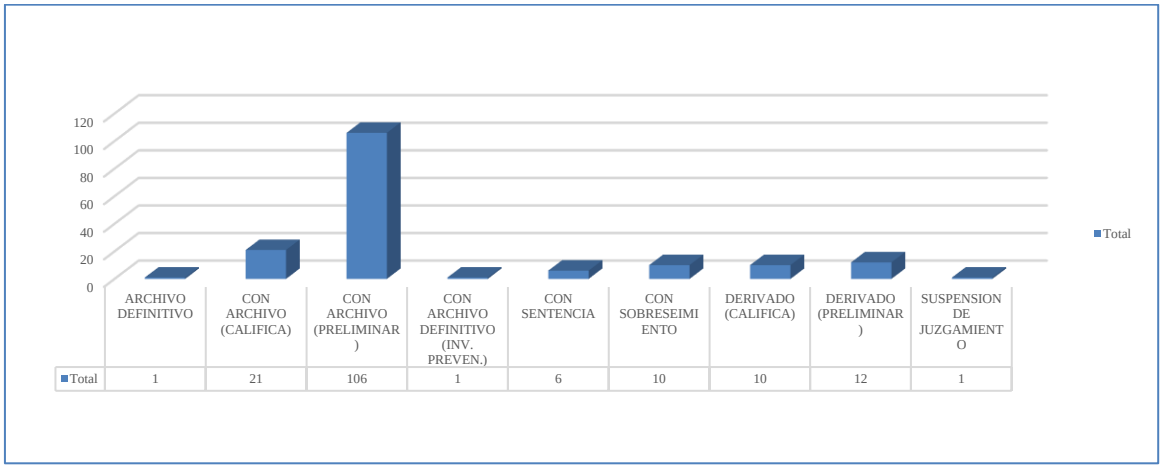


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se pensó que, de un total de 6 casos registrados en el distrito fiscal de Madre de Dios desde el año 2015 hasta el 2019, 4 fueron archivados en la etapa de calificación de la denuncia, 2 fueron archivados en la subetapa preliminar y ninguno de ellos llegó a la audiencia de juzgamiento.

Figura 17

Análisis de los casos de delitos informáticos en Loreto desde el año 2015 hasta 2020

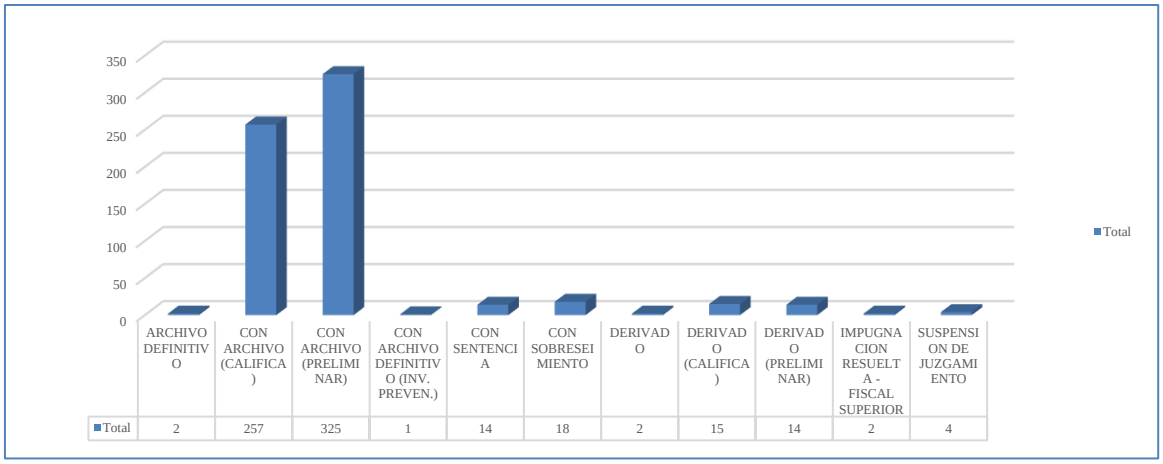


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se entendió que, de un total de 168 casos registrados en el distrito fiscal de Loreto desde el año 2015 hasta el 2020, 1 se archivó definitivamente en la investigación preparatoria, 21 se archivaron en la etapa de calificación de la denuncia, 106 se archivaron en la subetapa de investigación preliminar, 10 fueron sobreseídos en etapa intermedia y solo 6 fueron sentenciados.

Figura 18

Análisis de los casos de delitos informáticos en Lambayeque desde el año 2015 hasta 2020

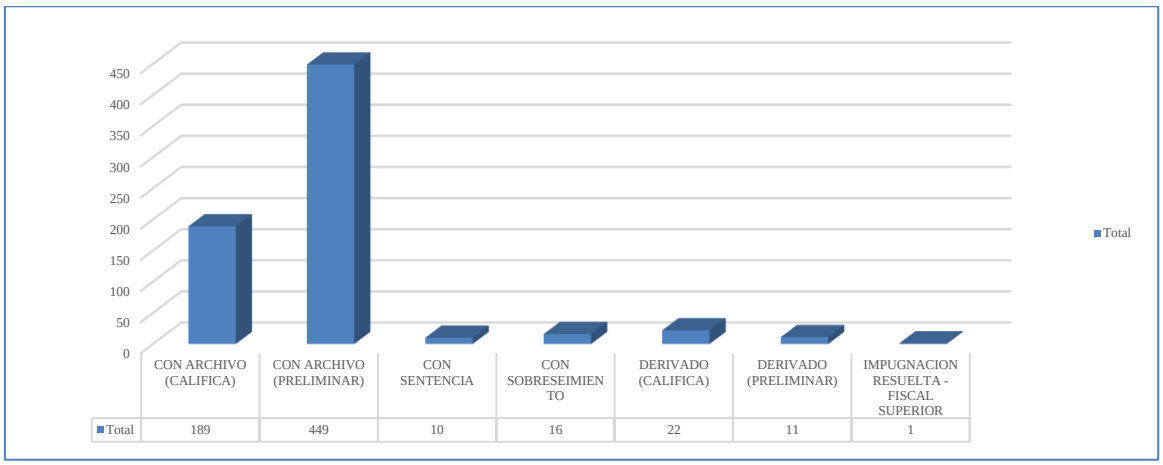


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 654 casos registrados en el distrito fiscal de Lambayeque desde el año 2015 hasta el 2020, se advirtieron múltiples casos de archivamiento, entre ellos, 2 casos archivados definitivamente en la etapa de investigación preparatoria, 257 archivados en la calificación de la denuncia, 325 archivados en la etapa preliminar y 1 caso con archivo definitivo en la investigación preventiva. Cabe indicar que durante los seis años solo llegaron a la etapa de juzgamiento 14 casos y con sobreseimiento en la etapa intermedia 18 casos.

Figura 19

Análisis de los casos de delitos informáticos en La Libertad desde el año 2015 hasta 2020



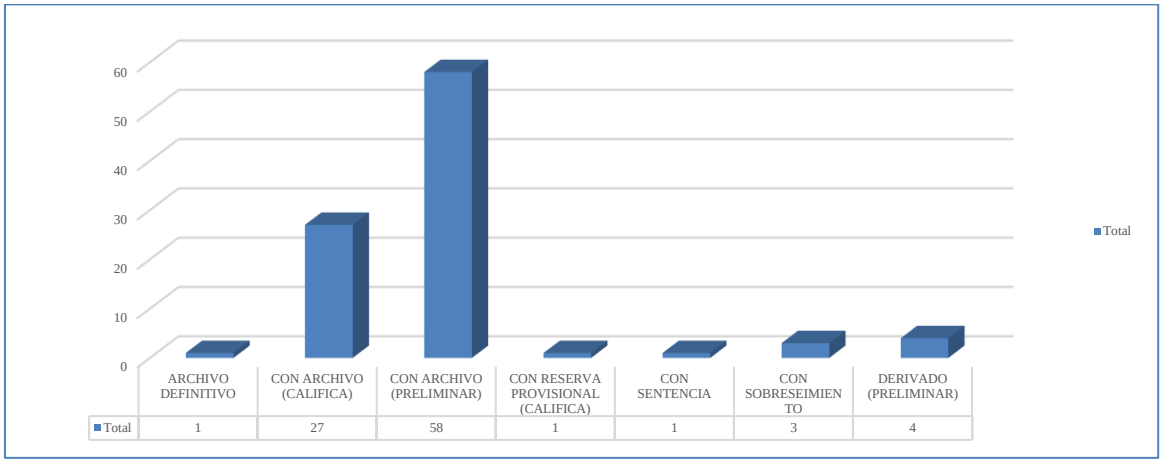
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se advirtió que, de un total de 698 casos registrados en el distrito fiscal de La Libertad desde el año 2015 hasta el 2020, 189 se archivaron en la calificación de la denuncia, 449 archivados en la etapa de investigación preliminar, solo en 10 casos se

emitieron sentencias en la etapa de juzgamiento y 16 con sobreseimientos en la etapa intermedia.

Figura 20

Análisis de los casos de delitos informáticos en Junín desde el año 2015 hasta 2020

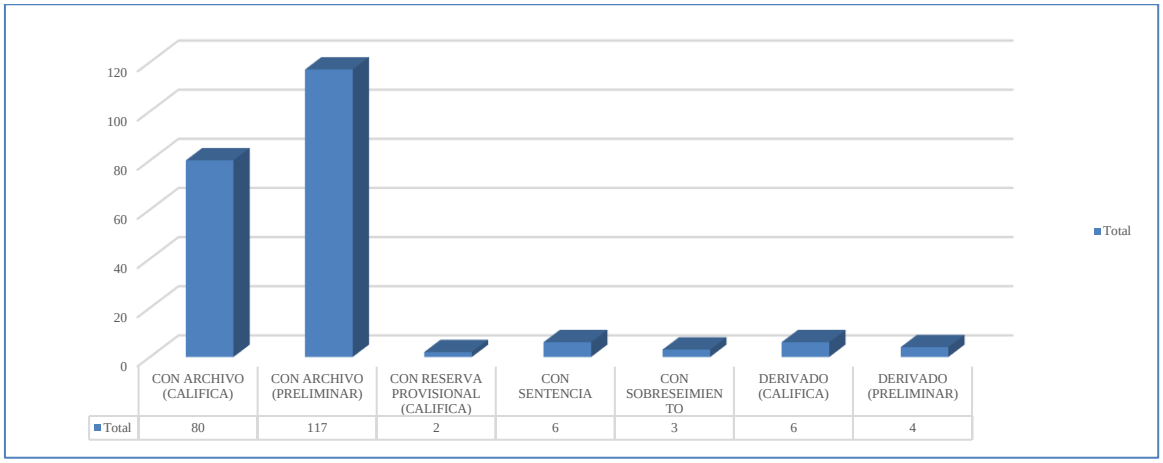


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se observó que, de un total de 95 casos registrados en el distrito fiscal de Junín desde el año 2015 hasta el 2020, 1 caso se archivó definitivamente en la etapa de investigación preparatoria, 27 archivados en la calificación de la denuncia, 58 archivados en la etapa preliminar, solo 1 llegó a la etapa de juzgamiento y 3 casos con sobreseimientos en la etapa intermedia.

Figura 21

Análisis de los casos de delitos informáticos en Ica desde el año 2015 hasta 2020



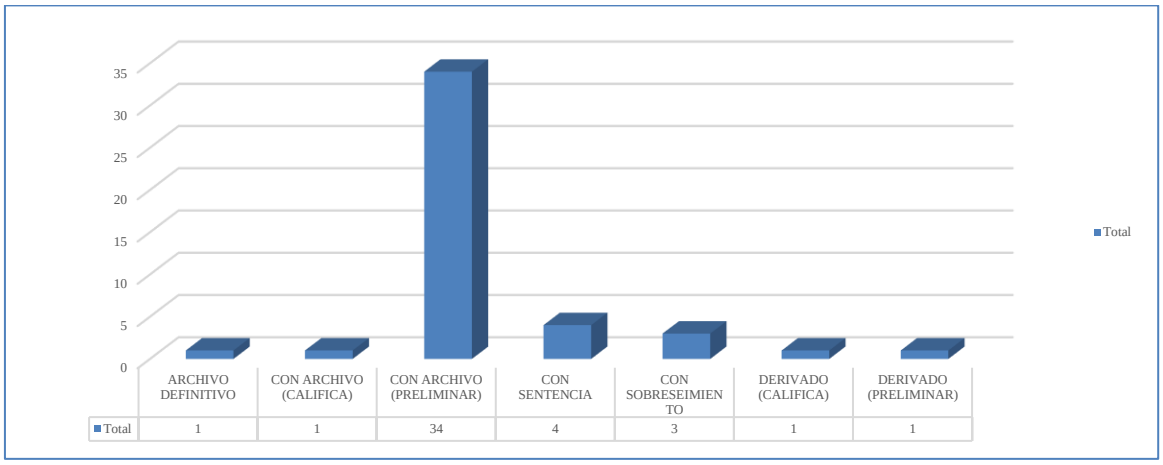
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se apreció que, de un total de 218 casos registrados en el distrito fiscal de Ica desde el año 2015 hasta el 2020, 80 casos archivados en la calificación de la denuncia,

117 archivados en la etapa preliminar, solo en 6 casos se emitieron sentencias en la etapa de juzgamiento y 3 casos fueron sobreseídos en la etapa intermedia.

Figura 22

Análisis de los casos de delitos informáticos en Huaura desde el año 2015 hasta 2020

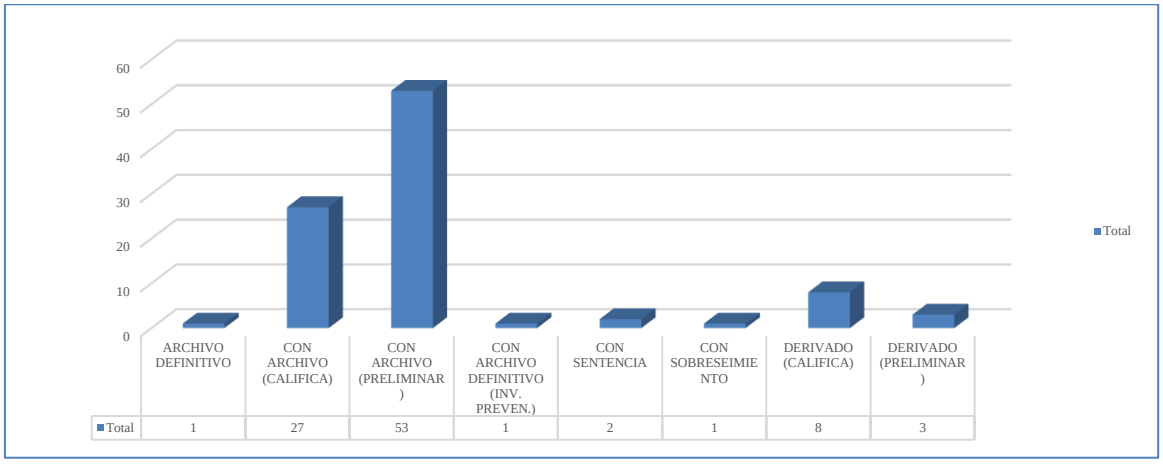


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se detalló que, de un total de 45 casos registrados en el distrito fiscal de Huaura desde el año 2015 hasta el 2020, 1 caso se archivó definitivamente en la etapa de investigación preparatoria, 1 caso se archivó en la calificación de la denuncia, 34 casos se archivaron en la etapa preliminar, solo en 4 casos se emitieron sentencias en la etapa de juzgamiento y 3 casos fueron sobreseídos en la etapa intermedia.

Figura 23

Análisis de los casos de delitos informáticos en Huánuco desde el año 2015 hasta 2020



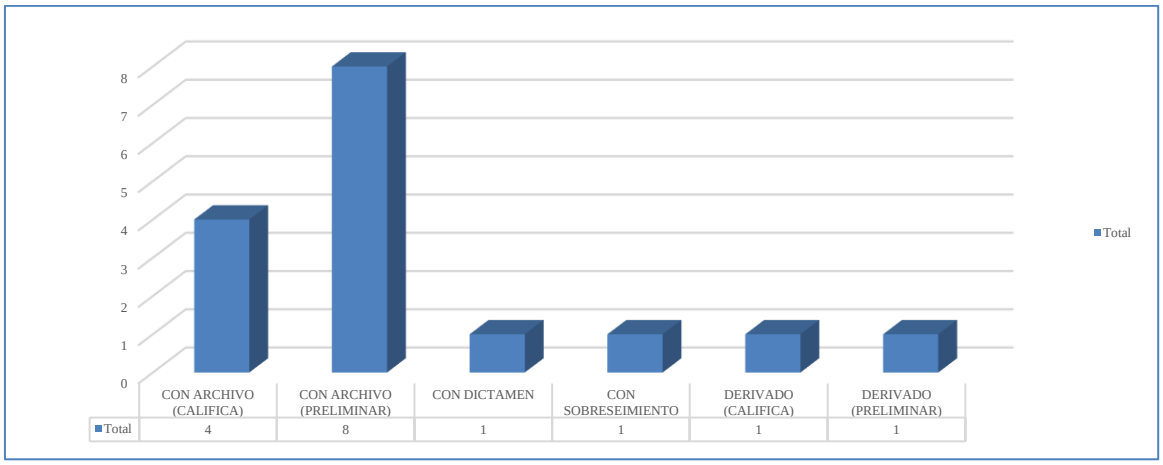
Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 96 casos registrados en el distrito fiscal de Huánuco desde el año 2015 hasta el 2020, se advirtió múltiples casos de archivamiento, entre ellos, 1 caso archivado definitivamente en la etapa de investigación preparatoria, 27 casos archivados

en la calificación de la denuncia, 53 archivados en la etapa de investigación preliminar y 1 caso con archivo definitivo en la investigación preventiva. Cabe señalar que durante los seis años solo llegaron a la etapa de juzgamiento 2 casos y se sobreseyó 1 caso en la etapa intermedia.

Figura 24

Análisis de los casos de delitos informáticos en Huancavelica desde el año 2015 hasta 2019

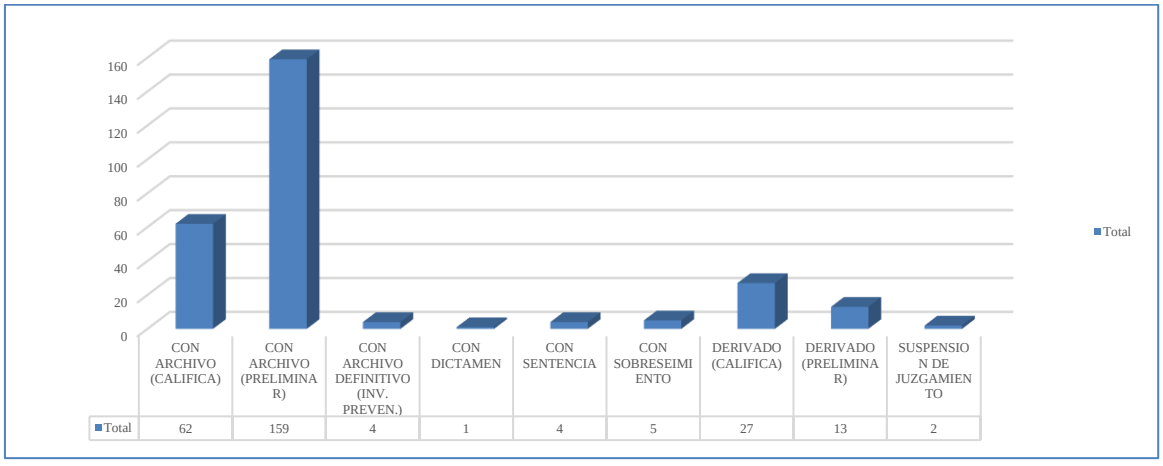


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se determinó que, de un total de 16 casos registrados en el distrito fiscal de Huancavelica en los años 2015, 2016, 2018 y 2019, se detalla 4 casos archivados en la calificación de la denuncia, 8 se archivaron en la etapa de investigación preliminar y 1 caso se sobreseyó en la etapa intermedia. Es curioso observar que durante esos cuatro años no haya algún caso que llegase a la etapa de juzgamiento.

Figura 25

Análisis de los casos de delitos informáticos en Cusco desde el año 2015 hasta 2020

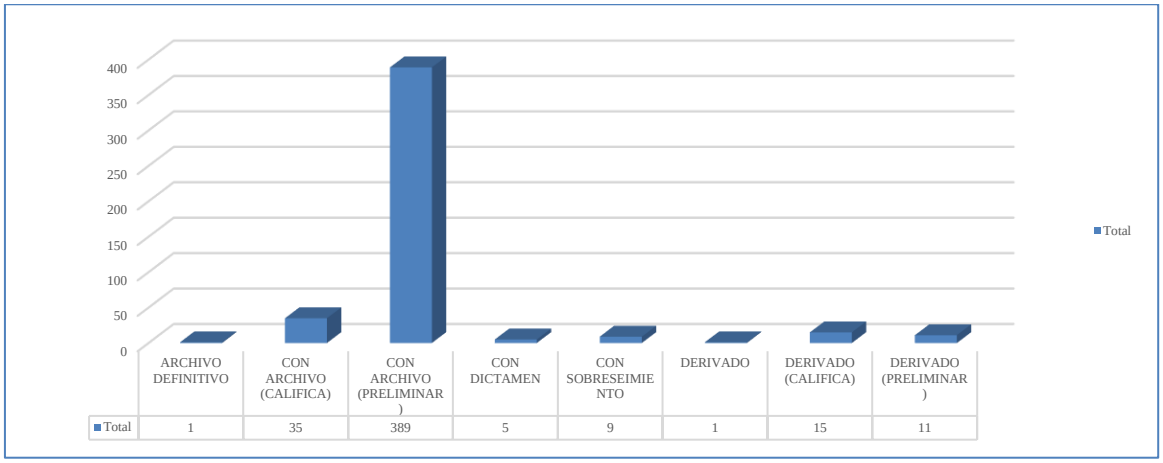


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 277 casos registrados en el distrito fiscal de Cusco desde el año 2015 hasta el 2020, se advirtieron múltiples casos de archivamiento, entre ellos, 62 casos archivados en la calificación de la denuncia, 159 archivados en la etapa preliminar y 4 casos con archivo definitivo en la investigación preventiva. Es peculiar indicar que durante los seis años solo llegase a la etapa de juzgamiento 4 casos y con sobreseimiento en la etapa intermedia 5 casos.

Figura 26

Análisis de los casos de delitos informáticos en Cañete desde el año 2015 hasta 2020

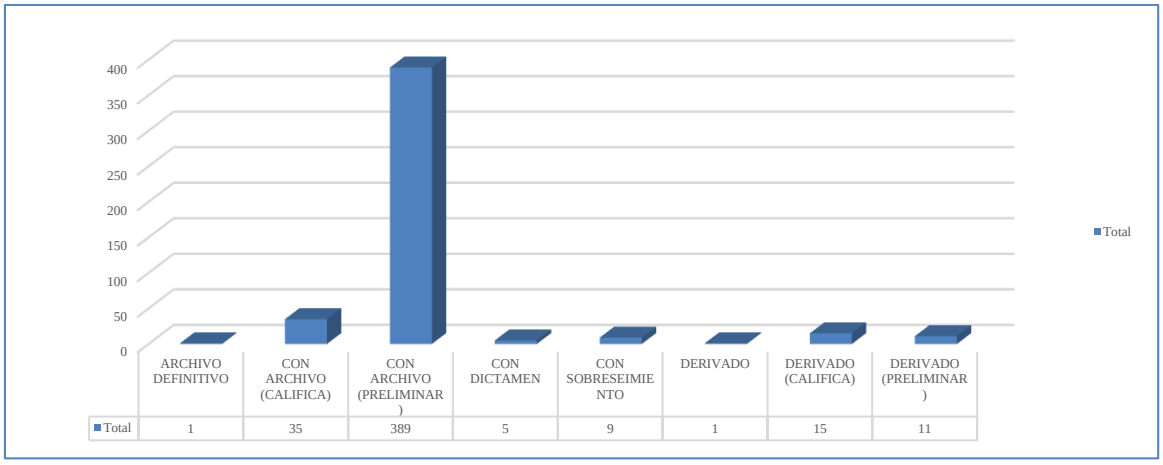


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se obtuvo que, de un total de 13 casos registrados en el distrito fiscal de Cañete en los años 2015, 2017 al 2020, solo 6 casos fueron archivados en la calificación de la denuncia y 7 archivados en la etapa preliminar, dando que pensar sobre la ausencia de los casos sentenciados.

Figura 27

Análisis de los casos de delitos informáticos en Callao desde el año 2015 hasta 2020

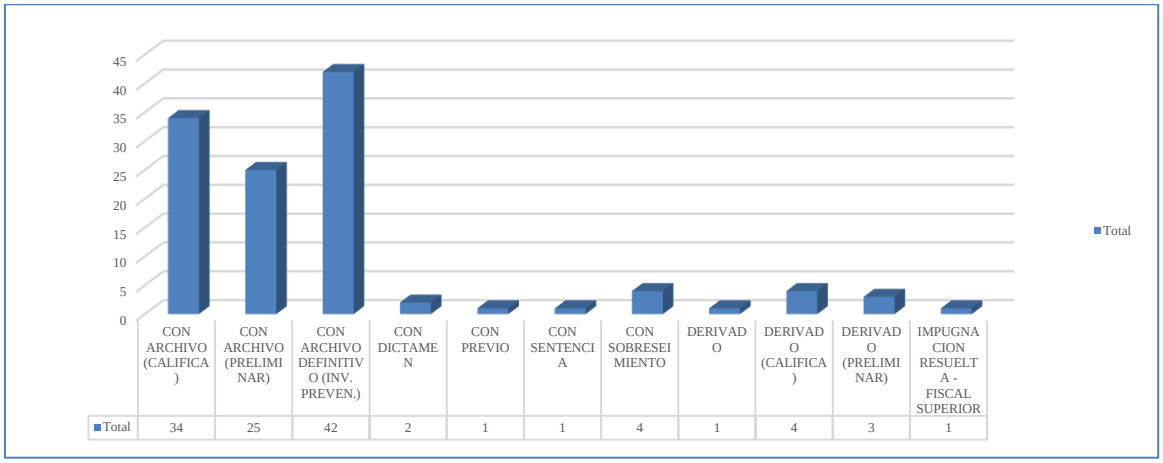


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se agregó que, de un total de 466 casos registrados en el distrito fiscal de Callao desde el año 2015 hasta el 2020, 1 caso archivado definitivamente en la etapa de investigación preparatoria, 35 casos archivados en la calificación de la denuncia, 389 archivados en la etapa preliminar y solo 9 casos con sobreseimiento. Dato peculiar es que durante los seis años no se haya sentenciado un solo caso relacionado a los delitos informáticos.

Figura 28

Análisis de los casos de delitos informáticos en Cajamarca desde el año 2016 hasta 2020

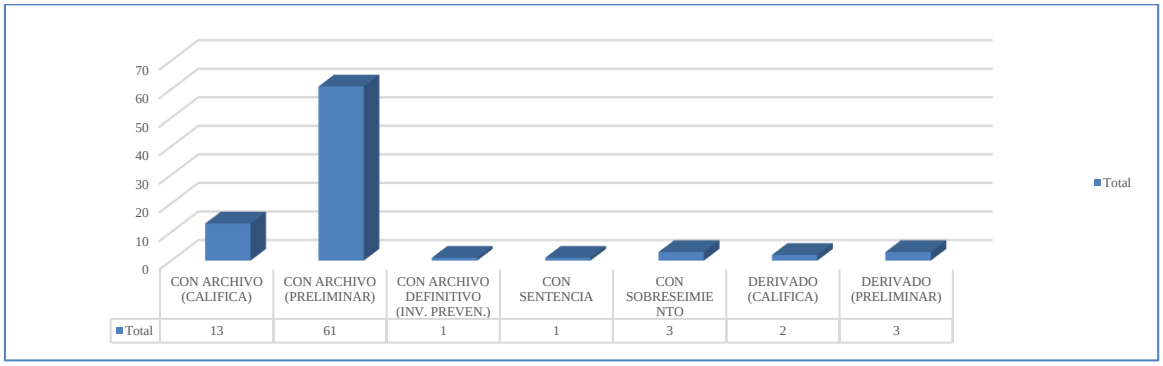


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se mostró que, un total de 118 casos registrados en el distrito fiscal de Cajamarca desde el año 2016 hasta el 2020, se advirtieron múltiples casos de archivamiento, entre ellos, 34 casos archivados en la calificación de la denuncia, 25 archivados en la etapa preliminar y 42 casos con archivo definitivo en la investigación preventiva. Cabe indicar que durante los cinco años solo llegase a la etapa de juzgamiento 1 caso y con sobreseimiento en la etapa intermedia 4 casos.

Figura 29

Análisis de los casos de delitos informáticos en Ayacucho desde el año 2016 hasta 2020

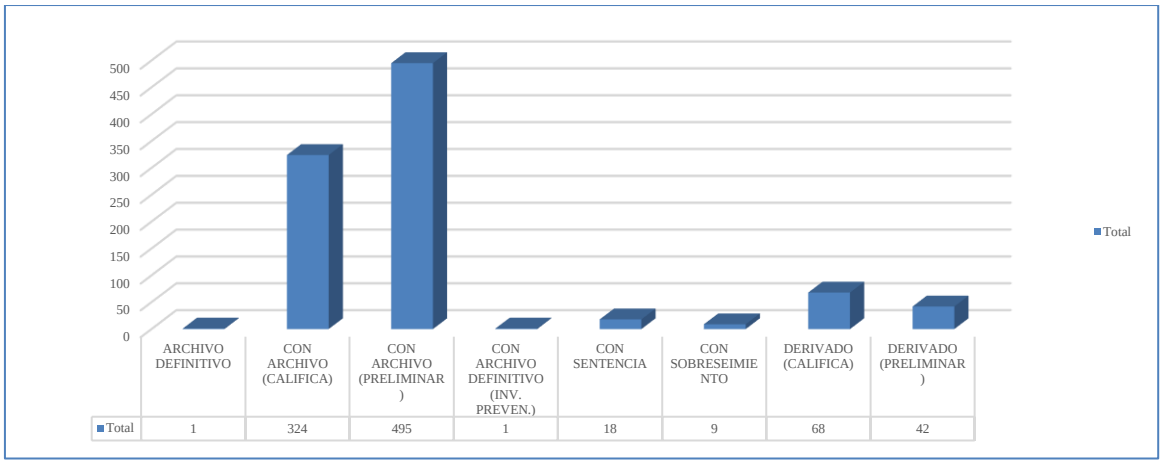


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se registró que, de un total de 84 casos registrados en el distrito fiscal de Ayacucho desde el año 2016 hasta el 2020, 13 casos fueron archivados en la etapa de calificación de la denuncia, 61 se archivaron en la etapa preliminar y 1 caso fue archivado definitivamente en la etapa de investigación preventiva. A su vez, solo en 1 caso se emitió sentencia en la etapa de juzgamiento y 3 casos fueron sobreseídos en la etapa intermedia.

Figura 30

Análisis de los casos de delitos informáticos en Arequipa desde el año 2015 hasta 2020

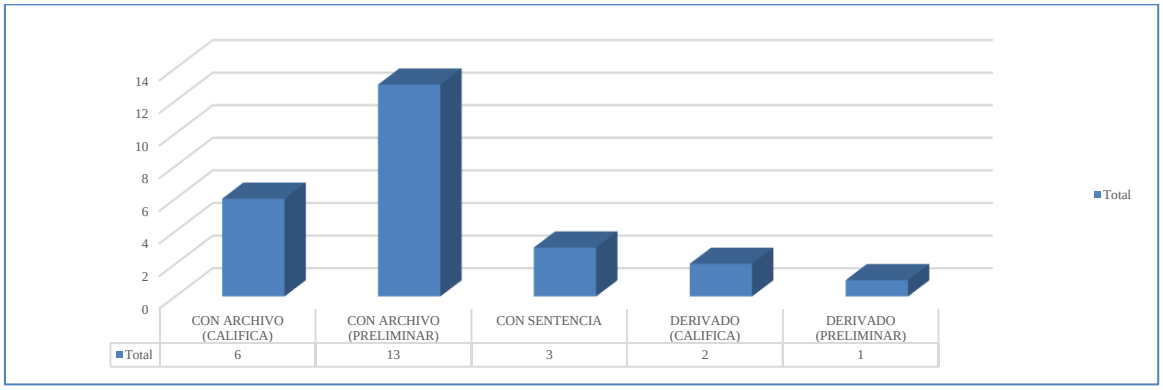


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 958 casos registrados en el distrito fiscal de Arequipa desde el año 2016 hasta el 2020, se advirtieron múltiples casos de archivamiento, entre ellos, 1 caso archivado definitivamente en la etapa de investigación preparatoria, 324 casos archivados en la calificación de la denuncia, 495 archivados en la etapa preliminar y 1 caso con archivo definitivo en la investigación preventiva. Cabe mencionar que durante los cinco años solo llegaron a la etapa de juzgamiento 18 casos y con sobreseimiento en la etapa intermedia 9 casos.

Figura 31

Análisis de los casos de delitos informáticos en Apurímac desde el año 2016 hasta 2020

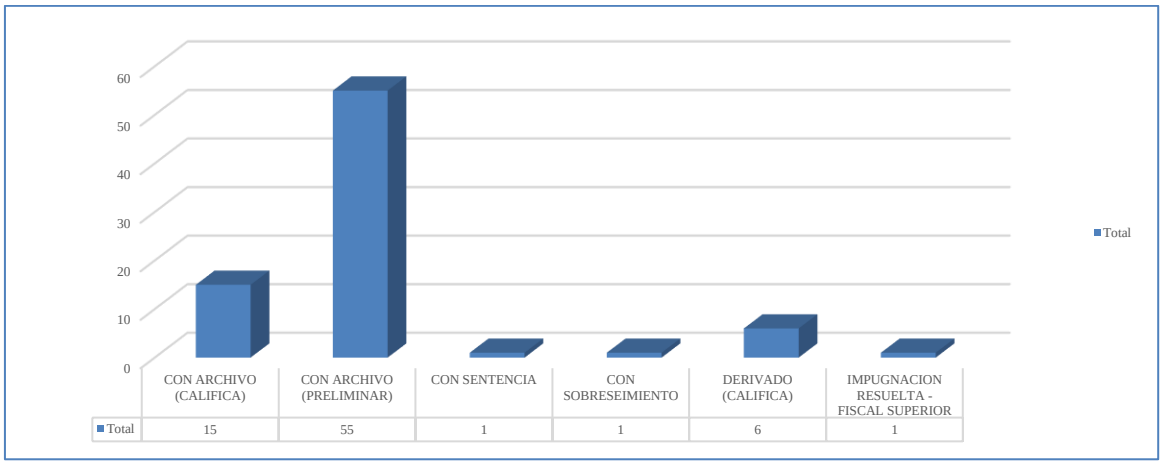


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se demostró que, de un total de 13 casos registrados en el distrito fiscal de Apurímac desde el año 2016 hasta 2020, 6 casos fueron archivados en la etapa de calificación de la denuncia, 13 se archivaron en la etapa preliminar y un dato curioso es que solo llegaron a la etapa de juzgamiento 3 casos.

Figura 32

Análisis de los casos de delitos informáticos en Amazonas desde el año 2015 hasta 2020

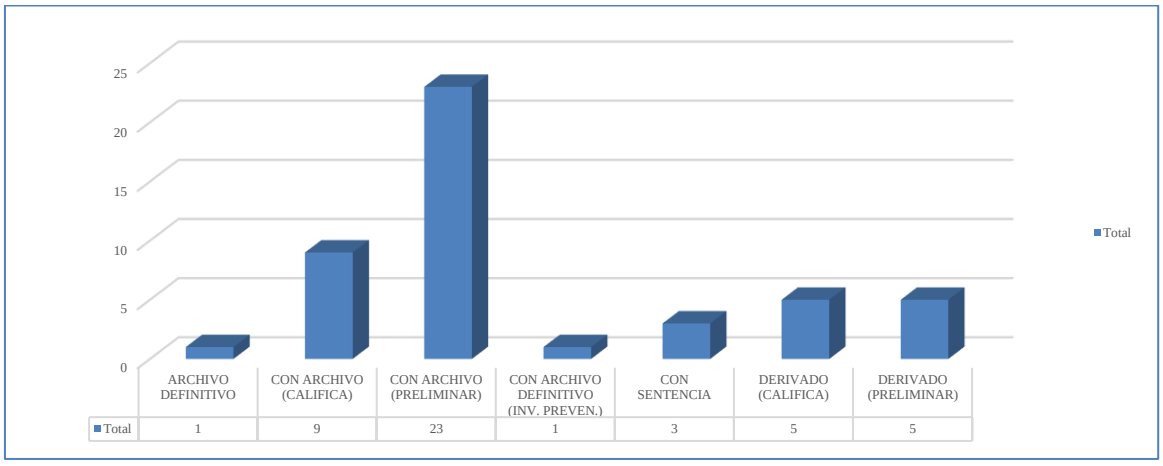


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: Se abordó que, de un total de 79 casos registrados en el distrito fiscal de Amazonas desde el año 2015 hasta el 2020, 15 casos fueron archivados en la etapa de calificación de la denuncia y 55 se archivaron en la etapa preliminar. Una particularidad es que solo 1 caso llegó a la etapa de juzgamiento y 1 caso se sobreseyó en la etapa intermedia.

Figura 33

Análisis de los casos de delitos informáticos en Áncash desde el año 2015 hasta 2020



Fuente: Elaboración propia a partir de los resultados obtenidos.

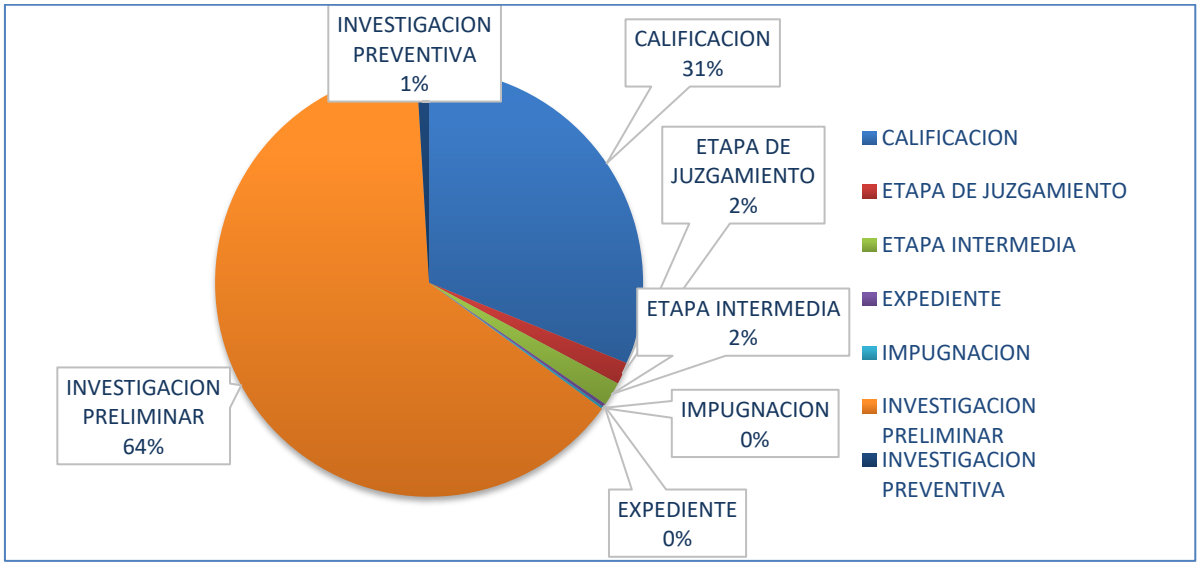
Interpretación: De un total de 47 casos registrados en el distrito fiscal de Áncash desde el año 2015 hasta el 2020, se advirtieron múltiples casos de archivamiento, entre ellos, 1 caso

archivado definitivamente en la etapa de investigación preparatoria, 9 casos archivados en la calificación de la denuncia, 23 fueron archivados en la etapa preliminar y 1 caso con archivo definitivo en la investigación preventiva. Asimismo, se detalla que durante los seis años solo llegaron a la etapa de juzgamiento 3 casos.

Figura 34

Análisis general de la etapa final de los casos fiscales

Etapa final	Cantidad de casos	Porcentaje
Calificación	1954	31.1%
Etapa de Juzgamiento	104	1.7%
Etapa Intermedia	113	1.8%
Expediente	16	0.3%
Impugnación	11	0.2%
Investigación Preliminar	4017	64.0%
Investigación Preventiva	59	0.9%
Total	**6274**	**100%**



Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación general: Luego de realizar el análisis de los documentos con la información de 33 de los 34 distritos fiscales nos permitió detectar que el Sistema de Administración de Justicia a través de las Fiscalías Provinciales resulta inapropiado en el procesamiento de los delitos informáticos, puesto que se evidencian algunas deficiencias durante la investigación, la conservación de la prueba digital y la proposición de actos de investigación por lo que terminan archivándose en investigación preparatoria o sobreseyéndose en la etapa intermedia.

Asimismo, se debe considerar la carencia de una adecuada infraestructura, la falta de herramientas tecnológicas, la ausencia de material logístico idóneo, la insuficiencia de

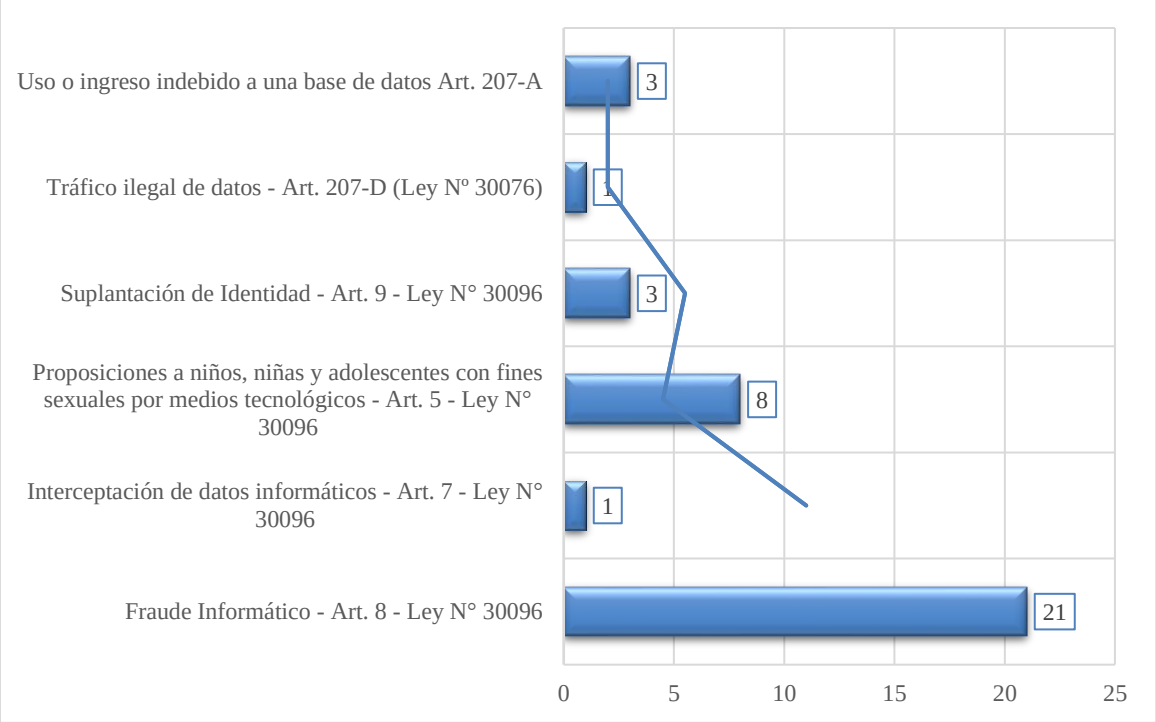
personal técnico especializado, y una percepción negativa de la sociedad, esto es, la desconfianza de los justiciables en nuestras instituciones públicas.

A su vez, debe mencionarse lo referido a la cifra negra en los delitos informáticos, es decir, la cantidad de casos que se desconocen o los que no han sido denunciados en el registro del Ministerio Público porque las víctimas desconfían de nuestra Administración de Justicia, también se advierte un desconocimiento sobre el procedimiento y el lugar en dónde se debe acudir ante cualquier vulneración relacionada a los medios digitales.

3.1.2. Análisis documental del Poder Judicial

Figura 35

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2016

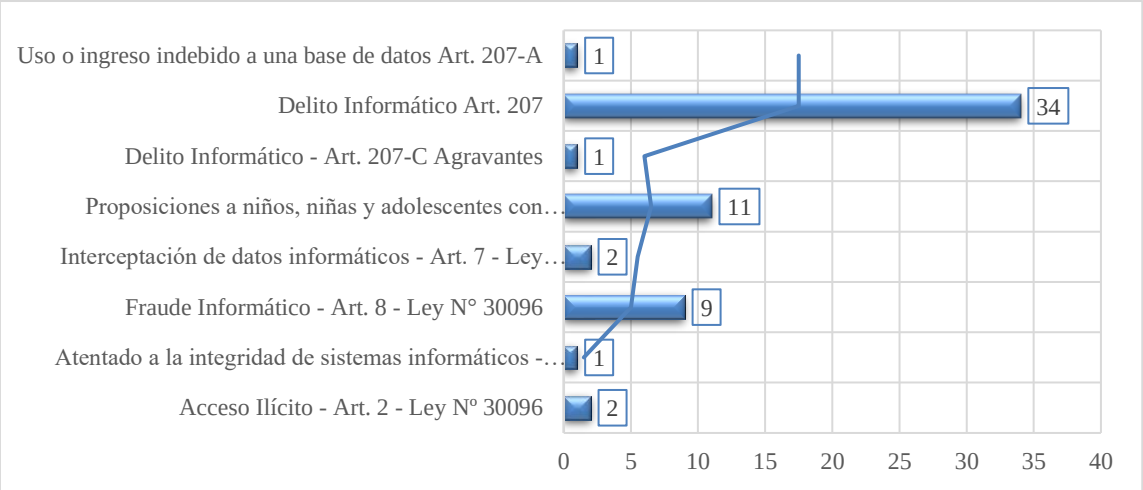


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 37 casos atendidos durante el año 2016, los cuales se encuentran debidamente contenidos en el Registro Nacional de Condenas, 33 fueron sentenciados por la comisión de delitos informáticos regulados en la Ley N.° 30096 y 30171, entre los más recurrentes encontramos, fraude informático, interceptación de datos informáticos, suplantación de identidad y proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Agregado a ello, 4 casos del total fueron sentenciados por la comisión de delitos contra el patrimonio regulados desde el artículo 185 al 208, entre ellos, tráfico ilegal de datos y uso o ingreso indebido a una base de datos.

Figura 36

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2017

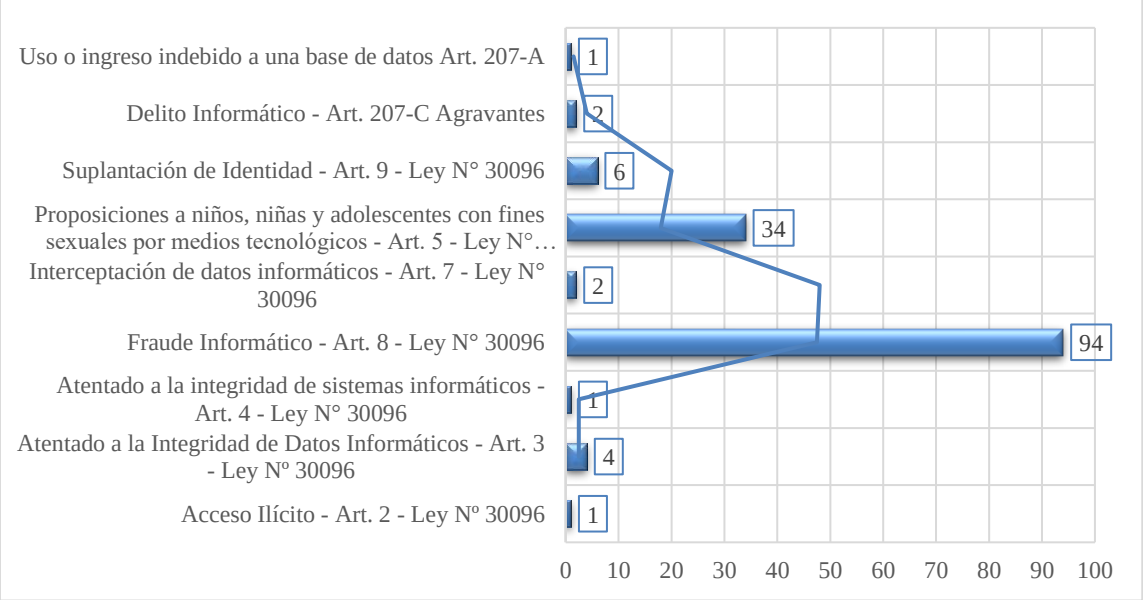


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 61 casos atendidos durante el año 2017, los cuales se encuentran debidamente contenidos en el Registro Nacional de Condenas, 25 fueron sentenciados por la comisión de delitos informáticos regulados en la Ley N.° 30096 y 30171, entre los más recurrentes encontramos, el acceso ilícito, atentado a la integridad de sistemas informáticos, fraude informático, interceptación de datos informáticos, proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Adicionalmente, 1 delito informático con agravantes, 34 delitos informáticos regulados en el artículo 207 y 1 de ellos configurado como uso o ingreso indebido a una base de datos.

Figura 37

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2018

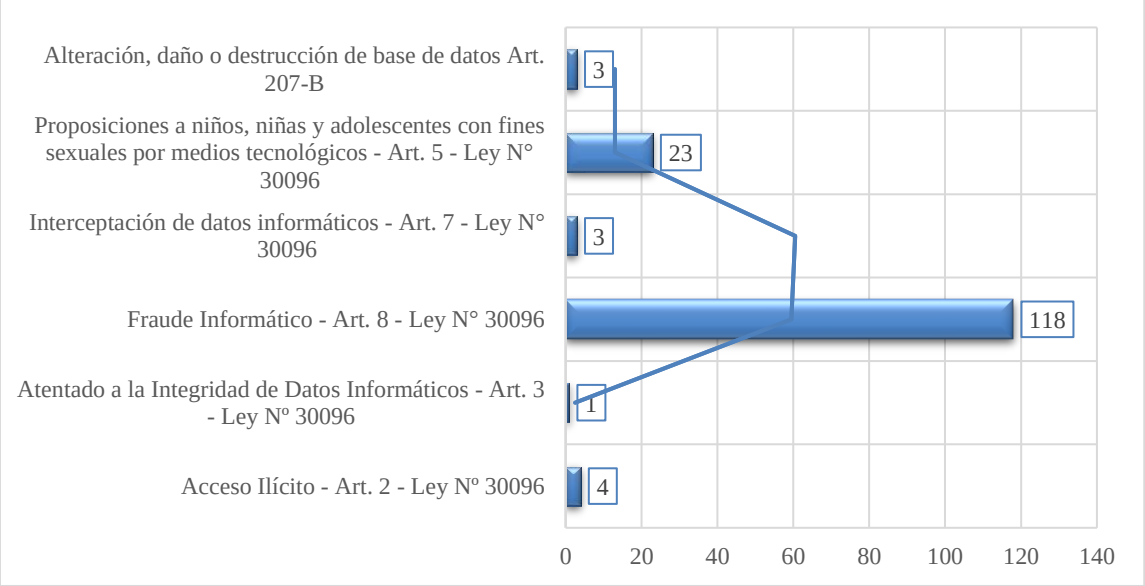


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 145 casos atendidos durante el año 2018, los cuales se encuentran debidamente contenidos en el Registro Nacional de Condenas, 142 fueron sentenciados por la comisión de delitos informáticos regulados en la Ley N.° 30096 y 30171, entre los más recurrentes encontramos, el acceso ilícito, atentado a la integridad de datos informáticos y sistemas informáticos, fraude informático, interceptación de datos informáticos, proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y suplantación de identidad. En adición, 3 casos del total fueron sentenciados por la comisión de delitos contra el patrimonio regulados desde el artículo 185 al 208, entre ellos, el uso o ingreso indebido a una base de datos y el delito informático regulado en artículo 207 con agravantes.

Figura 38

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2019

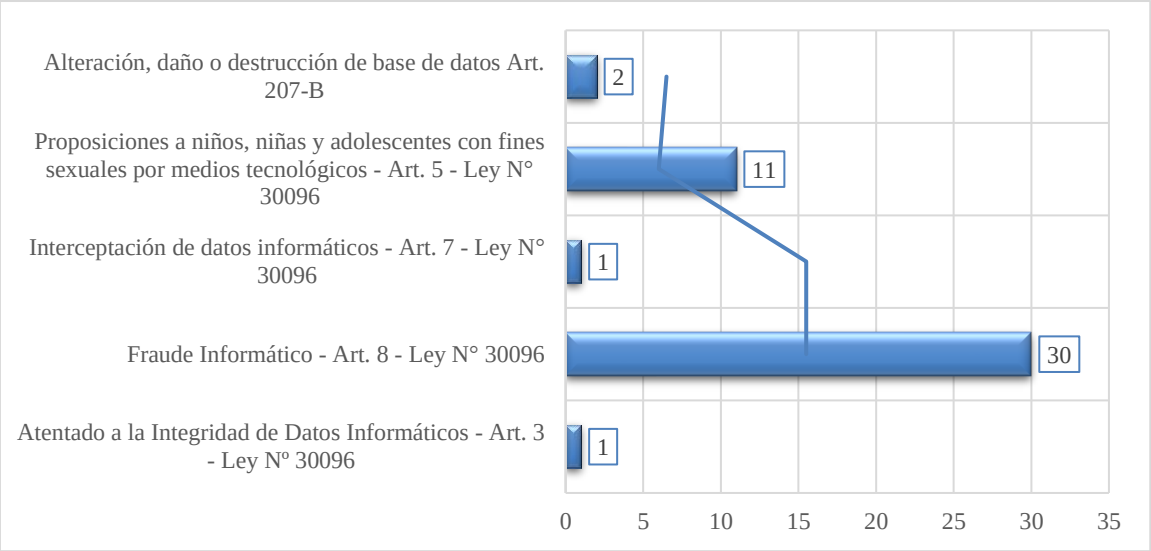


Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 152 casos atendidos durante el año 2019, los cuales se encuentran debidamente contenidos en el Registro Nacional de Condenas, 149 fueron sentenciados por la comisión de delitos informáticos regulados en la Ley N.° 30096 y 30171, entre los más recurrentes encontramos, acceso ilícito, atentado a la integridad de datos informáticos, fraude informático, interceptación de datos informáticos, proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Adicionalmente, 3 casos del total fueron sentenciados por la comisión de delitos contra el patrimonio regulados desde el artículo 185 al 208, entre ellos, la alteración, daño o destrucción de base de datos regulado en el artículo 207-B.

Figura 39

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2020



Fuente: Elaboración propia a partir de los resultados obtenidos.

Interpretación: De un total de 45 casos atendidos durante el año 2020, los cuales se encuentran debidamente contenidos en el Registro Nacional de Condenas, 43 fueron sentenciados por la comisión de delitos informáticos regulados en la Ley N.° 30096 y 30171, entre los más recurrentes encontramos, el atentado a la integridad de datos informáticos, fraude informático, interceptación de datos informáticos, proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. Agregado a ello, 2 casos del total fueron sentenciados por la comisión de delitos contra el patrimonio regulados desde el artículo 185 al 208, entre ellos, la alteración, daño o destrucción de base de datos regulado en el artículo 207-B.

Figura 40

Análisis general de los delitos informáticos

Delitos	Cantidad de casos	Porcentaje
Acceso Ilícito - Art. 2 - Ley Nº 30096	7	1.8%
Atentado a la integridad de datos informáticos - Art. 3 - Ley Nº 30096	6	1.5%
Atentado a la integridad de sistemas informáticos - Art. 4 - Ley N° 30096	2	0.5%
Fraude Informático - Art. 8 - Ley N° 30096	272	69.4%
Interceptación de datos informáticos - Art. 7 - Ley N° 30096	9	2.3%
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos - Art. 5 - Ley N° 30096	87	22.2%
Suplantación de Identidad - Art. 9 - Ley N° 30096	9	2.3%
Total	**392**	**100%**

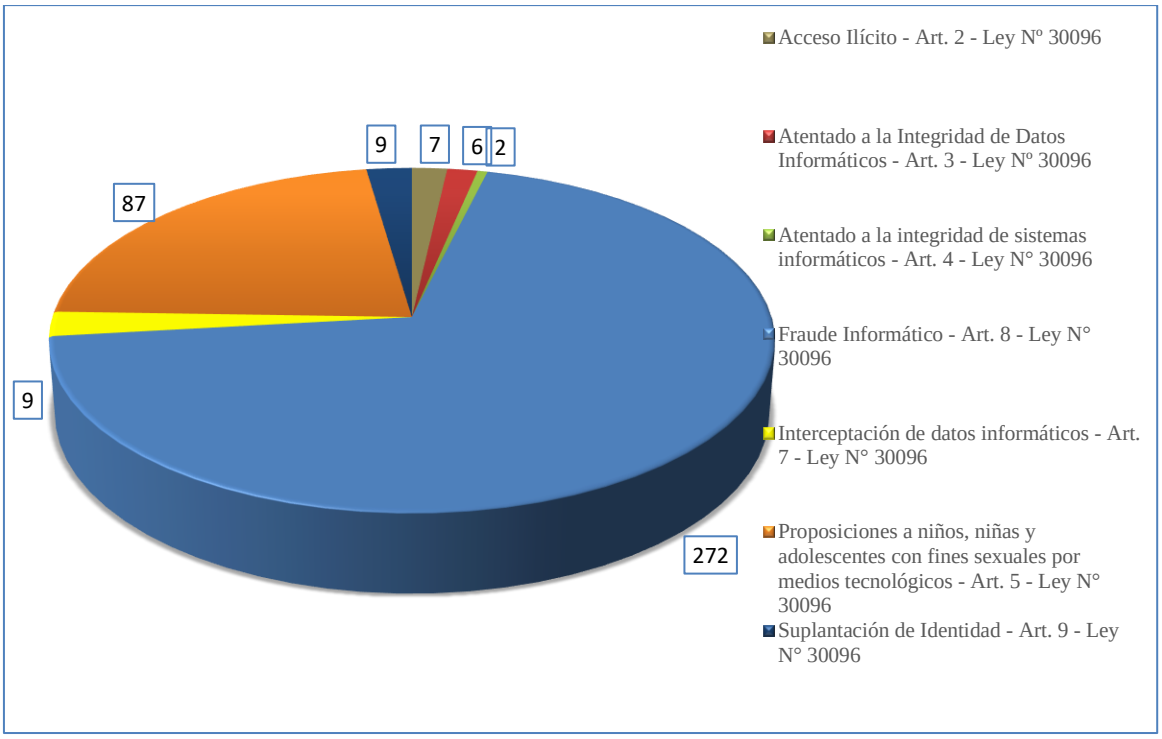
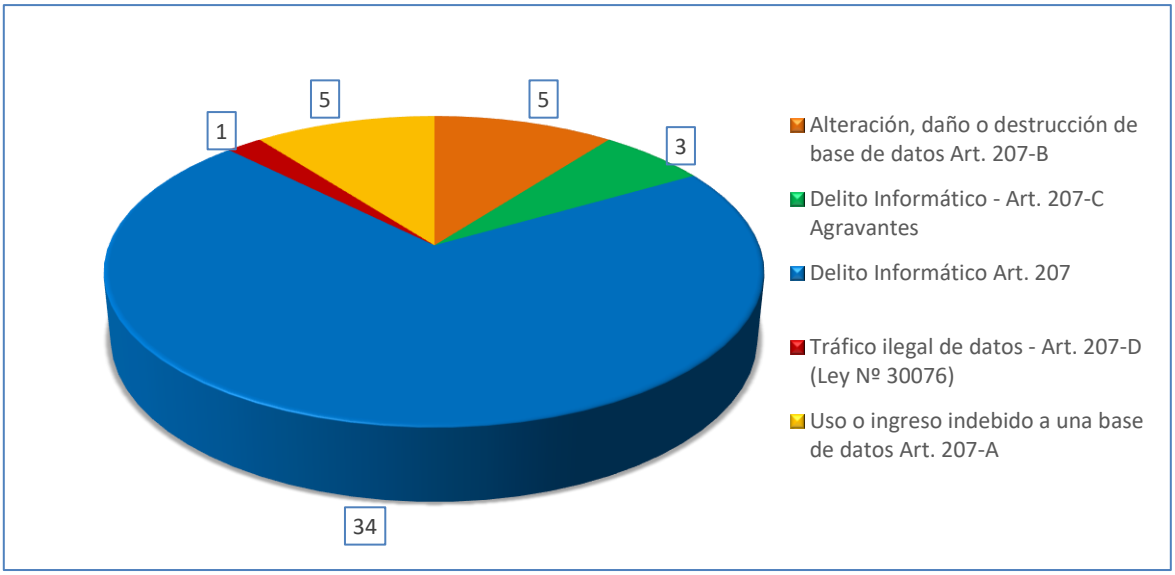


Figura 41

Análisis general de los delitos contra el patrimonio (artículo 185 al 208)

Delitos	Cantidad de Casos	Porcentaje
Alteración, daño o destrucción de base de datos Art. 207-B	5	10.42%
Delito Informático - Art. 207-C Agravantes	3	6.25%
Delito Informático Art. 207	34	70.83%
Tráfico ilegal de datos - Art. 207-D (Ley Nº 30076)	1	2.08%
Uso o ingreso indebido a una base de datos Art. 207-A	5	10.42%
Total	**48**	**100%**



Interpretación general:

Habiendo revisado el análisis documental de la información proporcionada por la Sub Gerencia de Estadística de la Gerencia de Planificación del Poder Judicial se descubrió que la ausencia de Juzgados Especializados en Ciberdelincuencia impide la realización de una eficiente impartición de justicia, debido a que aún no cuentan con conocimiento especializado sobre la valoración de la prueba digital, se presenta inconvenientes al momento de recibir la información técnica proporcionada por la fiscalía y la defensa del acusado, así como resulta contraproducente que los jueces resuelvan un día casos de hurto o robo y al día siguiente un caso tan complejo como ciberdelincuencia, por lo que resulta necesaria su implementación como correlato de la Fiscalía Especializada en Ciberdelincuencia.

En el análisis documental se mostraron los casos atendidos por las Fiscalías Provinciales, comprobándose que nuestra actual Administración de Justicia no resulta apropiada para el procesamiento de los delitos informáticos, principalmente porque carecen de la capacidad especializada para proponer diligencias y llevar a cabo investigaciones idóneas con el afán de esclarecer los hechos e individualizar a los presuntos responsables del ilícito penal. Asimismo, se dilucidó que los Juzgados necesitan el mismo nivel de especialización para que en la etapa de juzgamiento puedan comprender con mayor amplitud los elementos propios de los delitos informáticos, exista una mejor valoración de la prueba y consecuentemente entiendan los conceptos técnicos que se utilizan durante la audiencia para lograr una inmediación óptima.

3.2. Resultados del análisis de las entrevistas

En este apartado de los resultados se transcribieron las respuestas de las preguntas formuladas a nuestros especialistas nacionales e internacionales, las cuales fueron planteadas en relación a los objetivos trazados en la presente investigación. Con el propósito de preservar la integridad de la información obtenida, se extrajo el contenido más relevante e imprescindible para responder los objetivos planteados, tal y como se describe a continuación:

3.2.1. Análisis de las entrevistas internacionales

OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.

1. ¿Cuáles son las deficiencias de las Fiscalías y Juzgados Especializados en la atención de los casos de Ciberdelincuencia?

El Dr. Carretero (2020) manifestó que la mayor deficiencia es la capacitación de profesionales y de los operadores del derecho, no solo por los temas jurídicos sino por las cuestiones técnicas porque este tipo de delitos se maneja un lenguaje totalmente distinto, hay una forma de evidenciar diferente y a la vez es un proceso que difiere de los otros tipos penales.

En relación a esta pregunta el Dr. García (2020) señaló que la deficiencia radica en la falta de capacitación de los operadores judiciales y los demás colaboradores que actúan en el proceso por la comisión de un delito de estas características. Es importante privilegiar el recurso humano, así como el recurso técnico relacionado al hardware y software, dado que para formar un equipo consolidado es necesario que cuenten con las herramientas que sean útiles para las investigaciones que se llevan a cabo.

La Dra. Lamperti (2020) comentó que la deficiencia principal en Argentina es la ausencia de Fiscalías Especializadas porque hasta la fecha solo han implementado en algunas provincias como Chubut y en la Ciudad de Buenos Aires. Sin embargo, el hecho de no contar con una mayor cantidad de fiscalías en todo el país genera un notorio retraso y por tanto se debería evaluar cómo es el tratamiento de la evidencia digital y cómo investigan los casos que tienen componentes informáticos.

Dentro de ese orden de ideas el Dr. Migliorisi (2020) enfatizó que, en la actualidad, si analizamos cualquier Código Penal de argentina o de cualquier país podemos interpretar que la mayoría de los delitos pueden configurarse a través de medios informáticos, lo que ha cambiado es la modalidad de analizar y buscar la prueba o procesarla porque existen casos que están en la nube o se encuentran fuera de la jurisdicción.

El Dr. Rincón (2020) sostuvo que la gran deficiencia que enmarca la mayoría de países es la congestión judicial ante la inexistencia de Fiscalías y Juzgados Especializados en Ciberdelincuencia porque todos los casos se dirigen al mismo sitio y en consecuencia se genera lentitud en los procesos. Asimismo, la falta de preparación y de conocimiento específico sobre los temas de tecnología, el uso de acrónimos que son tan evidentes en temas de tecnología, trae como consecuencia que los jueces se encuentren sin mayor fundamentación, siendo la peor deficiencia de todas.

Particularmente el Dr. Maza (2020) sostuvo que el problema principal de los delitos informáticos es que los abogados, fiscales y jueces tienen una deficiencia relacionada al uso de las tecnologías. Es decir, hay mucho operador jurídico que tiene problemas para utilizar el programa Word o un procesador de textos similar, imagínense cuando se trata de hablar de pruebas digitales. Al final, los delitos informáticos o los delitos que se cometen en internet no son más que la versión 2.0 de cualquier delito. Por ejemplo, el acoso o las amenazas practicadas en entornos digitales. Desde mi punto de vista, el problema está en la carencia de información sobre el manejo de sistemas y la falta de conocimiento y de formación. Pienso que es más fácil que un ingeniero estudie derecho y no viceversa para comprender la complejidad tecnológica e informática de este delito.

Al respecto el Dr. Acurio (2020) mencionó que el problema está dado por una falta de capacitación de ¿cómo se debería investigar esta clase de delitos? En el caso de Ecuador, desde abril del 2002 se tipificaron los delitos informáticos. Se comenzó por reconocer la ventaja de la oralidad en el procedimiento inquisitivo y la aplicación del principio de inmediación. Ahora bien, la Policía Especializada en delitos Informáticos y Cibernéticos, así como la Policía Especializada en Informática Forense aprovechó el robustecimiento de conocimientos en esos temas, mientras que la Fiscalía y el Juzgado priorizaron otros aspectos. Debe recordarse que no se pretende transformar en conocedores absolutos a los administrados de justicia, sino que debe profundizarse el conocimiento con el que cuenta, ya que no es equiparable resolver un caso de robo y un fraude informático.

El Dr. Temperini (2020) afirmó que son muy pocas las Fiscalías Especializadas en Ciberdelincuencia. Solo cuentan con una en la ciudad de Buenos Aires, la deficiencia tiene que ver con los límites que encierran estos delitos porque se debe armar la estructura capacitando al personal. Sin embargo, quedará muy pequeña porque los recursos para investigar esta clase de delitos son muchos dado que no solo se necesitan fiscales, sino también personal policial especializado, laboratorios forenses que puedan revisar las pericias. En ese sentido, el modelo de tener fiscales especializados en distintas Fiscalías es lo más alcanzable y practicable.

2. ¿Qué opina sobre los fiscales que investigan y los jueces que imparten justicia en los casos de Ciberdelincuencia?

El Dr. Carretero (2020) sostuvo que en argentina se presenta a menudo muchos casos de nulidades de procesos por temas de la evidencia siempre que pasa por los elementos personales, es decir por derechos constitucionales como el derecho a la privacidad. En

ese sentido, la mayoría de estos delitos cuando se ingresa a los dispositivos digitales se debe considerar al momento de pericia de la evidencia y al mismo tiempo ser muy meticuloso de cómo se va a acreditar porque es ahí donde roza el derecho a la privacidad y la posibilidad de vulnerar otro derecho constitucional que de ser el caso pues automáticamente se produce la nulidad de los procesos.

Asimismo, el Dr. García (2020) refirió que en la fiscalía de Buenos Aires hay fiscales especializados en delitos conexos a trata de personas y delitos mal llamados de pornografía infantil que deberían llamase delitos de explotación sexual infantil y el delito de Grooming. Respecto a las fiscalías especializadas en ciberdelincuencia recién van a ser creadas y conformadas por un grupo de fiscales cono conocimientos investigativos avanzados en tecnología. Siendo ello así, los operadores de justicia requieren de capacitaciones y actualizaciones constantes, en la medida que el delito va mutando, así como las nuevas metodologías de ciberdelincuencia que utilizan los ciberdelincuentes para lograr eludir la acción de la justicia.

En esa línea de análisis, la Dra. Lamperti (2020) mencionó que principalmente se debe establecer como una necesidad la capacitación de esas personas que van a intervenir en el proceso judicial porque la evidencia del tratamiento digital tiene algunas características que difiere de la evidencia física que hace que se requiera de conocimientos específicos para atender las distintas cuestiones que se van dando en el tiempo. Asimismo, la autora enfatizó que no es lo mismo atender un homicidio o robo que posiblemente no tendrá evidencia digital, que atender un daño informático. Reiteró que eso dependerá del grado de conocimiento de los fiscales y jueces para la eficiente atención de los procesos judiciales en materia de ciberdelincuencia.

El Dr. Migliorisi (2020) dijo que en Buenos Aires funciona muy bien, es bastante ágil, el nivel de esclarecimiento de la prueba es muy alto. Sin embargo, en diversas fiscalías que no han invertido en tecnología tienen la deficiencia que sus procesos son más difíciles porque el ciberespacio es más complejo de analizar y de tomar una decisión. En ese sentido, hay jurisdicciones que decidieron apostar en lo referido a la prevención y al futuro estarán a la vanguardia por sobre otras provincias que decidieron invertir en otro tipo de políticas.

Aunado a esto Rincón (2020) desarrolló que el hecho más significativo por regla general es contar con fiscales especialistas o expertos en lo que están investigando y eso hace presumir que los fiscales tienen conocimiento de los delitos y conjuntamente de la

tecnología. Por esa razón, es importante que los fiscales aprendan y se fundamenten jurídicamente muy bien para efectos que su labor sea la de un aporte que contribuya a la mejor aplicación en la administración de justicia.

El Dr. Maza (2020) planteó que en las Fiscalías y los Juzgados se reparten los casos según la afinidad o interés que puedan tener, eso es muy bueno porque es mejor que los jueces que entienden delitos económicos sean los que normalmente los instruyan. Lo que sucede con España es que cada vez con cada reforma se van creando nuevos Juzgados Especializados. Asimismo, es cierto que se incrementa la cantidad de fiscales y jueces que se van formando en delitos económicos y ciberdelitos. El hecho de que un juez o un fiscal sea generalista no está mal, dado que hace más el que quiere que el que puede, entonces tener voluntad de esclarecer un hecho te motivará a estar con los mejores.

Además, el Dr. Acurio (2020) describió que la investigación en esta clase de delitos tiene un componente tecnológico, pues uno debe contar con conocimientos sobre el manejo de las plataformas en internet. Un ejemplo para aterrizar la idea es el siguiente: se realizó una transferencia electrónica de dinero proveniente de una cooperativa hacia una persona natural, en la que se presentó un supuesto fraude informático, porque se configuró el perjuicio patrimonial. Lo primero que tendría que hacer el fiscal es realizar la diligencia de pericia de los correos electrónicos de las cabeceras técnicas, porque estos se pueden rastrear. Entonces, el fiscal debe saber técnicas de investigación y contar con un plan de investigación para cada caso en concreto. Asimismo, el juez debe saber cuáles son los límites del debido proceso para evitar la vulneración de algún derecho fundamental, pero evidentemente demarcado en delitos informáticos.

El Dr. Temperini (2020) suscribió que conoce fiscales que son buenos en lo que hacen, pero la mayoría no están preparados para llevar adelante este tipo de investigaciones, siendo un problema que se estira a otros tantos delitos, porque en la actualidad la comisión de un delito de homicidio, robo, extorsión empiezan a aparecer elementos informáticos que exigen el conocimiento como si se llevará adelante una investigación de ciberdelincuencia. Esta especialidad es particular porque se exige demasiado al fiscal al conocer sobre medicina, evidencia digital, entre otros. Por ello, el fiscal debe contar con un cuerpo de profesionales expertos que lo terminen asesorando para evitar que recaiga todo en la misma persona. Caso contrario sucedería si se implementase Fiscalías dedicadas a determinados delitos y no que la misma atienda diversos casos.

3. ¿Por qué la mayoría de los casos de Ciberdelincuencia registrados en los últimos 5 años han sido archivados?

El Dr. Carretero (2020) afirmó que el tema pasa por la evidencia y reiteró la falta de capacitación técnica de los operadores de justicia. En argentina se está buscando promover cursos de cómo obtener la evidencia en materia de informática para evitar la vulneración de otros derechos con la obtención de la evidencia digital porque la mayoría pasa por ese lado que finalmente hacen caer los procesos. Asimismo, algunos casos también son archivados por corrupción, pero son temas ajenos a la presente investigación.

Mientras tanto el Dr. García (2020) definió que el 80 % de los fiscales y los demás operadores que coadyuban en el sistema no están capacitados en las áreas de ciberdelincuencia, cibercrimen y delitos informáticos. Actualmente, se evidencian casos en los que se interpone la denuncia para averiguar un paradero, un robo o un hurto, siempre tienen un tinte tecnológico. Para poder brindar una óptima atención, se requiere una capacitación multidisciplinaria, esto implica capacitar tanto a los fiscales referentes en la materia, así como aquellos fiscales ordinarios.

La Dra. Lamperti (2020) sostuvo que el problema es probatorio más que de otro tipo, puede ser de la autoría, quizá sí se adjuntó la prueba, pero no se puede hallar al responsable, entonces para que los casos sean ganables se debe custodiar y presentar adecuadamente las evidencias digitales a fin que los responsables puedan ser localizados en el menor tiempo posible.

En paralelo el Dr. Migliorisi (2020) propuso que existe mucha gente que no denuncia por miedo, desconocimiento o por descreimiento que la justicia va investigar de forma eficiente. Por otro lado, los delitos que sí se denuncian en diversos casos ocurren por producción de prueba. La falta de capacitación de los funcionarios, Fiscalías o Juzgados hace que un procedimiento ordinario demore meses y algunas veces la prueba es presentada oportunamente y en otros casos desconocen cómo llegar a ella o cómo solicitarla, motivos por las cuales se desestima la causa por falta de pruebas.

El Dr. Rincón (2020) mencionó el tema de la ambigüedad, ante la dificultad de precisar la tipicidad de la comisión de un delito informático contribuye a la realización de estas situaciones que ocasiona en el juez duda y por tanto considere que no hay suficiente mérito.

En consecuencia, las múltiples situaciones generen la obtención de sentencia beneficiaria para la persona que está encausada. Un claro ejemplo es aquella persona que clona una tarjeta, la misma que está cometiendo un delito de clonación de tarjetas, si bien es cierto cometió un delito, pero no de clonación porque eso no existe, sino el delito de violación de datos personales. Es ahí donde el juez presenta la dificultad de comprender la correcta terminología en ciberdelincuencia al no haber suficiente conocimiento para detectar y determinar los delitos informáticos de manera específica.

Similarmente, Maza (2020) sostuvo que desconoce el funcionamiento de la ley peruana, pero entiendo que no debe ser muy distinta a la ley procesal en España y en el resto del mundo. En esa línea, la parte denunciante debe demostrar como mínimo los indicios de la comisión delictiva. Habiendo realizado esa aclaración, desde mi opinión muchas veces se archivan, primero porque el abogado o el defensor público no sabe enfocar la defensa o acusación del caso, tampoco son capaces de asegurar la prueba porque el agraviado ha perdido el celular que contiene la prueba o se le rompió la pantalla. Al no asegurar la prueba digital o dirigir una pericial informática, el factor clave de la investigación no se completa, por lo que resulta lógico que nuestros fundamentos carezcan de suficiencia probatoria.

El Dr. Acurio (2020) refirió que el principal factor es el tema de la cooperación de la información. Es decir, si contásemos con esta en el país y fuese accesible se podría procesar al imputado sin ningún inconveniente. Diferente es el panorama si no se cuenta con la información y se necesita que un tercero la facilite. Por ello, considero que el archivamiento de los casos ha sido por la inoportuna y burocrática derivación de la información requerida. Pues no olvidemos que los delincuentes se encuentran en la mayoría de casos en otros países, dada la naturaleza transnacional de estos delitos.

El Dr. Temperini (2020) postuló que la mayoría de los casos de ciberdelincuencia han sido archivados porque el sistema no cuenta con los elementos adecuados para llevar adelante una investigación con un mínimo de eficacia. Asimismo, comenta que hay delitos que aún con todos los recursos dedicados no van a poder ser investigados porque la tecnología pone barreras al derecho que aún le cuesta reconocer. De acuerdo a los estudios realizados en el Observatorio de delitos informáticos de Latinoamérica señalan que 8 de cada 10 delitos no son investigados y forman parte de la cifra negra. La gente no denuncia porque no tiene expectativa que el sistema lleve adelante investigaciones con un mínimo de eficacia, la misma que no existe por diversos motivos, algunos son motivos

tecnológicos, la falta de recursos, la falta de interés del sistema porque la inversión económica que lleva investigar estos delitos informáticos, o sea la inversión del sistema procesal es tan grande que a veces no tiene rédito penal.

4. ¿Qué medidas debe adoptar el Estado argentino para una eficiente investigación y administración de justicia en los casos de Ciberdelincuencia?

El Dr. Carretero (2020) mencionó que es importante y necesario que todos los Estados cuenten con Tribunales Especializados. Actualmente en Argentina existe la Fuerza de Seguridad Especializada en Ciberdelitos que actúa en forma complementaria con los operadores de justicia para tener acceso a la información, así también el personal de la Fuerza de Seguridad debe ser constantemente capacitado en derecho dado que en el instante en que se tenga la evidencia no se vulnere ningún derecho constitucional y el proceso se venga abajo.

Sucede lo mismo en caso de los operadores de justicia, porque tienen el pleno conocimiento en derecho, pero técnicamente no saben lo que es un hashing, manejar un móvil, desconocen el punto de pericia que se tiene que solicitar para no violentar otros derechos, ignoran quién es el encargado de abrir uno de los dispositivos, que se debe investigar dentro de los aparatos tecnológicos y como debe llevarse a cabo ese procedimiento.

Asimismo, el Dr. Garcia (2020) sostuvo que uno de los aspectos más resaltantes es la cooperación nacional e internacional según los proscrito por la convención de Budapest, también se debe respetar la legislación vigente y de ser necesario realizar reformas procesales en los códigos para investigar de manera clara los delitos que van evolucionando, poder concretar allanamientos remotos, pericias en los lugares de los hechos, evitando la vulneración de las garantías constitucionales. No se debe olvidar que en la actualidad la comisión de estos delitos trasciende la jurisdicción de los fiscales intervinientes y por ello se requiere la cooperación inmediata para sacar adelante este tipo de investigaciones complejas.

La Dra. Lamperti (2020) enfatizó que el Estado argentino sobre todo tiene que proporcionar herramientas para la investigación, como establecer un orden o jerarquía dentro de cada organismo, no solo en la ciudad sino también en cada uno de los Estados Provinciales autónomos. Asimismo, cada Estado debe promulgar leyes que establezcan la necesidad de contar con Fiscalías Especializadas para el tratamiento de casos que

ameriten estos temas. Los operadores del derecho deben contar con capacitaciones sobre temas de ciberdelincuencia por la vinculación a la evidencia digital. A su vez, el Estado debe brindar herramientas para la atención de casos como por ejemplo la conexión a internet 24/7 en las oficinas con el propósito de coadyuvar con la investigación en los casos de ciberdelincuencia.

Además, el Dr. Migliorisi (2020) describió que en la actualidad no existe fronteras entre las provincias y países, considera que el nivel de inversión y capacitación del Poder Judicial tiene que ser parejo en todas las jurisdicciones, es decir se debe contar con una base sólida y a raíz de eso empezar a construir el manejo amplio de la ciberdelincuencia al observar casos interprovinciales donde el delito se comete en un lugar y los efectos en otro.

Por esa razón, es necesario que ambas provincias y Poderes Judiciales tengan el mismo nivel de infraestructura para dotar del caso. Asimismo, conocer los delitos transnacionales, en caso una persona puede cometer un ilícito, amenaza, extorsión en Buenos Aires a un ciudadano que se ubica en Lima, supuesto que necesitará una coordinación a nivel probatorio, judicial con la celeridad que en estos tiempos requieren las altas tecnologías.

El Dr. Rincón (2020) consideró tres aspectos importantes siendo el primero, la existencia de una intercomunicación de orden internacional a través de convenios con autoridades mundiales que luchen contra los delitos informáticos a fin de establecer marcos jurídicos colaborativos entre pares institucionales.

El segundo aspecto es la permanente actualización y capacitación a los jueces porque son quienes cuentan con un nivel de información muy importante y a su vez las modalidades de estos delitos están cambiando progresivamente, razón por la que se exige que los jueces deben estar a la vanguardia de la tecnología y de esta forma se logre la comprensión de la problemática actual.

El tercer aspecto está relacionado a la función del Estado porque a través de los Ministerios deben exigir que los currículos académicos de los programas de formación en derecho o ciencias jurídicas en general, deben tener un contenido significativo en este entorno porque cuando estas personas lleguen a los órganos de la Administración de Justicia tengan una debida fundamentación en temas de ciberdelincuencia y manejo de la Tecnología.

De manera similar, el Dr. Maza (2020) comentó que son varios parámetros los que hay que tener en cuenta empezando por la protección de los datos personales que sigue siendo una asignatura pendiente para toda Latinoamérica. Por ejemplo, si pongo una página web en la que debo asegurar los datos personales de los usuarios y no se hace nada de lo que ellos no hayan consentido, nos obligan como empresa a controlar los procesos y saber con quién se trabaja. Lo que permite tener un control de los datos de navegación, de dónde vienen las IP y las conexiones de los servidores. Por eso, cuando se obliga a ser más proteccionista con los derechos de las personas, al final se genera un control sobre el tráfico web y concientizas a los usuarios a generar este sistema preventivo de seguridad. Lo segundo sería invertir en equipos y expertos en sistemas que el Estado a menudo no suele asumir porque cuenta con recursos limitados.

El Dr. Acurio (2020) refirió que debemos partir de una política pública de Estado que pueda aterrizarse en la Administración de Justicia y en el Ministerio Público. Al formar parte del Convenio del Cibercrimen se cuenta con mayores posibilidades en cuanto a inmediatez para obtener la cooperación internacional. A su vez, explotar la ventaja de la virtualidad para capacitarse frecuentemente. Adicionalmente, se recomienda intercambiar experiencias en congresos u otros eventos similares por su consecuencia enriquecedora y sumamente aprovechable. Finalmente, no debe olvidarse que es un trabajo conjunto, por lo que es necesario que se implementen en las universidades y los colegios instrucción general sobre casos de ciberdelincuencia.

El Dr. Temperini (2020) señaló que es necesario contar con fiscales que entiendan cuáles son las medidas de investigación a practicarse, siempre con respeto a las garantías constitucionales porque en la actualidad se evidencia a jueces y fiscales que autorizan medidas que en diversos casos afectan muchos derechos, también se necesitan equipamientos y recursos porque de nada sirve tomar buenas medidas desde el punto de vista legal para que después se tenga en la práctica un dispositivo digital y demore 6 meses un dictamen pericial de laboratorio. Asimismo, el fortalecimiento de la parte procesal para asegurar las medidas por parte de los fiscales, jueces y abogados de la defensa que se sepa que están autorizando medidas que el Derecho prevé y que no están siendo inventadas en el camino. A su vez, es necesario contar con normativa que obligue a las empresas privadas a tener un mínimo de cooperación internacional para lograr una eficiente justicia.

OE_1: Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

5. ¿Qué se ha logrado con la incorporación de las Fiscalías Especializadas en Ciberdelincuencia?

El Dr. Carretero (2020) mencionó que se ha logrado encausar los procesos, a pesar de la ausencia en las capacitaciones, por lo menos han empezado a especializarse en temas técnicos y todo el tratamiento que conlleva esta clase de delitos al ser completamente diferente al manejo de un proceso normal o tradicional, considerando la complejidad de los casos de ciberdelincuencia por la realización y análisis en un entorno virtual.

A su vez, el Dr. García (2020) abordó que dentro de los logros más importantes destaca la forma en que se ejecutan las investigaciones más complejas debido a su trascendencia espacial y que los denunciantes reciban una mejor atención debido a los protocolos incorporados, evitando así que sean revictimizados. Un ejemplo plausible sería que la víctima que lleva su celular con contenido sexual para ser utilizado como material probatorio, este no sea impreso, para evitar su distribución. Con esto se logra no revictimizar a la víctima. La conformación de un grupo de peritos especializados en la materia, permite que se realicen preguntas concretas a las víctimas y sus familiares, relacionadas a la prueba digital, la preservación de la prueba, la cadena de custodia, todas cuestiones derivadas de este tipo de problemáticas.

La Dra. Lamperti (2020) comentó que se ha logrado diversas cosas; primero, esclarecer las diferencias entre la evidencia física y digital, el tratamiento y la forma en la que se puede llegar a los casos exitosos. Al hacer foco en cuestiones específicas lo que se necesita también es una cantidad de información que permita tomar cursos de acción, así como contar con estadísticas a fin de ver que casos deben ser atendidos con mayor celeridad y dónde suceden con mayor frecuencia para brindar una atención oportuna y eficaz.

Aunado a lo anterior, el Dr. Migliorisi (2020) definió que hasta la fecha Buenos Aires ha logrado que la gente sepa donde hacer las denuncias al momento. Sin embargo, el personal de atención o encargado debe ser un conocedor sobre la prueba, el mismo que pueda explicarle de forma clara que puede ser considerado como prueba en el proceso, datos específicos que son claves para la investigación. El autor ha visto casos donde la gente va a denunciar a una comisaría o a un Juzgado donde no tienen esa experiencia, y

lastimosamente detiene el ingreso a una investigación que podría ser exitosa. Por otro lado, la concientización ha ayudado a la prevención de delitos informáticos.

El Dr. Rincón (2020) señaló que se lograría la eficacia en la Administración de Justicia, siendo el aporte más significativo de implementar estas Fiscalías Especializadas. Esa variedad o dinámica que tienen los ciberdelincuentes genera que las autoridades puedan trabajar en conjunto y de esta manera obtener los Sistemas de Administración de Justicia más eficaces sobre todo para los delitos de mayor complejidad.

Asimismo, el Dr. Maza (2020) comentó que se obtendría agilidad y precisión para la atención de los delitos informáticos. Teniendo en consideración que los rastros son muy escuetos y las evidencias no es que desaparezcan, pero cuando más tiempo pase, la obtención de la información puede ser obstaculizada o entorpecida. Situación distinta se presentaría con un órgano especializado que pueda investigar y recabar elementos de una forma segura para poder utilizarlos dentro de un debido proceso.

El Dr. Acurio (2020) suscribió que se lograría la especialización de los fiscales, pero se debe tener en cuenta que no es tan sencillo como parece porque tendrán que hacer una carrera tanto en la fiscalía como en el órgano jurisdiccional. Está claro que no sirve formar y preparar a profesionales y después empezar a rotarlos. Ahora con eso no quiero decir que no habrá rotación entre los fiscales, sino todo lo contrario, habría una rotación en la misma unidad. Por ejemplo, un fiscal que investiga casos de pornografía infantil, puede verse afectado a corto plazo. En ese supuesto, se realizará la rotación del personal especializado, pero en la misma unidad especializada, esto es, ya no vas a ver el delito antes mencionado, sino delitos de fraude informático para asegurar la objetividad y el equilibrio mental del colaborador.

El Dr. Temperini (2020) sostuvo que se ha logrado mayor visibilización de este tipo de problemáticas porque el hecho que exista una Fiscalía Especializada significa que el problema tiene una gravedad que merece contar con personal capacitado para eso. Asimismo, brinda mayor posibilidad de cooperación porque al contar con dicha Fiscalía en donde todos hablen el mismo idioma hace que el personal logre un mejor entendimiento con otras Fiscalías de otros países con mayor grado de cooperación. La UFECI atiende casos de ciberdelincuencia, pero solo en la ciudad de Buenos Aires y para determinados delitos, siendo un problema actual para el resto de Argentina.

6. ¿En su opinión ante el aumento de los delitos informáticos cómo ha sido la respuesta de las Fiscalías Especializadas en Ciberdelincuencia?

El Dr. Carretero (2020) mencionó que según su experiencia las Fiscalías están atestadas de causas porque se ha presenciado diversos casos de ciberdelincuencia de naturaleza doméstico, o sea, casos de fishing, suplantación de identidad, acoso a menores por redes, delitos que han sido recientemente incorporados.

Asimismo, los delitos en materia comercial sobre todo en las empresas, antes de la crisis sanitaria, no consideraban relevantes temas relacionados a la Ciberseguridad porque la mayoría de las operaciones se realizaban en un entorno real, ajeno a la virtualidad, cuestión que se transformó de un día para otro. Razón por el que, se ha visto una gran cantidad de casos en las pocas Fiscalías existentes y la respuesta de los operadores es atender la mayor cantidad de casos en lo posible, a su vez tratan de responder según sus posibilidades y con los recursos y conocimientos que poseen.

Asimismo, el Dr. García (2020) detalló que el problema se intensificó con la llegada de la pandemia porque desde el punto de vista de la criminología hay dos cuestiones importantes a considerar, estos son el aumento desmedido de los casos y la adicción de las personas a distintas plataformas y video juegos. La respuesta para afrontar estos problemas implicó mayor esfuerzo de los colaboradores y operadores de la ley. Lo cierto es que no solo se han presentado denuncias clásicas que provienen de una comisaría, un correo electrónico o una plataforma tradicional, sino que esto derivó en denuncias a través de plataforma de vídeo juegos o streaming, tales como Fornite o Zoom. Por eso, es muy importante la capacitación y actualización permanente del lado de la justicia, así como de los encargados de cumplir la ley en el Poder Ejecutivo.

Adicionalmente, Lamperti (2020) refirió que específicamente se ha intervenido muchos casos de grooming, la distribución de imágenes de abuso sexual infantil y la respuesta de las autorizadas ha sido eficiente. Aún queda pendiente múltiples desafíos por la carencia de Fiscalías y Juzgados Especializados en Ciberdelincuencia.

El Dr. Migliorisi (2020) sostuvo que bajo su perspectiva las autoridades competentes desempeñan correctamente sus funciones porque cuentan con las herramientas para hacerlo en los delitos que les competen. Asimismo, precisó que el hostigamiento no es un delito sino una contravención en la ciudad, permitiendo que las víctimas solo puedan denunciar siempre que el hecho ocurra dentro de la misma ciudad.

Por lo tanto, lo que ha demostrado la Fiscalía es la excelencia del trabajo, tomar la denuncia, investigar y gracias a los convenios que se tienen a nivel internacional se puede esclarecer muchos casos. En otras palabras, la celeridad y el marco probatorio son claves para el desarrollo en los casos de ciberdelincuencia.

Así también Rincón (2020) argumentó que la respuesta ha sido en relación a la imagen y eficacia que puedan ver las personas porque si uno observa un sistema de justicia eficaz la gente se sentirá más tranquila, así cuando uno no confía en la administración de justicia, la sociedad siempre estará al asecho, pasa cuando la gente confía en los operadores de justicia se convierte en algo significativo porque el hecho que los demás países implementen este sistema mejorará la eficacia de la Administración de justicia relacionados a los delitos informáticos.

El Dr. Maza (2020) enfatizó que en España se cuenta con el Ministerio Fiscal, quien se encarga de formar a personal en delitos informáticos desde el año 2015 que se realizó la reforma del Código Penal con la inclusión de estos delitos, pude apreciar que la respuesta fue muy buena en cuanto a colaboración. Sobre todo, con lo casos que han sido iniciados de oficio por la Fiscalía, las fuerzas y cuerpo de seguridad del Estado tienen mucha efectividad, por lo que en reiteradas ocasiones los imputados no tienen otra alternativa más que negociar las conformidades y demás. Los datos que se pueden obtener de estos delitos son tan amplios que podíamos identificar la dirección de una persona, el número de teléfono desde donde se cometió el delito, entre otros.

Aunado a ello, el Dr. Acurio (2020) reveló que se evidencian problemas con el recurso humano, dicho en otras palabras, no hay peritos en informática forense que manejen aspectos indispensables en la investigación, tales como administración de redes, bases de datos, sistemas operativos, lenguajes de programación, entre otros. Una solución inmediata puede ser que se solicite al Colegio de Abogados la iniciativa de capacitaciones sobre estos temas, porque recordemos que alrededor del mundo hay excelentes profesionales con la experticia necesaria para instruir sobre el tema. Siempre he pensado que «el conocimiento que no se moviliza, simplemente no es conocimiento».

El Dr. Temperini (2020) mencionó que se han realizado campañas de prevención en caso de phishing, grooming porque es muy importante que los fiscales especializados salgan a las calles y cuenten a los ciudadanos de a pie las consecuencias del uso de la internet, por mencionar algún ejemplo, las estafas. Asimismo, considera que, ante el crecimiento de los casos, las Fiscalías Especializadas o fiscales visibilicen casos de éxito en los medios

de comunicación para que la gente tenga al menos la sensación de que si hace una denuncia hay posibilidades de llevar adelante una investigación. A su vez, indica que existe una cifra negra en estos casos de ciberdelincuencia y entre el ranking del ¿por qué las personas que no denuncian? Está el sentirse culpables del delito que sucedió y hay una que se relaciona con que la víctima no está pensando que el delincuente reciba su sanción, sino solo en resarcir o reestablecer lo que se perdió.

7. ¿Por qué es necesario que los fiscales cuenten con conocimientos en derecho y en tecnología para detectar, individualizar y perseguir los casos de Ciberdelincuencia?

El Dr. Carretero (2020) mencionó que se tiene un lenguaje diferente y poder comprender e identificar una encriptación de datos es complejo más aún que casos que versan sobre un lenguaje técnico en la forma de delinquir, porque no es lo mismo un acoso callejero que un acoso virtual a través de una red, el lenguaje de hash, email, WhatsApp o realizadas mediante otras redes.

Por eso la necesidad de capacitar y dominar sobre temas básicos para la realización eficiente de sus funciones es la clave de la ciberdelincuencia. En ese sentido, la exigencia de conocimientos y capacitación debe ser igualitaria para los profesionales como por ejemplo en los casos de homicidio o violación, el fiscal debe saber al menos lo básico de medicina porque entiende como se asesinó a una persona o como empuñó el arma y la dirección de la bala, entre otros. De igual forma, debe suceder en los fiscales que investigan casos relacionados a ciberdelincuencia.

Asimismo, el Dr. García (2020) refirió que es fundamental conocer sobre esos temas, puedo responder la pregunta con un ejemplo, si en la actualidad viene una persona a denunciar el delito que sea en donde el presunto imputado se encuentre en alguna red social, tales como Facebook, Instagram, WhatsApp o Twitter, lo primero que se debe hacer es la preservación de esa evidencia digital, esto es, conservar la cuenta para posteriormente solicitar los requerimientos nacionales o internacionales según corresponda.

Para ello, es básico y necesario que el fiscal y su grupo de trabajo cuenten con conocimientos para preservar la prueba desde su despacho o el lugar en el que se encuentre. Como pueden darse cuenta, este paso que parece sencillo, resulta primordial para avanzar con la investigación. Por consiguiente, es imprescindible el conocimiento

en derecho y tecnología para este tipo de delitos y el que no se adecúe a este nuevo paradigma de investigación generará retrasos en la administración de justicia.

La Dra. Lamperti (2020) sugirió que la importancia en la que se relaciona la informática y el derecho consiste en saber o comprender como funciona el aspecto técnico, por ejemplo, uno entiende bien la biopsia porque viene un médico legista y explica el informe, pero en caso de la informática esta atraviesa todo el proceso, entonces entender que es una IP, dónde se puede ubicarlo, ostenta mayor complejidad que la comisión de un delito tradicional.

Asimismo, toma un mayor tiempo para la investigación y localización del responsable por efectuarse en un espacio técnico. Por estos motivos, el abogado no solo debe saber de leyes y normativa, el abogado especialista en delitos informáticos debe tener el pleno conocimiento de cómo funcionan los medios informáticos. El otro tema importante es conocer más allá, es decir salir de la zona de confort porque en la realidad existen abogados que se niegan a comprender algo adicional o que tomará más pasos conseguirlo, por ello todo dependerá del entusiasmo y predisposición de quienes verdaderamente quieren aprender sobre estos temas.

Adicionalmente, el Dr. Migliorisi (2020) aludió que el concepto de cibercrimen está ligado directamente con el Derecho Penal y es fundamental que el profesional se capacite porque el criminal en cierta forma le es más rentable y menos riesgoso operar desde internet que hacerlo de forma física, mediante la comisión de ciertos delitos como la estafa, extorción e inclusive relacionado al secuestro, es decir, los delincuentes exigen monedas virtuales como pago del rescate, entre otros.

A su vez, el profesional quién acompañará a la víctima a instar la acción debe ser uno capacitado en la materia porque a decir verdad si la víctima no es acompañada por un profesional es poco probable que el caso llegue a buen puerto, salvo que sea una cuestión realmente grave. Por esa razón, es importante q los funcionarios también se capaciten para estar a la vanguardia y poder hablar un mismo idioma.

El Dr. Rincón (2020) consideró que todas las carreras deben aprender sobre tecnología, una vez que salió dicha rama todos los profesionales tuvieron que adaptarse al uso de la tecnología y los que manejaban la tecnología eran los que delineaban el desarrollo del mismo. Esto debe ser un acto voluntario y no obligatorio, más aún si la mayoría de profesionales aprendieron temas de tecnología por necesidad, pero no se está viendo el

tema de forma contraria, es decir los tecnólogos tiene un concepto de forma errada y sostienen que los temas jurídicos no son importantes. Así como los demás profesionales han adquirido el conocimiento en las áreas de tecnología, debo señalar que el Derecho también tiene implicancia en todas partes y en consecuencia es responsabilidad de todas las personas que son fiscales tengan conocimientos básicos en el tema para el desarrollo de su actividad.

De manera similar, el Dr. Maza (2020) planteó que es algo muy evidente y necesario, pues imaginemos que debemos valora un informe pericial de 100 folios en los cuales se está desgranando y detallando el funcionamiento de una red de intercambio de archivos o servidor para saber cómo ha sido manipulada. Un ejemplo sería que todos sabemos cuándo un constructor hizo bien o mal una casa, porque diferenciamos una pared bien o mal hecha. En síntesis, cuando nos familiarizamos con algo sabemos decidir entre los factores que la componen. Es medular cuanto más conocimiento se tenga sobre el manejo de internet y sus sistemas para valorar mejor el camino que eligió el criminal.

El Dr. Acurio (2020) agregó que es una de las competencias que nuestra realidad actual exige. Lamentablemente, la pandemia forzadamente nos obligó a adaptarnos. Los abogados particulares y los que trabajan en el sector público tienen que empezar a pensar en el futuro, sobre algunos temas relevantes como el blockchain, bitcoins, ransomeware, entre otros. Esto ya dejó de ser una alternativa, puesto que ahora es una necesidad. La tecnología es neutra, quien la utiliza la convertirá en buena o mala. Por eso, los cibercrímenes tienen una mayor lesividad al ser pluriofensivos porque no solo afectan a un bien jurídico protegido, a eso se le debe agregar los efectos multiplicadores del internet. Por eso, la ciberseguridad debe ser una cultura general de cada individuo. Tenemos que pasar a una justicia virtual, diferente a la que tenemos actualmente porque solo se adaptó el modelo tradicional vigente.

El Dr. Temperini (2020) postuló que es crucial que el fiscal tenga conocimiento en tecnología sino no va saber qué perseguir o qué ocurrió. En ese sentido, un especialista en seguridad de la información para que pueda recomendar debe entender cómo se hacen los ataques, bajo esa lógica difícilmente un fiscal podrá llevar adelante una investigación exitosa sino entiende de tecnología. Asimismo, la relación continua del abogado e informático debe ser la idónea en cuanto al manejo de información porque el informático ve que el abogado no sabe de informática rápidamente se pone en una postura de no cooperación porque se da cuenta que no se le pregunta con conocimiento. Entonces es

importante que los fiscales tengan conocimiento y entiendan todas las maniobras que se presentan para engañar al Sistema Financiero.

8. ¿Cuáles son las ventajas y desventajas de incorporar Fiscalías Especializadas en Ciberdelincuencia?

El Dr. Carretero (2020) señaló que la ventaja es que mediante la práctica van a especializarse, capacitando en manejar este tipo de lenguaje y técnicas. La desventaja es la poca cantidad de Fiscalías Especializadas en Ciberdelincuencia implementadas en Argentina y que lamentablemente todos los casos de ciberdelincuencia serán atendidos por estas dos Fiscalías. En ese sentido, la escasez de Fiscalías Especializadas es un problema actual en todo el territorio argentino. Por lo mismo, considero que es necesario implementar más Fiscalías Especializadas dada la complejidad de los delitos informáticos, los mismos que van mutando progresivamente con nuevas técnicas porque a medida que uno va descubriendo la forma de delinquir, los delincuentes también van descubriendo nuevos procederes para evitar ser descubiertos por los especialistas en ciberdelincuencia.

Asimismo, el Dr. García (2020) comentó que como parte de las ventajas obtenidas podemos ubicar sin duda alguna a la celeridad con la que se desarrollan los procesos, la aplicación de un óptimo procedimiento en cuanto a la cadena de custodia, conservación de la prueba, atención de las víctimas y un mejor trabajo interdisciplinario para afrontar esta tarea. Sin embargo, también se identifican desventajas como la falta de recurso humano y analistas forenses especializados que trabajen con el software «Universal Forensic Extraction Device» – UFED, cuya traducción en español es Dispositivo Universal de Extracción Forense para dispositivos móviles.

La Dra. Lamperti (2020) sostuvo que las ventajas consisten en un mejor tratamiento a la evidencia digital, una mejor respuesta a las víctimas que también están buscando o esperando tener un apoyo adecuado a su conflicto porque si un equipo verdaderamente está abocado a la resolución de casos similares, seguimiento de patrones, modalidades que se repiten o se encuentra en los mismos grupos que son reincidentes en estos delitos, la posibilidad de éxito es más alta que los casos que están dispersos o aislados.

Algunas veces los casos que son aislados se tienen que archivar porque aparentemente no hay pistas para la localización del responsable, en cambio sí se procede a unificar 3 o 4 casos que son similares o que tienen algo en común por la información entrecruzada hace

que se llegue a identificar a las bandas organizadas de gran magnitud, la misma que se logra cuando se tiene la información concentrada en una Fiscalía Especializada en Ciberdelincuencia.

La desventaja es que justamente por contar con una Fiscalía Especializada los demás no se preocupan en capacitarse y ante cualquier delito que implica una mediación tecnológica tenga que ser trasladado a una Fiscalía que está investigando a una banda dedicada a la clonación de tarjetas de crédito. Bajo esa lógica las Fiscalías van a ser especializadas o divididas en la medida que se dediquen a algo muy concreto o específico y al mismo tiempo el resto de Fiscalías se capaciten sin perjuicio a ello sobre todo lo relacionado a evidencia digital.

Adicionalmente, el Dr. Migliorisi (2020) postuló que la Ciudad de Buenos considera es muy importante por el avance en el cibercrimen desde la creación de hace 12 años de Fiscalías Especializadas. Era evidente el cambio de delitos tradicionales a ciberdelitos, entonces es fundamental que ese proceso se haga con tiempo para que poco a poco inicien con la especialización a funcionarios, se cree tecnología, se implemente laboratorios de forense, peritos especializados porque previo a la investigación surgen diversas actuaciones relacionadas a la intervención de dispositivos electrónicos. Por ello, es necesario que se cuente con la preparación de laboratorios, funcionarios y la justicia en la atención de esta clase de delitos, porque de lo contrario, poco o nada se hará para combatir los casos en ciberdelincuencia.

El Dr. Rincón (2020) abordó que la ventaja más importante es buscar que la Administración de Justicia sea más eficaz, efectiva y oportuna porque pueden ser impregnados por corrupción y cuando las personas pierden la confianza en la justicia se pierde lo más importante en una sociedad.

Existen situaciones que dan que pensar en la Administración de Justicia como por ejemplo una vez intervenido y capturado al sujeto, lo liberan muy pronto o las decisiones no corresponden al delito que se cometió, siendo situaciones absolutamente graves. Entonces la mayor ventaja de implementar Fiscalías Especializadas es la eficacia de la justicia para que las personas perciban los aspectos positivos en la mayoría de países.

En cuanto a la desventaja, pero llamémoslo dificultad son los costos que pueden implicar la implementación de las Fiscalías y Juzgados, nuevos funcionarios y como es evidente

sería muy costoso, pero no lo vean como desventaja sino como dificultad, pero si se está dispuesto a implementar se debe considerar estos puntos.

Además, el Dr. Maza (2020) manifestó que se lograría mayor efectividad en la persecución del crimen porque no solo se investigarán hechos que culminarán en condena si efectivamente hubo un delito, sino que se puede prevenir la comisión de estos. Considerando que, a mayor efectividad de la justicia, mayor efecto del código penal de un país. Entonces, la ventaja es que se reduciría la criminalidad por disuasión, los criminales al saber que el enemigo cuenta con mejor preparación y equipamiento, lógicamente los intimidaría.

Por otro lado, la desventaja es el mismo tema visto al revés, si se observa que las autoridades no cuentan con los recursos para perseguir estos delitos, fomenta que sigamos potenciando nuestras herramientas tecnológicas delictivas e indagando en cómo se pueden cometer delitos informáticos. Se tienen que respetar los principios del derecho penal, generar seguridad jurídica al ciudadano o residente con la misma exigencia que se aplica a otras plataformas como Amazon, Facebook y Netflix.

El Dr. Acurio (2020) sostuvo que una de las ventajas es contar con un grupo especializado que permita ser más efectivo en la investigación de esta clase de delitos, también se debe implementar un plan de renovación para que cada cierto tiempo las personas que estén dentro de la unidad puedan trasladar sus conocimientos a través de las escuelas judiciales, escuela de fiscales y así ese conocimiento se masifique en la sociedad. Más que una Fiscalía Especializada se debe tener una Unidad de Colaboración para que coadyuve a la realización de las Fiscalías Especializadas. Estos datos son parte de un Plan que responde a una estrategia nacional de combate a la ciberdelincuencia, puesto que toda iniciativa no debe ser para mitigar el delito (ex post) sino todo lo contrario, se debe buscar prevenir la comisión de estos delitos (ex ante).

El Dr. Temperini (2020) manifestó que una de las ventajas es que la gente se anime a denunciar más porque uno de los grandes problemas del por qué la gente no denuncia es porque no saben a dónde ir o en las páginas de ayuda brindan teléfonos que no contesta nadie o al momento que uno va a una comisaría o a un lugar de centro de denuncias las personas que te reciben no están capacitados para recibirlas, otro punto importante es ante la llegada de la víctima a una comisaría, el policía suele revictimizar o plantea preguntas desatinas o en el peor de los casos señala a la víctima que este caso no es un delito cuando él no es indicado para hacerlo y entre otras cosas. Otra ventaja de contar con fiscalías

especializadas es que reciben denuncias online siendo importante porque permite a las victimas tener confianza a denunciar y contar con mayor libertad lo ocurrido sin temor a que te juzguen a planteen preguntas desatinadas, todo lo mencionado anteriormente son ventajas para la sociedad.

9. ¿Qué aspectos cree usted que pueden ser emulados por los países de Sudamérica en base a la experiencia de Argentina con la incorporación de Fiscalías Especializadas en Ciberdelincuencia?

El Dr. Carretero (2020) indicó que existen convenios que contienen protocolos de ayuda entre los países de Sudamérica. Asimismo, durante el 2020 fue designado para intercambiar experiencias con personas de Perú y tomar de la legislación peruana aspectos que argentina carece y viceversa, este intercambio de información es algo nuevo y reciente, pero mediante esta forma de intercambiar información sabremos a ciencia cierta como es el tratamiento de estos delitos en diferentes países. Asimismo, el convenio de Budapest no soluciona mucho porque con la vigencia del convenio lo que está haciendo es que los países se comprometan a modificar sus normativas jurídicas internas a diferencia de la Convención de Ministros de Justicia de los Países Iberoamericanos en el que, los países se comprometen a prestar asistencia en caso se presenten hechos ligados a ciberdelincuencia a nivel internacional.

Adicionalmente, el Dr. García (2020) aludió que lo más importante es que puedan realizar procesos de trabajo automatizados. En Argentina se ha logrado implementar estos programas a la hora de ejecutar una investigación. En caso se necesite obtener los registros de conexiones IP a distintas plataformas, ¿cómo las procesamos? Contamos con la herramienta para copiar y pegar, y lograr la automatización ese proceso. Debemos tener en cuenta que todas las conexiones que vienen de otros países contienen unos horarios en Coordinated Universal Time - UTC, por lo cual hay que restarle tres horas, eso que se hacía antes en una plantilla Excel, ahora se realiza a través de un programa que sistematiza todo ello, generando un reporte que permite ahorrar muchas horas de trabajo.

Asimismo, la Dra. Lamperti (2020) postuló que contar con Fiscalías Especializadas y requerir que se brinden recursos de capacitación, tecnológicos para atender la alta demanda debe estar ligado a contar con personal adecuado, caso contrario será muy difícil que sin herramientas se llegue lejos. Por eso es necesario las capacitaciones y algo muy importante en temas de redes es contar con internet las 24/7, las mismas que son redes de cooperación internacional porque en la actualidad existen bandas que migran de un lugar

a otro. Por lo tanto, la necesidad de una buena conexión de internet y la concentración de información de todo América permitirá que la mayoría conozca temas relevantes sobre los delitos informáticos.

El Dr. Migliorisi (2020) precisó que la coordinación a nivel internacional es fundamental porque el ciberespacio ha cambiado el concepto del Derecho y de las Telecomunicaciones. Asimismo, ha potenciado la libertad de expresión. Por ello, es imprescindible que todos los países tengan Fiscalías Especializadas, las mismas que estén coordinadas entre sí porque es un universo paralelo que conecta de forma permanente dejando de ser un delito transnacional común.

De manera similar, el Dr. Rincón (2020) afirmó que argentina ha marcado a nivel de nuestra región Sudamericana un liderazgo en el desarrollo en Tecnología y Derecho Informático y viendo en un plano internacional los referentes son muy importantes. El hecho de mirar u observar cómo argentina ha implementado este sistema debe constituirse aporte de información para los demás países, a su vez aquellas deficiencias en la implementación, los países pueden investigar y evitar incurrir en esos desaciertos y poder hacer un proceso mucho menos traumático en cada uno de los países.

El Dr. Maza (2020) sostuvo que en general, sería reforzar la comunicación entre las autoridades para poder pedir colaboración en la investigación pues es muy difícil y se aletarga el proceso. Dotar de recursos humanos y logísticos, los mismos colaboradores van a generar ese cambio e innovación y se convertirán en el motor que refuerce los puntos débiles. Siempre debe procurarse avanzar, sin importar el ritmo.

Asimismo, el Dr. Acurio (2020) abordó que lo más importante es la cooperación internacional, el hecho que se pueda implementar Fiscalías, Juzgados y Policías Especializadas es un tema de cooperación, es decir generar puntos de contactos a nivel internacional dada la naturaleza de estos delitos informáticos. En ese sentido, una vez se logre dicha cooperación también debe implementarse reuniones para conocerse, el hecho de intercambiar información y generar protocolos de actuación en base a los diferentes tipos penales reconocidos en el convenio, los mismos que deben ser adaptados por cada legislación nacional. Por lo tanto, la idea crucial es homologar la tipología de la ciberdelincuencia a fin de evitar lagunas o vacíos legales en beneficio de los delincuentes y a su vez realizar reformas considerando que el Convenio de Cibercrimen es de 2001.

El Dr. Temperini (2020) recomendó que debe ser emulado el hecho de poder mostrar a la sociedad que el Sistema se encuentra medianamente preparado, si uno tiene la estructura armada brinda mayor grado de confianza para la víctima, entonces ante el estado de indefensión que siente va a tener mayor expectativa de denunciar porque sabe que esa Fiscalía cuenta con personas que van a entenderla y velar por sus intereses.

OE_2: Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

10. ¿Qué opina sobre la Administración de Justicia no Especializada en Sudamérica para los casos de Ciberdelincuencia?

El Dr. Carretero (2020) refirió que la exigencia de contar con conocimientos tecnológicos no solo debe ser hacia los fiscales sino también para los jueces y el personal encargado de analizar estos temas. Es necesario que los jueces estén capacitados por las complejas características de estos delitos, así como los jueces están capacitados para ver algunos aspectos en caso de los delitos de homicidio, más aún se debe exigir el dominio y constante capacitación para los delitos informáticos. De lo contrario, no tendría sentido incorporar Fiscalías y no Juzgados Especializados porque finalmente son ellos quienes tendrán la última palabra y decisión dentro de un proceso judicial.

A su vez, el Dr. García (2020) abordó que en estos casos podemos comentar que se presentan problemas para llegar a juicio en un tiempo razonable y conseguir una satisfacción para la víctima. Siendo muy objetivos las actuales fiscalías ordinarias no están capacitadas para asumir esta clase de investigaciones, lo que finalmente se hace es derivar la investigación al personal policial, el cual se encuentra sobrecargado de trabajo. Por esas consideraciones es muy importante que se fomente la creación de Fiscalías Especializadas en Ciberdelincuencia que se dediquen a este tipo de tareas y que puedan representar la función pública de una manera adecuada que es lo que espera la sociedad.

La Dra. Lamperti (2020) sostuvo que también es importante la capacitación permanente de los Juzgados porque son quienes Administran Justicia en la sociedad, razón por la que deben conocer la actuación de los Fiscales asociados a una determinada persona o usuario en internet a fin de determinar al responsable de la maniobra.

Por ello, la necesidad que los jueces tengan una capacitación sobre el tema, al menos mínima y luego seguir profundizando porque el conocimiento es de acceso público y eso

no debería ser una limitante. En conclusión, los jueces deben entender los conocimientos técnicos y el lenguaje que se utiliza en los casos de ciberdelincuencia.

Además, el Dr. Migliorisi (2020) refirió la importante labor que tiene el juez al decidir la culpabilidad o no de un procesado en un juicio pueda comprender la producción de la prueba. Por ello, es muy importante el trabajo de los peritos en explicar todo el procedimiento de la obtención de la prueba y la cadena de custodia.

La cadena de custodia es uno de los factores fundamentales porque una vez que el juez toma conocimiento de la prueba, se procederá a explicar cómo se produjo, pero la cadena de custodia es estratégica y fundamental porque podría traer abajo toda una investigación. En ese sentido, el autor consideró que seguiremos viendo más casos relacionados a los delitos cometidos mediante el uso de la tecnología que los tradicionales.

El Dr. Rincón (2020) manifestó que lamentablemente uno encuentra jueces que no entienden la problemática, que no dimensionan la magnitud del problema, no solo de los delitos sino del impacto que puede producir un fraude económicamente hablando simplemente por desconocimiento y no por mala fe.

Asimismo, consideró que es una situación muy delicada porque hay personas que hasta les aburre manejar un simple celular y el hecho de resolver temas de mayor complejidad pues es necesario que todos los jueces entiendan que deben capacitarse porque esta brecha de la tecnología puede demandar una cantidad de situaciones y generar conflictos sustanciales a la sociedad.

En esa línea de pensamiento, el Dr. Maza (2020) describió que se carece de conocimiento sobre el funcionamiento de algo tan básico como una red social, también es verdad que los jueces actuales pueden ser muy acertados en sus fallos leyendo la jurisprudencia de otros jueces. Sin embargo, en la parte más personal que sería empatizar con los hechos o con la condena que se impone, es lógico que al desconocer aspectos fundamentales de las nuevas tecnologías no tengan la misma aproximación y empatía con los casos, porque en ningún supuesto se pondrán en el lugar de la víctima o el agraviado. Por ejemplo, el típico caso de una persona que intentó comprar de forma online y fue estafado o de las personas que son víctimas del ciberbullyng, entonces la efectividad de la sentencia puede ser aceptable, pero nunca se va a generar innovación en la jurisprudencia. Un juez no puede estar viendo un día casos de violencia de familia y al otro día un caso de ciberdelincuencia.

El Dr. Acurio (2020) declaró que el tema es que si uno va a una audiencia de juicio oral y practica el testimonio de un perito formulando ciertas consultas como desde dónde obtuvo el hash o los códigos de integridad de los mensajes de datos o del contenido digital que está usado como prueba documental, el perito va entender, pero no hay certeza de que los jueces puedan hacer lo propio. Por eso, primero se debe aterrizar muchos términos a un lenguaje que pueda ser entendido por la mayoría porque quizá el juez no comprenda que son los códigos de integridad, pero sí la firma digital. Por esa razón, no se le puede exigir a los fiscales y jueces ser ingenieros de sistemas, sino al menos tener una formación en Derecho Informático y en la Informática Forense porque temas de informática no solo será visto en los juicios penales sino también en los casos de naturaleza civil.

El Dr. Temperini (2020) refirió que tiene que ver más con la habilidad del abogado que le presenta el caso al juez, si el abogado es suficientemente claro al momento de presentar la cuestión, los jueces con un poco de sentido común van a resolver bien. Lo que sucede es que uno presenta el caso demasiado complejo o muy técnico, el mismo que generará que los jueces tengan mayores incertidumbres al momento de resolver. A su vez, es importante contar con abogados que conozcan jurisprudencia europea a fin de tener mayor amplitud de conocimientos y saberlo interpretar a vista del juez.

11. ¿Qué opina sobre la necesidad de implementar Juzgados Especializados en Ciberdelincuencia como correlato de las Fiscalías Especializadas recientemente incorporadas?

El Dr. Carretero (2020) sostuvo que claramente es lo que debe hacer todo país, es decir que debe existir competencia en función de la materia en ciberdelitos donde encontremos a Fiscalías Especializadas, Cuerpos Especializados o sea que trabajen en conjunto las Fuerzas de Seguridad Especializados en Ciberdelitos con las Fiscalías y a su vez con los Juzgados Especializados, todos en forma conjunta porque de esa manera será la única vía idónea para mitigar estos problemas relacionados a la ciberdelincuencia.

En adhesión a lo anterior, el Dr. García (2020) desarrolló que es una pregunta bastante atractiva y considero que deben incorporarse juzgados especializados porque sucede muchas veces que no haya una paridad en cuanto a conocimiento jurídico y técnico de la causa. Requiere muchas veces que nos acerquemos al juzgado y le expliquemos acerca de nuestra pretensión, por ejemplo, si estamos hablando de un «Triage en el domicilio», que en otras palabras es el allanamiento en el inmueble para adquirir el volcado de memoria de los datos que tiene el imputado en el ordenador.

Todos esos procedimiento y herramientas que van a ser utilizadas, no son concedidas por la carencia de conocimiento o capacitación de los operadores de justicia. Para que puedan estar en similares situaciones cognoscitivas es necesario que se implemente un juzgado especializado para llevar adelante estas investigaciones complejas.

La Dra. Lamperti (2020) agregó que podría darse el caso de implementar estructuras de Juzgados Especializados atendiendo la misma demanda o competencia de las Fiscalías Especializadas. En otras palabras, los jueces que atienden casos de homicidio y robo también deben entender sobre tecnología en caso se presente un medio probatorio como un móvil o laptop y que comprendan por lo menos la obtención de información por WhatsApp, cómo se hace la extracción forense en un dispositivo, supuestos que deben ser totalmente entendidos por los operadores del Derecho. En ese sentido, la existencia de Juzgados Especializados tiene como correlato a las Fiscalías Especializadas en la medida que se les asigne alguna competencia en específico en la atención de casos de ciberdelincuencia.

Al respecto, el Dr. Migliorisi (2020) señaló que es fundamental porque el juez tiene que entender lo que está juzgando y para eso deben especializarse, considerando que en estos tiempos es imprescindible que la justicia esté especializada en esta rama. Por esa razón, se debe estar pensando de forma paralela el avance de la tecnología y la capacitación constante a los operadores del Derecho, no solo cuando se haya implementado Fiscalías Especializadas en distintos países, sino como medida de prevención, es decir fomentar las capacitaciones desde ahora.

A su vez, el Dr. Rincón (2020) comentó que esto tiene que ser un imperativo, o sea es necesario la obligatoriedad porque hacer lo contrario resultaría más costoso como el caso en el Sistema de Salud. Si hay una buena previsión en el sistema de salud no se va a ver afectado porque si uno previene la gente no va a ser la afectada, entonces pasa algo parecido en los casos de ciberdelincuencia porque un buen trabajo en este tipo de aspectos va hacer más fácil para la gente conocer esta situación y las capacitaciones no es un tema de un simple curso sino algo más profundo y constante.

Otro punto es tratar de difundir información sobre la configuración de los ciberdelitos. Un claro ejemplo es que si una persona mira el celular del otro es necesario que las personas sepan que puede llegar a configurarse un delito. Por otro lado, los medios de comunicación influyen muchísimo en la gente, entonces si los ciudadanos tienen el pleno

conocimiento sobre estos temas no se dejarán influenciar por las cosas ciertas e inciertas que transmiten los medios de comunicación.

El Dr. Maza (2020) trasladó que siguiendo la sintonía de la entrevista creo que es una necesidad y sería una garantía para los ciudadanos que al final haya Fiscalías y Juzgados que se dediquen a investigar e instruir, respectivamente un mismo tema y que se les descargue de trabajo por estar especializados para el resto del tiempo poder estar formándose en nuevas herramientas tecnológicas.

De manera similar, el Dr. Acurio (2020) postuló que tanto las Fiscalías y los Juzgados van a conocerse y saber con quienes están trabajando directamente para mantener una relación más fluida en un entorno de entendimiento y que ambos sean imparciales y objetivos. Se necesita que ambos operadores del derecho estén netamente activos más no sean activistas porque este concepto quita objetividad tanto para fiscal e imparcialidad para el juez. Por esta razón, es necesario contar con un marco de cooperación y debido proceso porque se está juzgando a personas que tienen derechos, los mismos que deben ser respetados en el marco al debido proceso. Por lo tanto, la jerga informática va a ser común y mejor entendida tanto para Fiscales como Jueces y eso les va a permitir encontrarse en una mejor situación cognoscitiva en la persecución del delito y en la administración de justicia.

El Dr. Temperini (2020) manifestó que es menos necesario contar con Juzgados Especializados en Ciberdelincuencia que Fiscalías, para que el juez sea imparcial no debe participar en la investigación. En ese sentido, el juez debe saber de derecho y no tanto de tecnología porque el que tiene que saber o dominar de tecnología es el fiscal para llevar adelante la investigación. El juez si debe tener noción para saber si lo que el fiscal presenta es suficiente para considerar a una persona culpable o inocente.

12. ¿Qué recomendaría al Estado peruano para aprovechar la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia en base a la experiencia argentina?

El Dr. García (2020) mencionó que es fundamental que conformen un equipo interdisciplinario que no solo comprenda a los funcionarios judiciales, sino que se necesitan psicólogos, peritos informáticos, analistas forenses y personal capacitado para realizar el trabajo de agentes reveladores. Se busca que se pueda trabajar en las fiscalías y que solo se derivan en menor proporción los casos a las dependencias policiales.

Asimismo, la Dra. Lamperti (2020) postuló que debe enfocarse en la capacitación del personal, la puesta a disposición de recursos en la atención de las demandas, la elaboración de estadísticas para ver cómo evoluciona el cibercrimen porque es fundamental contar con un observatorio o un mapa del delito o saber que se denuncia o si hace falta concientizar a la población en aspectos de ciberseguridad. Otro tema importante es promover campañas de concientización, campañas de prevención porque existen delitos que se pueden prevenir a tiempo.

El Dr. Migliorisi (2020) manifestó que en principio considera que todos deben capacitarse en altas tecnologías porque en una necesidad no solo consta del foro penal sino también en todas las áreas. En la actualidad la prueba la encontramos en el ciberespacio y la dinámica que tiene el internet es tan impresionante porque quizás mañana contaremos con el 80 % de las causas con una conexión directa de internet, por esta razón es imprescindible que todos los profesionales se capaciten constantemente en las altas tecnologías.

El Dr. Maza (2020) desarrolló que el haber incorporado una unidad de expertos en este ámbito no significa que podrán abarcar el volumen de delitos informáticos que se estén denunciando, entonces la difusión de los conocimientos en estos casos siempre es un buen punto de partida. Para ello, esta unidad debe estar formando a los colaboradores del Sistema de Justicia, ya no solo con el objetivo de mostrar conocimientos básicos, sino de generar el interés real de otras personas, previa creación de una base ocupacional.

Así también, el Dr. Acurio (2020) proscribió que la Unidad Fiscal Especializada en Ciberdelincuencia debe generar documentos de trabajo, instrucciones, protocolos de actuación para que la mayoría sepa cómo proceder frente a los ciberdelitos. En Ecuador se implementó el Manual de Manejo de Evidencias Digitales para toda clase de infracciones y pueda utilizarse en los casos que involucre un componente informático electrónico y se sepa cómo actuar en la cadena de custodia, cómo se tiene que embalar, el proceder en una evidencia y dónde localizar esta evidencia digital, esto es en dispositivos o redes, en memorias rash, en discos ópticos o discos sólidos. La idea es saber cómo actuar frente a los diversos casos de ciberdelincuencia y se maneje un conocimiento uniforme a nivel policial, fiscal y de administración de justicia.

El Dr. Temperini (2020) mencionó que sería poco eficaz que la Fiscalía solo tenga recursos, destino persecutorio y no hubiese nada de prevención porque la gente no se daría cuenta cuando es víctima de un delito. La recomendación es que la reciente

incorporación de esta Fiscalía como órgano de prevención es interesante y bueno como primera etapa de 6 meses a 1 año es un gran avance, pero la misma debe ir capacitando un equipo de profesionales internos que sea interdisciplinario con aportes de psicología, sociología porque cuando más disciplina se tiene, mejores son los resultados. Asimismo, empezar a absolver ciertas dudas sobre estos casos y no dejar de prestar colaboración o asesoría a otras fiscalías no especializadas.

13. ¿Alguna sugerencia o recomendación que desee agregar?

El Dr. Carretero (2020) manifestó que es importante considerar el ingresar al ámbito virtual es como si nos encontráramos en el medio de la calle con un megáfono diciendo todo lo que cargamos en las redes, como los viajes, paseos, compras, salidas, entre otros. Por ello, todo lo que se sube a las redes no es privado y hago hincapié en la responsabilidad digital porque uno mismo es responsable de lo que informa abiertamente en la virtualidad.

Otro punto importante son las claves de seguridad, estas son como las llaves de una casa, uno no tiene una sola llave para cada puerta porque si se traslada ese supuesto en el ámbito digital, será más fácil acceder a las cuentas personales. Por lo tanto, se debe tener presente que la virtualidad no es privacidad.

A su vez, el Dr. García (2020) comentó que es muy importante concientizar a la ciudadanía sobre las contraseñas que utilizan para sus redes sociales y cuentas bancarias y evitar que controlen nuestras cuentas. Se recomienda activar la capa de seguridad personal, esto es, el control de identidad en dos pasos. Asimismo, conversar con los menores del hogar y advertirles que no hablen con desconocidos, tampoco ingresen a plataformas no seguras, siempre por los sitos oficiales. En ese sentido, los padres deben tener la responsabilidad con los hijos y acompañarlos en este mundo de la tecnología. Los niños en su habitación se encuentran en una cancha de fútbol en donde hay muchísimas personas extrañas y son vulnerables, por eso los padres tienen la tarea de evitar que sus hijos sean víctimas de estos delitos tan aberrantes.

La Dra. Sabrina (2020) agregó que se promueva información relacionada a Ciberdelitos, y que tal vez los más jóvenes de la familia puedan ayudar a los más adultos a generar algún tipo de sinergia a fin de evitar brindar información más allá de lo permitido. Asimismo, los organismos como la Defensa del Pueblo, Defensa del Consumidor, entre otras, promuevan cursos de capacitación o al menos conocimiento general a la población,

mensajes a través de los medios de comunicación, campañas de difusión, prevención y todo lo que sea posible para utilizar a favor de la prevención de estos delitos.

Por lo tanto, es muy importante e interesante que se involucren otros actores de la sociedad civil y poder comprender el fenómeno del cibercrimen, más allá de lo conocido como crimen físico y comprender el fenómeno del cibercrimen, adoptarlo y generar respuestas que permitan una mejor convivencia en sociedad.

Asimismo, el Dr. Migliorisi (2020) señaló que los delitos que se configuran a través de la internet en muchos casos se pueden prevenir. En la actualidad tenemos la extorción, casos de grooming que también se pueden prevenir, el fraude, entre otros delitos; y es importante resaltar que estos delitos se encuentran en el top de los últimos años en Cibercrimen. A su vez, el autor consideró que con el buen uso de las tecnologías se podrán prevenir los delitos informáticos y de esa manera ahorrarse un disgusto que significa ser víctima de estos delitos, tales como el hackeo o las descargas de malware.

Téngase en cuenta que los bancos, redes sociales, tarjetas de crédito piden validar datos sin previa solicitud. Por lo tanto, la forma de prevención es clara y concreta más allá que la modalidad delictual o el modus operandi. Es una cuestión de permanente capacitación por parte del Estado, Fiscalías y Juzgados a fin que la gente capte la información, difunda y ponga en práctica todo lo aprendido.

El Dr. Rincón (2020) enfatizó que es una responsabilidad de todos quienes deben estar a la vanguardia en los temas de la tecnología, siendo una cosa que sí o sí se debe hacer, no admite más dilación o temas de demoras. Es inaceptable que se presente una prueba y que los fiscales no tengan conocimiento o puedan objetar sin tener la claridad sobre esos temas.

En autor señaló que en la mayoría de entrevistas suele comentar el siguiente ejemplo, uno para tener un auto no es necesario que sea mecánico, pero sí conocer al menos lo básico en caso se presente alguna contingencia en pleno camino, entonces se debe contar con conocimiento en ciberdelincuencia y en la medida que se tenga esa claridad en el conocimiento se podrá llegar a establecer un marco regulatorio amplio que sea más coherente con la realidad.

Aunado a ello, el Dr. Maza (2020) sostuvo que lo primero es la seguridad informática, puesto que prevenir va a ser siempre y lo es ya, la mejor solución para evitar la comisión de delitos informáticos. También es recomendable que cambien la contraseña de todas

sus redes sociales, para evitar la vulneración de sus cuentas, en la medida de lo posible se debe utilizar copias de seguridad para restituir la información. Finalmente, no envíen datos personales a ninguna cuenta que lo solicite, tampoco deben difundir su vida privada en redes sociales, solo el material necesario como una cuenta de trabajo en la que se difundan logros académicos y otros similares.

El Dr. Acurio (2020) indicó que uno debe ser muy cauteloso cuando realice transacciones en internet y debe verificar la seguridad, no creer en correos electrónicos de dudosa procedencia y más aún cuando uno está desempleado las entidades suelen enviar correos orientados a facilitar un crédito inmediato, entre otros. Otro punto importante es que si algo es gratis en internet uno ya no es el cliente sino el producto, o sea todos tus datos personales es lo único que requieren las redes para que funcionen entre sí, por ese motivo uno debe ser desconfiado y estar atendo a este tipo de situaciones y sobre todo conocer los canales virtuales de sus instituciones financieras y al momento de hacer transacciones presenciales no recibir ayuda de extraños y además contar con un antivirus en sus dispositivos de uso diario y poco a poco llegar a tener una higiene cibernética.

El Dr. Temperini (2020) mencionó que se debe tratar de practicar a todo momento un pensamiento crítico sobre lo que uno recibe, entender que todo puede ser falso entonces cada correo electrónico, publicidad o cada cosa que uno ve por lo menos dimensionar la posibilidad que esa información sea falsa y a partir de ahí plantearse algunas preguntas que permitan generar duda sobre la procedencia e información de estos mensajes. En sentido, se debe tener la cautela utilizada en la calle y practicarlo en internet, porque es más fácil hackear a humanos que a sistemas. Por último, se debe ser consciente del grado de inseguridad que tenemos y actuar como tal, con un nivel de desconfianza que permita detectar los ataques más comunes.

3.2.2. Análisis de las entrevistas nacionales

3.2.2.1. Análisis de las entrevistas a abogados especialistas

OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.

1. ¿Cuáles son los problemas más recurrentes durante el desarrollo del proceso judicial entre una Fiscalía Especializada en Ciberdelincuencia y un Juzgado no Especializado en la materia?

El Dr. Guerrero (2020) comentó que debemos tener en cuenta que existen dos supuestos para la comisión de estos delitos. De un lado, tenemos a los delitos informáticos que han sido creados a través de una ley especial, tales como la suplantación de identidad, el acceso ilícito a un sistema informático, entre otros. De otro lado, tenemos a los delitos que son mediados por la tecnología y que alguno de ellos no está en la ley descrita anteriormente, por ejemplo, el acoso cibernético. Las fiscalías han consolidado una experticia en base a la experiencia. Sin embargo, no hay juzgados que sean especializados en resolver casos de delitos informáticos y menos aún de aquellos mediados por la tecnología. Es así que, el principal problema es el desconocimiento sobre el funcionamiento de la tecnología que se utiliza para cometer estos delitos, es cierto que el Ministerio Público adquirió cierta experiencia en algunos delitos, pero eso aún es imperceptible en el Poder Judicial.

De igual forma el Dr. Elías (2020) expuso que no tenemos fiscales especializados en cibercrimen en el Perú, la idea a largo plazo es contar con ellos, lo que recientemente se creó a inicios de año es una Unidad Administrativa y de Coordinación Técnica, esto es, los fiscales comunes continuarán realizando las investigaciones dentro de cibercrímenes previstos en la ley de delitos informáticos. El problema que experimenté dirigiendo el Observatorio Peruano de Cibercriminalidad, es el mal sistema de comunicación entre el Ministerio Público y el Poder Judicial en materia especializada. Esto quiere decir que, si a un juez penal le hablas sobre el delito de child grooming, seguro podrá entender. Sin embargo, al hablarle de ataque de negación de servicios o la identidad virtual en entornos digitales como juegos de rol o señalas aspectos técnicos como el uso de bitcoins o criptomonedas en los delitos tradicionales ya es muy complicado y no porque no lo sepan, sino por ser demasiado novedoso y requiere una capacitación especializada. Entonces, los problemas más recurrentes están relacionados a la falta de conocimiento específico en la materia especializada de cibercriminalidad y prueba digital.

El Dr. Cuadros (2020) señaló que una de las falencias que existe en el Ministerio Público y en otras instituciones vinculadas al sistema de administración de justicia es el aspecto presupuestal. Esta Fiscalía tendrá que afrontar un adecuado manejo de la evidencia digital, así como un buen manejo de las herramientas tecnológicas e informáticas. Sobre lo primero, el problema se presentaría desde el momento de obtenerla hasta el momento de su actuación en juicio, espacio en el que se convertiría en prueba. Respecto a la Unidad Fiscal que prestará apoyo a los despachos fiscales será de mucha utilidad en aspectos

investigativos, pero al no contar con Juzgados con el mismo nivel de especialización no se podrá decidir acertadamente.

2. ¿Cómo será el proceso de adaptación de la Unidad Fiscal Especializada en Ciberdelincuencia al no contar con Juzgados Especializados en la materia?

El Dr. Guerrero (2020) comentó que estas unidades especializadas ya existen en otros países como Argentina y Brasil desde hace muchos años, y la forma en la que han evolucionado es la siguiente, en un primer momento brindan acompañamiento y asesoría, fermentan la creación de capacidades a los fiscales, en un segundo momento dejan de ser meros acompañantes y se convierten en unidades titulares de la persecución del delito, es decir, investigan y litigan en juicio. Uno de mis temores es que no quedan muy claros algunos asuntos, tengo la impresión de que esta unidad empezará brindando asesoría, pero por la forma como funciona el Ministerio Público, no sé si se transformará en unidades que se dediquen a litigar este tipo de casos. Tampoco me queda claro si esta unidad solo perseguirá casos de delitos informáticos o incluirá también a los delitos mediados por la tecnología que en general puede ser cualquier delito. Por ello, al no haber una unidad especializada en delitos informáticos ni en delitos mediados por la tecnología, pienso que la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia que es muy bueno, seguirá siendo incompleto.

Igualmente, el Dr. Elías (2020) sostuvo que la idea es contar con una fiscalía especializada en el litigio del cibercrimen. Es decir, que investigue y que lleve estos casos a juicio. Sin embargo, esta Unidad Especializada no lo hace todavía, progresivamente lo hará, espero que en algún momento se concrete un plan piloto de fiscales en ello. En principio esta Unidad tiene que generar manuales, protocolos o instructivos de cómo investigar algunos tipos delictivos por ejemplo estafas en entornos digitales e intrusismo informático para que los fiscales comunes sepan como investigar mínimamente estos delitos. El segundo paso sería que los Fiscales Especializados investiguen este tipo de delitos y no fiscales comunes.

El Dr. Cuadros (2020) refirió que la creación de esta Unidad representa un gran paso en un camino muy extenso. La creación de Fiscalías Especializadas en cada distrito fiscal es una idea muy alejada de nuestra realidad porque lo más viable sería la creación de unos 8 o 9 despachos supraprovinciales en Lima y distribuir la competencia. El inconveniente que siempre estará presente es la falta de presupuesto y con el monto actual es inviable ponerlo en práctica.

3. ¿Qué resultados a nivel investigativo se obtendrán con la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

El Dr. Guerrero (2020) describió que dentro de los resultados positivos está la mejora en la visibilidad de los delitos informáticos o delitos mediados por la tecnología que ocurren en el Perú, también permitirá mejorar el entendimiento de lo grande que es este delito y cuáles llegan a ser denunciados. A nivel investigativo vamos a tener una imagen más completa de la comisión de estos delitos en el territorio nacional. Asimismo, se podrá apreciar el nivel de impunidad porque no todo delito visto por esta unidad va a llegar a la etapa procesal de Juicio Oral.

Además, el Dr. Elías (2020) mencionó que en el Observatorio de Cibercriminalidad se investigó el fenómeno delictivo de la ciberdelincuencia en el Perú. El punto preocupante radica en la formalización de fraudes informáticos porque solo se formalizaron desde el 2015 hasta el 2020, 138 casos. Es decir, de casi 6474 casos, se ha obtenido 10 sentencias y 1 terminación anticipada. Se observa que el grueso de los casos no llegó a mayores, esto es, un 2 % y evidentemente es una cifra muy baja en cuestión de formalización de casos. Pasemos a los delitos contra los datos y sistemas informáticos en el Perú, hemos obtenido en 5 años, solamente 23 formalizaciones, esto representa el 3 % de casos y si vemos los delitos de suplantación de identidad, en 5 años hemos obtenido en 0.44 % de formalizaciones. Es de entender que los casos no se están judicializando, por lo que necesitamos fortalecer las investigaciones preliminares para pasar a la investigación preparatoria, sino los casos seguirán estancados.

El Dr. Cuadros (2020) sostuvo que resulta beneficioso para el distrito fiscal y judicial de Lima porque es el único distrito en el cual se encuentra en vigencia el Código de Procedimientos Penales de 1940. Distinto es lo que se puede aplicar con el Código Procesal Penal de 2004 en donde el señorío de la investigación recae en el fiscal. También se reforzará los conocimientos sobre la correcta práctica de la cadena de custodia y la utilización del sobre Faraday para impedir que remotamente se elimine información que podría ser utilizada para el esclarecimiento de los hechos en la presunta comisión de un delito.

4. ¿Qué medidas debe adoptar el Estado peruano para una eficiente investigación y administración de justicia en los casos de Ciberdelincuencia?

El Dr. Guerrero (2020) señaló que hay dos tipos de medidas o políticas que las entidades dentro del Estado pueden promover, evidentemente cada una de ellas dentro de su ámbito de competencia. Ahora bien, el Ministerio Público realizó bastante con la creación de la UFEC, aunque podría hacer más con el cambio de su ley orgánica para permitir que esta unidad se encargue del litigio de estos casos. A su vez, se puede generar mayor concientización para que las personas no sean vulnerables a la comisión de este tipo de delitos. Adicionalmente, el Poder Ejecutivo a través de la Secretaria de Gobierno Digital que es una entidad adscrita al Consejo de Ministros definió quiénes son los llamados a combatir a la delincuencia en entornos digitales, principalmente mediante la Ley de Gobierno Digital y el Decreto de Urgencia de Confianza Digital, ambas leyes concluyen que el Poder Judicial, el Ministerio Público y la Policía Nacional del Perú son los encargados de liderar la lucha contra los delitos que se comenten a través de medios digitales.

Asimismo, el Dr. Elías (2020) comentó que luego de haber resaltado las cifras a nivel nacional, corresponde platicar sobre las mismas a nivel local. En el distrito fiscal de Cañete solo hubo 5 casos de Cibercriminalidad. A pesar de ello, no creo que sea así, o están mal registrados o la población no está denunciando por desconocimiento. Ahora bien, analicemos el tiempo de respuesta entre la interposición de la denuncia y la primera disposición, en el mejor de los casos 28 días y en el peor de los casos 290 días, que en su mayoría son rechazos liminares.

Los fundamentos del archivo es que no se cuenta con datos para identificar al autor del hecho denunciado, si estamos viendo suplantación de identidad obviamente no se conoce los datos, justamente por eso los agraviados acuden al Ministerio Público. Asimismo, en los casos donde sí se han llevado investigaciones preliminares, principalmente las diligencias fueron propuestas por las partes.

Es así que, se deben incorporar Fiscalías Especializadas, los fiscales deben otorgar una respuesta inmediata porque una de las características del cibercrimen es la volatilidad de la prueba y contar con manuales o protocolos que permitan al fiscal que no conoce sobre cibercrimen o está en proceso de especialización tener una mejor respuesta a los casos planteados por la ciudadanía, el último sería fortalecer nuestros laboratorios, así como el personal administrativo que se encarga de la investigación, esto es, la DIVINDAT.

El Dr. Cuadros (2020) aludió que a nivel del Poder Ejecutivo en coordinación con el Ministerio Público, el Poder Judicial y la Policía Nacional del Perú se debería destinar un

presupuesto específico para la creación de un subsistema especializado en ciberdelincuencia ya que es evidente el problema de que todos no manejamos la misma información y términos técnicos.

Ahora, ocurre que la Policía cuenta con una Unidad Especializada que no se abastece para abarcar todo el territorio nacional. De qué sirve tantos esfuerzos si al llegar a juicio, el juez no toma conciencia de la dañosidad de este tipo de conductas. Se debe crear un subsistema similar al que ahora existe en Crimen Organizado y Corrupción de Funcionarios. Además, pienso que deberían crearse oficinas de peritaje exclusivo de estos temas.

5. ¿Cómo debería distribuirse la Unidad Fiscal Especializada en Ciberdelincuencia para cubrir las zonas con mayor incidencia delictiva a nivel nacional?

El Dr. Guerrero (2020) mencionó que lo ideal sería que esta Unidad Especializada realice su trabajo a nivel nacional, pero la realidad peruana nos muestra inconvenientes en cuanto a prioridades presupuestales y nivel de incidencia de delitos informáticos. Respecto a esto último, se sabe que el mayor número de víctimas está concentrado en Lima, lo cual no tiene ningún misterio porque es donde hay más personas.

El problema es que el lugar en el cual se comete no es necesariamente donde se encuentra la víctima, no es posible aplicar lo que normalmente se haría en otros delitos como hurto, robo u otro. Hasta cierto punto es posible identificar desde dónde se comenten, pero en el caso de los delitos informáticos o de los delitos mediados por la tecnología desde su inicio no se puede saber necesariamente. Dado que, se necesita pasar por un proceso de investigación previa para recién saber si los delincuentes se encuentran en Perú u otros países. A decir verdad, sería ideal que haya una distribución a nivel nacional, pero considero que no será así al menos por un buen tiempo.

Adicionalmente, el Dr. Elías (2020) comentó que eso dependerá del presupuesto, si lo tuviésemos tendríamos una Fiscalía Especializada en cada uno de los distritos fiscales. Sin embargo, no creo que suceda esto a corto plazo. Antes de pensar en incorporarlas, considero que el Estado debería sincerar las cifras que tiene actualmente la Fiscalía porque según la investigación realizada por el Observatorio de Cibercrimen se encontró que en los últimos 5 años hay 9619 casos que no han sido catalogados, se señala que son de manera genérica delitos informáticos, pero no precisan si se tratan de delitos contra datos y sistemas informáticos, contra la indemnidad y libertad sexual, contra la intimidad

y el secreto de las telecomunicaciones, contra el patrimonio, contra la fe pública, o delitos comunes.

Entonces, si no sabemos cómo está distribuida esa carga, no lograremos conocer el nivel de incidencia en cada uno de los distritos fiscales. Luego de eso, deberían corroborar si están perfectamente catalogados los delitos porque parece que muchas denuncias ingresan por fraude informático y es la razón por la que ese delito está en tan alta incidencia, pero en realidad no son tal, sino son fraudes comunes que se cometen a través de entornos digitales. Por lo tanto, estamos inflando una cifra de un delito que no le corresponde. A su vez, deberían implementarse las Fiscalías Especializadas en distritos fiscales con mediana intensidad delictiva para que puedan empezar a trabajar y ver cómo es que están respondiendo el Ministerio Público estos casos. Adicionalmente, pienso que se debería investigar al margen de la pandemia, el uso de las plataformas virtuales como Zoom, Microsoft Teams, Google Meet, entre otras, con el propósito de realizar las diligencias y evitar el traslado físico.

El Dr. Cuadros (2020) suscribió que actualmente la unidad técnica solo brinda un apoyo general, no está realizando labor investigativa. Por lo que, sería más viable crear despachos supraprovinciales que se encuentren en Lima, pero con competencia a nivel nacional considerando que se va a trabajar con la Unidad de Cooperación Internacional del Ministerio Público para desarticular una red vinculada a la pornografía infantil.

OE_1: Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

6. ¿Qué opina sobre la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia como órgano consultor y no como órgano persecutor de estos delitos?

El Dr. Guerrero (2020) refirió que es un paso en la dirección correcta, sé que por muchos años la existencia de una Unidad Especializada estuvo rondando por el Ministerio Público, de la misma manera con otras materias especializadas. Entonces, reconozco que es un gran paso, pero sigue siendo parte del proceso. Seguramente hay muchos fiscales que han llevado casos vinculados a la ciberdelincuencia y advirtieron que es necesaria la implementación de una Fiscalía Especializada por el constante crecimiento de esta clase de delitos. En mi opinión, se tomó una decisión considerando el alcance del presupuesto y el volumen del personal, espero que con el tiempo puedan dar el siguiente paso, teniendo

en cuenta la experiencia extranjera. Al final, podremos ver en algunos años si el modelo funcionó en Perú y de ser necesario expandirlo.

Asimismo, el Dr. Elías (2020) mencionó que es adecuado, recordemos que llevamos retrasados más de 15 años. Es positivo que esta Fiscalía se encargue de tender los puentes y ser una especie de mentores o capacitadores de lo que es en la práctica la Cibercriminalidad. Me parece que es bueno, pero no completo. Hubiese sido ideal que empezáramos con esta entidad administrativa y adicionalmente un plan piloto con alguna Fiscalía que pudiera realizar las investigaciones.

El Dr. Cuadros (2020) postuló que la creación de esta unidad consultora o de guía es un acierto, dado que la data que se obtendrá permitirá tener una idea clara de los distritos con mayor incidencia de delitos informáticos. Además, recientemente se convocó a nivel nacional para que en cada distrito fiscal exista un fiscal provincial y un fiscal adjunto que integren la red de Fiscales Especializados en Ciberdelincuencia y quizá con las personas que integren el plan piloto se podrá crear Fiscalías Especializadas.

7. ¿En su opinión ante el aumento de los delitos informáticos fue oportuna la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

El Dr. Guerrero (2020) mencionó que fue oportuno y me atrevería a decir que su implementación pudo ser antes y si hubiese sido así, los resultados serían mejores porque la ocurrencia de estos delitos fue antes de la implementación de la Ley de Delitos Informáticos. De hecho, el Perú es uno de los últimos países que se ha suscrito al convenio de Budapest, lo hicieron otros países de la región con varios años de antelación. Esta Unidad nos permitirá conocer mejor la situación en la que estamos, si son críticas o todavía es manejable.

A su vez, el Dr. Elías (2020) refirió que en el año 2015 escribió un artículo llamado «Luces y sombras de la delincuencia informática en Perú» y una de mis propuestas fue la necesidad de implementar una Fiscalía Especializada en Cibercrimen y fortalecer la DIVINDAT y creo que este paso que hemos dado como Estado es muy importante.

El Dr. Cuadros (2020) describió que fue necesario, pero no oportuno porque debió crearse hace mucho tiempo. Debemos tomar en cuenta que nuestro país recién se suscribió al convenio de Budapest, pero desde antes se tomó este instrumento normativo internacional como modelo para el establecimiento del marco regulatorio. Al ser transnacionales estos

delitos, permiten que al otro lado del mundo pueden estar cometiendo un delito informático que está agraviando a un peruano.

8. ¿Por qué es necesario que los fiscales cuenten con conocimientos en derecho y en tecnología para detectar, individualizar y perseguir los casos de Ciberdelincuencia?

El Dr. Guerreo (2020) señaló que para que un fiscal investigue delitos de Crimen Organizado no solo basta el estudio y el conocimiento del derecho porque se necesitan múltiples capacidades para que lo pueda hacer de manera eficiente y segura. Lo mismo sucede con los casos de los delitos informáticos, puesto que el fiscal no solo debe estar capacitado para subsumir el hecho con el tipo penal, sino conocer qué herramientas tiene para poder hacer una investigación, imaginemos que un fiscal desconozca la manera de extraer información de un disco duro o carezca de conocimientos sobre el manejo de las redes sociales. Lo lógico será que no se realizará una investigación óptima y probablemente el caso sea archivado.

A su vez, el Dr. Elías (2020) refirió que los delitos se van sofisticando y el hecho de referenciar al cibercrimen no necesariamente significa que solo existe prueba digital, si observamos el resto de casos de corrupción de funcionarios, trata de personas, estafas y demás, cada vez el uso de entornos digitales o nuevas tecnologías son empleados por delincuentes, por eso los funcionarios que administran justica en nuestro país deben acceder a este tipo de herramientas o instrumentos.

Por lo tanto, un fiscal tradicional necesita conocer que es una técnica de búsqueda de fuente abierta como técnica OSIM, cómo se debe asegurar la prueba digital, para qué es importante el agente encubierto digital y no estamos hablando de delitos informáticos, estamos hablando de prueba digital en la investigación de delitos tradicionales, es por ello que los fiscales deben conocer sobre nuevas tecnologías porque ese es el reto que llegó hace varios años.

El Dr. Cuadros (2020) desarrolló que en la actualidad es indispensable que cualquier abogado al margen que pueda desempeñar una función pública o privada tenga conocimiento en tecnología y esto no solo para detectar, individualizar y perseguir casos de ciberdelincuencia, ya que hoy en día cualquier persona puede tener acceso a estos medios y cometer distintos ilícitos. Creo que si los que formamos parte de la Administración de Justicia no nos encontramos a la par, será complicado investigarlos y no se obtendrán los resultados esperados, brindándose un mensaje negativo a la sociedad.

9. ¿Cómo deben adaptarse los estudios jurídicos para el ejercicio de una adecuada defensa técnica ante la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

El Dr. Guerrero (2020) refirió que tanto para los delincuentes informáticos, así como la gente que se ve involucrada voluntaria o involuntariamente en estos delitos, van a tener que reforzar sus capacidades a nivel técnico. Me atrevo a decir que la idea no está direccionada al ámbito legal porque la ley ya está implementada, sino que la defensa técnica va a tener que educarse en técnicas investigativas para poder desbaratar la teoría fiscal. Uno de los principales inconvenientes se presentará cuando tanto los fiscales como los abogados defensores estén en el mismo nivel de especialización, en tanto que la primera limitación se va a presentar en el Poder Judicial al no contar con jueces especializados para resolver estas causas. La competición entre la defensa y la fiscalía terminará cuando el juez deje de entender de lo que le están alegando.

A su vez, el Dr. Elías (2020) mencionó que existe desconocimiento a nivel de Ministerio Público, así como de abogados defensores particulares, estos últimos muchas veces no saben que es un código hash, copia espejo, entre otros. Presentan pantallazos que pasado un tiempo no saben de dónde lo obtuvieron. En ese sentido, se advierte que hay un desconocimiento generalizado de los abogados defensores. Eso significa que tienen menos herramientas de las que pueden tener para ejercer una defensa. Además, al no encontrarse capacitados tienen menos posibilidades de cuestionar los argumentos de la fiscalía, eso ameritaría que se capaciten en Cibercrimen, Seguridad Informática y Prueba Digital por lo menos para ejercer una defensa eficiente en el estadío en el que nos encontramos.

El Dr. Cuadros (2020) señaló que actualmente existen muchos estudios jurídicos que están especializados en temas informáticos o tecnológicos vinculados al Derecho de forma general, no necesariamente en el ámbito del Derecho Penal o Procesal Penal. En ese sentido, podría decirse que los estudios se encuentran mejor preparados que los representantes de la Administración de Justicia. Se debería revisar el manual de evidencia digital porque es útil para cualquier tipo de investigación criminal.

OE_2: Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

10. ¿Qué aspectos cree usted que se puedan potenciar en el Sistema de Justicia para la atención idónea de los casos de Ciberdelincuencia?

El Dr. Guerrero (2020) mencionó que son tres puntos principales sobre lo que se puede potenciar el Sistema de Justicia. Cuando se creó la División de Investigación de delitos de Alta Tecnología y por la manera en la que se hizo público su trabajo, lo primero que uno piensa cuando es víctima o asiste a alguien que fue víctima de un delito informático o de alguno mediado por la tecnología es acudir a la DIVINDAT, al menos en Lima.

De acuerdo a mi experiencia puedo comentarles que esa unidad policial especializada es muy buena en ciertos delitos informáticos. Sin embargo, no son nada buenos en la atención de casos de acoso por internet, acoso sexual o chantaje sexual que ahora son delitos desde el 2018. La división policial no sabe qué hacer con estos casos. Primero porque no son delitos informáticos. Segundo porque tocan temas muy alejados de los que están acostumbrados a ver. Tercero es que la DIVINDAT agotó su capacidad de recepción por delitos distintos a los informáticos. Entonces, se debe mejorar la capacidad de atención de la División Especializada. Asimismo, la Unidad recientemente incorporada debe tener como visión capacitar a los demás fiscales para entender el tratamiento de este tipo de denuncias y cómo es que debe realizarse la investigación de los delitos mediados por la tecnología y no necesariamente delitos informáticos. Por último, el Poder Judicial debe actuar acorde educándose en estos temas para cuando los reciban sean tratados de manera eficiente.

En la misma línea, el Dr. Elías (2020) refirió que son necesarios los Juzgados Especializados en Cibercrimen, no sé si en estos momentos porque ni siquiera tenemos Fiscalías Especializadas en Cibercrimen, pero sí en algún momento. Luego de ver las cifras a nivel nacional, sencillamente un juez especializado en investigación preparatoria o juzgamiento no tendría nada que hacer durante todo el año. Entonces, necesitamos capacitar a nuestros operadores de justicia en aspectos básicos de entorno digitales para que por lo menos conozcan cómo se aborda la prueba digital porque en absolutamente todos los casos se requiere el levantamiento del secreto de las telecomunicaciones para acceder a los teléfonos o correos electrónicos, lamentablemente la mayoría de nuestros jueces no cuentan con esa preparación.

El Dr. Cuadros (2020) sostuvo que debería crearse un sistema especializado en cibercrimen o ciberdelincuencia y que se dote de los recursos necesarios de forma conjunta o coordinada tanto a la Policía, Ministerio Público y el Poder Judicial, ya que no

sirve de mucho que una institución pública se potencie y que esta institución tenga que arrastrar si no todos están en igualdad de condiciones. Al no obtenerse el resultado que se espera se brinda un mensaje inapropiado a la sociedad.

11. ¿Por qué hasta la fecha no hemos incorporado Juzgados Especializados en Ciberdelincuencia teniendo en cuenta la complejidad de estos casos?

El Dr. Guerrero (2020) mencionó que la respuesta no solo debe orientarse a estos delitos, sino para cualquier delito especializado, tales como crimen organizado o delitos en los que ingresa el factor de género. Todo es parte de un proceso, nuestro Estado es lento, las normas se expiden en tiempos muy prolongados, hay un presupuesto misérrimo o simplemente no lo gestionan y ejecutan correctamente. Pienso que todos estos factores involucrados son los causantes del retraso, lamentablemente nuestra realidad es así. Deberíamos empezar por implementar una comisión dentro del Poder Judicial y se consiga la atención política. Ahora bien, puede pasar que en algún momento el Ministerio Público, mediante la UFEC y la Policía Nacional del Perú, a través de la DIVINDAT empiecen a quejarse y exijan que también se cree un Juzgado Especializado en Ciberdelincuencia porque al llegar a juicio se presentan múltiples problemas con el buen resolver de los jueces.

Adicionalmente, el Dr. Elías (2020) refirió que no se ha considerado la necesidad de contar con estos órganos especializados de investigación, procesamiento y de solución en la materia. Recién con la pandemia se ha visto las diferentes formas en las que se puede ser víctimas de estos delitos, de los cuales estamos muy atrasados. Si uno revisa la Ley N.° 30096, en las disposiciones finales y complementarias se señala el deber del Estado en capacitar a los Policías, Fiscales y Jueces en materia de Cibercrimen y a la fecha son muy pocas cortes que realizaron conversatorios y salvo un curso especializado en Cibercrimen y Prueba Digital en el que participé con el Observatorio Peruano de Cibercriminalidad. El resto del país, los miles de jueces que tenemos no tienen conocimiento y es un problema lamentable.

El Dr. Cuadros (2020) señaló que el principal inconveniente es el tema presupuestal, recién a raíz de la pandemia se están masificando este tipo de delitos y hasta que uno no se sienta afectado directamente no toma conciencia sobre la delicadeza del asunto. Es como los temas de corrupción, al inicio no se entendía que los fondos del Estado nos afectaban a todos. Si bien es cierto existe una gran incidencia, pero aún no se valora de la

forma correcta pues de lo contrario ya se habría incorporado Juzgados Especializados, lo cual esperemos suceda muy pronto.

12. ¿Por qué deberíamos incorporar una Justicia Especializada en Ciberdelincuencia?

El Dr. Guerrero (2020) refirió que el Ministerio Público cumplió con el primer paso al incorporar a la Unidad Fiscal Especializada en Ciberdelincuencia por lo que ahora le corresponde al Poder Judicial hacer más que solo esperar que el caso llegue a juicio. Considero que la nueva normalidad son los delitos informáticos y aquellos cometidos en medios tecnológicos y mientras no se convierta en una prioridad, la justicia seguirá siendo ineficiente y lenta, y no cumplirá con las expectativas de la sociedad y para las que fueron creadas.

A su vez, el Dr. Elías (2020) mencionó que debemos incorporarla a un mediano plazo porque el juez que conoce un caso de omisión de asistencia familiar, estafa, hurto o robo, no tiene las mismas competencias específicas para conocer una suplantación de identidad o cómo funcionan los agentes encubiertos. Lo que requerimos es la creación de estos Juzgados para que nuestros jueces tengan conocimiento específico en estos temas, caso contrario por más formalizaciones que tengamos de nuestros fiscales, los jueces no sabrán cómo procesar esa información.

El Dr. Cuadros (2020) propuso que los temas relacionados a los delitos informáticos, ciberdelincuencia y Cibercrimen son temas que requieren conocimientos técnicos especializados, no solo en Derecho sino también en la Tecnología. A su vez, no solo se debe contar con conocimientos teóricos sino también prácticos que son adquiridos a través de la experiencia. Por ello, es necesario crear un sistema especializado en ciberdelincuencia y fortalecer la justicia especializada en delitos informáticos, no porque estos delitos no son tipificados o no exista un órgano encargado para que investigue, sino que la falta de conocimiento, especialidad, técnicas de investigación y de herramientas, genera que no se llegue a identificarlos o prevenir la comisión de los delitos informáticos.

13. ¿Alguna sugerencia o recomendación que desee agregar?

El Dr. Guerrero (2020) mencionó que desde mi experiencia les puedo decir que de la misma manera en que los jueces, fiscales y policías deben educarse, también lo deben hacer los ciudadanos, preferentemente en el uso de la tecnología sobre todo porque eso redunda en su propio beneficio, porque si uno entiende cómo funciona un producto o

servicio por internet puede estar menos expuesto a la comisión de un delito. Intentemos trasladar las prácticas del mundo físico al mundo digital, esto es, no confiemos en todo lo que vemos o nos muestran porque no todo es seguro. Un claro ejemplo de trabajo en conjunto son los grupos de Facebook que se están creando en donde se alertan entre ellos y se empieza a crear sentido común, para ello tengamos la voluntad y seamos acuciosos antes de tomar alguna acción en los medios informáticos. No obstante, si son víctimas de estos delitos puedan saber que cuentan con unidades especializadas tanto en la Policía Nacional del Perú como en el Ministerio Público – Fiscalía de Nación.

Asimismo, el Dr. Elías (2020) refirió que una forma segura de prevenir la comisión de estos delitos es usar contraseñas fuertes, no utilizar las mismas claves para cada una de sus cuentas bancarias, correos electrónicos, entre otros. En la medida de lo posible hacer un factor de doble autentificación para fortalecer las medidas de seguridad. Capacitarnos en cursos de seguridad informática para conocer cómo es que se practican las nuevas estafas en los entornos digitales. Finalmente, si son víctimas de estos delitos, no duden en denunciarlos porque lamentablemente hay una gran cifra negra por conocer.

El Dr. Cuadros (2020) sostuvo que la única forma de prevenir estos tipos de delitos es con conocimiento. El tener los conocimientos adecuados para no asumir determinados riesgos cuando uno entrega información personal en un formato abierto. Esas personas que extorsión mediante la internet, mucha de la información que obtienen es a través de redes sociales, al subir fotos, mantener su perfil de Facebook en modo público o publican constantemente fotografías con sus familiares, donde viven, cantidad de hijos, escuelas de los menores, placa de su vehículo, entonces uno mismo publica sobre su información que puede ser obtenida por determinadas personas y puede ser mal utilizada. Por ello, si no se tiene conocimiento de los riesgos antes de, quizá sea poco o nada lo que uno puede hacer desde su esfera para ayudar a prevenir esta clase de delitos.

3.2.2.2. Análisis de las entrevistas al efectivo policial de la DIVINDAT

OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.

1. ¿Considera que la DIVINDAT cuenta con los recursos logísticos suficientes para atender las denuncias a nivel nacional?

Jiménez (2020) señaló que cuentan con dos departamentos en investigación de delitos informáticos y una sede en Arequipa. La DIVINDAT en temas logísticos a nivel nacional

no se abastece, motivo por el cual existen las DIRINCRI, estas son unidades de departamentos que investigan casos de menor complejidad. Asimismo, las unidades en mención fueron capacitadas por la DIVINDAT mediante charlas y orientaciones sobre delitos informáticos. Cabe resaltar que la DIVINDAT es una Unidad Especializada con competencia para la recepción y orientación de ciudadanos sobre las denuncias vinculadas a delitos informáticos porque las víctimas suelen apersonarse a la institución por denuncias que no corresponden. Por lo mismo, se debe promover la difusión de los delitos en específico que atiende la DIVINDAT.

2. ¿Cuál es el procedimiento para la atención de una denuncia interpuesta en provincia por la comisión de un presunto delito informático?

En palabras de Jiménez (2020) las diligencias son las siguientes, una vez que toma conocimiento la DIRINCRI o la Comisaria de la jurisdicción de provincia, se comunica la denuncia al Ministerio Público pronunciándose mediante una Resolución Fiscal, los mismos que determinarán si se llevará el caso en la misma sede donde se realizó la denuncia primigenia o se trasladará a la DIVINDAT de Lima a fin de continuar con las diligencias correspondientes; estas son, manifestaciones, pericias y obtención de información de fuentes abiertas con el propósito de esclarecer el hecho denunciado, entre otras.

OE_1: Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

3. ¿A qué se debe el incremento anual de los delitos informáticos?

Jiménez (2020) comentó que desde el año 2000 el uso de la internet se empezó a masificar y los bancos financieros empezaron a perfeccionar sus sistemas informáticos e implementaron aplicaciones de seguridad, entre ellas, las bancas móviles con el propósito de brindar mayores facilidades a los usuarios. Sin embargo, las personas comenzaron a utilizar dichas herramientas sin haber realizado un previo estudio sobre las políticas que brindan los servicios de la internet, siendo muchas veces víctimas de los ciberdelincuentes. Asimismo, los delitos más usuales son los fraudes informáticos.

4. ¿Considera usted que el Fiscal actualmente se encuentra capacitado para investigar plenamente los delitos informáticos?

El efectivo policial Jiménez (2020) dijo que los fiscales no están capacitados en delitos informáticos por la inexistencia de una Unidad Especializada. Por esta razón, la DIVINDAT solicita y recomienda que se implemente una Fiscalía Especializada en Ciberdelincuencia, con la finalidad de que los fiscales tengan el pleno conocimiento sobre esta materia y por ende se lleve una mejor investigación para esclarecer los hechos denunciados. Asimismo, el tema de la burocracia en el Perú hace que todo sea más lento al no contar con información directa del banco o de otra índole relacionado con los delitos informáticos seguirá generando retrasos en el esclarecimiento de hechos y con el pasar del tiempo la confianza de la población.

5. ¿Considera usted la necesaria implementación de Fiscalías Especializadas en Ciberdelincuencia?

Jiménez (2020) planteó que es necesario entablar una misma comunicación y contar con conocimientos básicos de informática. Estos delitos se realizan mediante la investigación en dispositivos electrónicos u otros medios informáticos que coadyuven a dar con la ubicación de los responsables. En ese sentido, ante la complejidad de estos delitos se necesita implementar Fiscalías Especializadas en el menor tiempo posible.

OE2: Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

6. ¿Cuáles son los delitos informáticos más recurrentes en la DIVINDAT durante el 2020?

Jiménez (2020) refirió que durante el año 2020 los delitos más recurrentes fueron, fraude informático, contra el patrimonio, lo que se materializa en las transferencias bancarias, compras por internet sin autorización, clonaciones de tarjetas y delitos de pornografía infantil, así como el acoso a menores de edad, el grooming, el enamorado ficticio a través de internet, el ransomware, las transferencias ilícitas, el phishing y vishing. Por ello, la importancia de la cultura informática en los usuarios siempre será la clave para evitar ser potenciales víctimas de los ciberdelincuentes.

7. ¿Alguna sugerencia o recomendación que desee agregar?

Jiménez (2020) postuló que la recomendación final es verificar la procedencia de los mensajes que son enviadas por las entidades financieras o comerciales y evitar difundir los datos personales, claves de tarjetas de créditos o códigos token, dado que este último

es como la llave de una casa, si uno brinda más de lo debido podría convertirse en una víctima más de estos delincuentes.

Asimismo, el rol de los padres es importante en la medida que los vigilen, debe existir una constante comunicación y confianza con los hijos, porque el peligro no solo se vive en un mundo real, sino también de manera virtual y muchas veces puede tener el mismo o un peor impacto en el menor y familiares más vulnerables.

Finalmente, evitar hacer publicaciones de índole personal en redes sociales (fuentes abiertas) porque los delincuentes cibernéticos están siempre en la búsqueda de incautas, es decir personas que hacen pública su vida sin medir las consecuencias de sus actos.

3.3. Resultados del análisis de la doctrina

Conforme al desarrollo de la investigación se integraron datos de suma relevancia en cuanto a múltiples aspectos doctrinarios. Es de entender que para un correcto análisis se creyó pertinente incorporar dos tablas con la descripción de las ideas principales sobre el tema objeto de análisis en concordancia con los objetivos de la presente investigación, se consideró a la doctrina internacional como primera tabla, mientras que la doctrina nacional se presentó en la segunda tabla, de acuerdo al siguiente detalle:

Tabla 11

Resultados de los análisis de la doctrina internacional

País	Autor	Año de publicación	Ideas principales
Colombia	Posada	2019	El problema de la capacitación y especialización a los fiscales aún persiste debido a la constante rotación de un despacho a otro.
Colombia	Cortes	2015	La constante preparación y capacitación de fiscales y jueces ha sido insuficiente, por ello es necesario la implementación de fiscalías especializadas y contar con el apoyo de personal que facilite las herramientas suficientes para estos casos.
España	Meza	2017	La delincuencia mediante el uso de las TIC seguirá en aumento y el tratamiento será complejo, razón por la cual es necesario reforzar la actuación del Ministerio Fiscal.
Ecuador	Prieto y Vargas	2020	Actualmente Ecuador carece de fiscalías especializadas, siendo la Unidad de Patrimonio Ciudadano el encargado de tramitar los delitos informáticos. La falta de personal especializado genera retraso ante la complejidad de los casos.
Ecuador	Marchal	2016	La necesaria formación y preparación a los jueces sobre las nuevas tecnologías, lo cual permitirá que cuenten con los conocimientos mínimos para enfrentarlos y luchar contra esta clase de delitos.

Argentina	Ministerio Público Fiscal de la Provincia de Salta	2020	El procurador de la provincia de Salta, Abel Cornejo, señala que notó desamparo en la investigación de ciberdelitos. No obstante, con la creación de la Fiscalía e inserción de personal especializado en informática y criminalidad se logró un mejor tratamiento de los casos de ciberdelitos.
Uruguay	Jackson y Scrollini	2020	Ante la ausencia de Fiscalías y Juzgados Especializados, se dispuso la implementación de un grupo para la elaboración de un protocolo para la actuación del Estado ante los ciberdelitos.
México	Vásquez	2019	La escasez de los órganos especializados en el tratamiento de los delitos cibernéticos y la deficiente capacitación son los problemas que actualmente adolece el país mexicano.
España	Organización Internacional de Policía Criminal – Interpol	2021	Los ataques cibernéticos desconocen frontera y su evolución es imparable. Los ciberdelincuentes perfeccionan sus ataques a gran escala y el rol de la policía debe ser combatir los posibles daños a la sociedad.

Fuente: Elaboración propia a partir de los resultados obtenidos.

Del presente cuadro de análisis de la doctrina internacional, podemos inferir que Colombia ha incorporado capacitaciones constantes tanto para los fiscales y jueces siendo hasta la fecha insuficientes, por lo que requieren la implementación de Fiscalías y personal técnico especializados. Por otro lado, ante la ausencia de Fiscalías Especializadas en Ecuador, la Unidad de Patrimonio Ciudadano es el órgano encargado de tramitar los casos de ciberdelincuencia.

Asimismo, en Argentina según lo mencionado por el procurador de la provincia de Salta, Abel Cornejo, ante el abandono en las investigaciones de ciberdelitos, es necesario la creación de Fiscalías y de personal con especialización tanto en informática como en criminalidad a fin de continuar mejorando los procesos de ciberdelincuencia.

Por último, en el caso de España los ataques cibernéticos siguen en aumento constante, por lo que es necesario que los efectivos policiales luchen para combatir los posibles daños a causa de los ciberdelincuentes porque a medida que la tecnología crece, los mismos perfeccionan sus habilidades para evitar sospecha y posterior captura.

Tabla 12

Resultados de los análisis de la doctrina nacional

País	Autor	Año de publicación	Ideas principales
Perú	Díaz	2019	La excesiva confianza de los cibernautas ha permitido el incremento de los casos de ciberdelitos. En ese sentido, la virtualidad requiere responsabilidad de los usuarios porque la

			comisión de estos delitos puede ejecutarse desde cualquier lugar.
Perú	Flores	2018	Ante el aumento de los ataques cibernéticos, el Perú ocupa el quinto lugar en Latinoamérica, afectando a uno de los sectores más importantes esto es, el financiero.
Perú	Morachimo	2019	Podría confundirse la incorporación del Perú al Convenio de Budapest, pues desde su adopción hasta su entrada en vigencia transcurrieron 18 años.
Perú	La Ley	2019	La incorporación más transcendental es la confrontación de los delitos informáticos y los cometidos mediante el uso de la internet, considerando la mejora de las técnicas y cooperación internacional.
Perú	Presidencia del Consejo de Ministros	2019	El Convenio de Budapest busca la protección general ante la evidente desprotección por la ciberdelincuencia, a su vez que sea adaptada a la realidad y siga mejorando en relación a la cooperación internacional.
Perú	Elías	2014	La Policía Nacional de Perú ha logrado la especialización de sus divisiones y de esta forma combatir los delitos informáticos, caso contrario, sucede con el Ministerio Público y el Poder Judicial, por lo que requieren actualizar y especializar al personal dada la complejidad de los casos.
Perú	García	2019	Los ciberdelincuentes poseen aparatos modernos para la realización de estos delitos, conociendo este supuesto y los posibles daños hacia el país, el Estado debería actuar de forma inmediata.
Perú	Herrera	2018	Uno de los obstáculos actuales es la incorrecta adecuación del hecho con el tipo penal y el problema principal es la ausencia de especialización de los fiscales para perseguir esta clase de delitos.
Perú	LP Pasión por el Derecho	2020	No es suficiente la modificación de la Ley de los Delitos Informáticos, sino el factor humano, la integración de fiscales y jueces que permitan el avance integral. Asimismo, la creación de Fiscalías y Juzgados Especializados es totalmente necesario para colaborar con la labor de vienen realizando los efectivos policiales.
Perú	Tenorio	2018	Es necesario que la incorporación de Fiscalías y Juzgados Especializados cuenten con el apoyo de personal calificado para el tratamiento de estos delitos, en paralelo con la cooperación internacional para evitar futuros problemas relacionados a la ciberdelincuencia.

Fuente: Elaboración propia a partir de los resultados obtenidos.

Con la misma lógica, en el caso de la doctrina nacional, podemos advertir que Diaz indica que, el problema de la ciberdelincuencia es por la desmesurada confianza de los usuarios en el uso de la internet, por ello, el ciberespacio es importante en la medida que los

cibernautas sean responsables de su actuar frente a la virtualidad y el avance de la tecnología.

Asimismo, Flores agrega que, el Perú ocupa el quinto lugar en Latinoamérica, tras el incremento de los ciberataques, perjudicando en un nivel significativo al sector financiero y coloca a la sociedad peruana en posible riesgo económico.

A su vez, La Ley menciona que, la incorporación más relevante en los casos de ciberdelincuencia es el mejoramiento de las técnicas digitales y la cooperación internacional, los mismos que serán de utilidad para la atención, tratamiento e identificación de los ciberdelincuentes.

Cabe señalar que Elías resalta los avances de la Policía Nacional del Perú al haber especializado a sus divisiones para combatir el actuar de los ciberdelincuentes, caso contrario, sucede con el Ministerio Público y Poder Judicial, motivo por el cual es necesario la preparación y especialización de todo el personal que coadyuve con el logro de la investigación dada la complejidad de estos casos.

En ese sentido, Tenorio hace hincapié en la necesidad de implementar Fiscalías y Juzgados Especializados, los mismos que cuenten con el personal idóneo para el tratamiento de los delitos informáticos y a la par se refuerce la cooperación internacional con la finalidad de eludir posibles ataques o contingencias vinculados a casos de ciberdelincuencia.

3.4. Resultados del análisis de la legislación

A lo largo del desarrollo del presente trabajo se expusieron las leyes más relevantes en delitos informáticos, desde los proyectos iniciales en el año de 1999 hasta la última modificación de la ley de delitos informáticos realizada en el año de 2014. Se creyó necesario sintetizar la información en tablas para que exista un mejor entendimiento sobre el análisis exhaustivo practicado. El orden plasmado fue siguiendo la tendencia cronológica desde el documento normativo más antiguo hasta el más actual, según se muestra a continuación.

Tabla 13

Proyectos de ley antecesores a la creación de la ley de delitos informáticos

Proyecto de Ley	Fecha de presentación	Título	Autor
Nro. 05071	18/08/1999	Ley de delitos informáticos	Jorge Muñiz Ziches

Nro. 05132	31/08/1999	Informática: Pena delitos informáticos	Susana Díaz Díaz
Nro. 05326	18/10/1999	Código penal: 196 pena manipulación informática transferencia de patrimonio	Anastacio Vega Ascencio
Nro. 4643	02/08/2019	Ley que declara de interés nacional y necesidad pública la creación de la fiscalía especializada en delitos informáticos	Juan Carlos Gonzales Ardiles

Fuente: Elaboración propia a partir de los datos proporcionados por la página oficial del Congreso de la República.

Los tres primeros proyectos de ley presentaron las propuestas iniciales por las que se incorporaron los delitos informáticos al Código Penal, considerando que en esa época nuestro ordenamiento jurídico de 1991 solo regulaba el hurto telemático como agravante del hurto agravado en su artículo 186 en donde se describía el sub tipo penal en tres supuestos, tales como el sistema de transferencia electrónica de fondos, los sistemas de la telemática en general y la violación del empleo de claves secretas.

Con respecto al último proyecto de ley es menester informar que entre los aportes medulares se puedo identificar que la Fiscalía de la Nación contaba con un procedimiento regular establecido en la Ley Orgánica del Ministerio Público, la cual se aprobó mediante el Decreto Legislativo N° 52, el mismo que confiere facultades a la Fiscal de la Nación para que designe a un grupo de fiscales en la intervención especializada de hechos delictivos.

No obstante, se advirtió que la coyuntura exigía un nivel especializado de investigación y para ello era indispensable incorporar medios técnicos y fiscales con formación tecnológica para evitar el mínimo vestigio de impunidad. Es una responsabilidad del derecho la regulación de los delitos que afecten intereses privados o colectivos con mayor grado de lesividad, así como de aquellos que lo ejercen estar a la vanguardia y en concordancia con los cambios de la colectividad.

Indistintamente de la denominación que se le pretenda acuñar a la Fiscalía que sería la responsable de perseguir, identificar y representar a la sociedad en juicio, es innegable que su creación es inminente y simplemente surgió un retraso por parte de las autoridades investidas de las potestades para concretarlo. En respuesta a ello, recientemente se creó una Unidad Fiscal Especializada en Ciberdelincuencia, quien asumió funciones a partir del 15 de febrero del año en curso, dejando muchas dudas en el aire que hasta el momento no han sido esclarecidas.

A pesar de ello, debe elogiarse este primer paso porque representa el inicio de una cadena de logros institucionales contra la delincuencia informática en beneplácito de la sociedad. Con esta investigación no se pretende desprestigiar el intenso y loable trabajo desarrollado por los fiscales que integran nuestro sistema de justicia, sino cuestionar con fundamento las falencias evidenciadas.

Dos de las más evidentes falencias advertidas fueron que dentro de sus atribuciones no se había considerado que esta Unidad se haga cargo de la investigación y tampoco de la persecución de estos delitos, así como de su sustentación en audiencia de juzgamiento y demás etapas procesales. Lo que originó la segunda falencia fue que, al no contar con unidades independientes y autónomas en sus funciones, aumentaremos la carga procesal de nuestros 34 distritos fiscales.

En efecto, países como Argentina han iniciado con unidades consultoras como la propuesta por nuestro país. Sin embargo, las situaciones y los tiempos fueron totalmente distintos porque el país vecino advirtió en su momento que era necesario otorgar un tratamiento diferenciado para los casos vinculados con delitos informáticos, siendo que hasta la fecha esas unidades consultoras se han convertido en unidades detectoras, persecutoras y represoras de la cibercriminalidad organizada.

Tabla 14

Evolución de la ley de delitos informáticos

Ley	Fecha de presentación	Título
Nro. 27309	17/07/2000	Ley que incorpora los delitos informáticos al Código Penal
Nro. 28251	07/06/2004	Ley que modifica los artículos 170, 171, 172, 173, 174, 175, 176, 176-A, 179, 180,181, 182, 183, 183-A, e incorpora los artículos 179-A, 181-A, 182-A a los Capítulos, X y XI del Título IV, del Libro Segundo del Código Penal
Nro. 30096	22/10/2013	Ley de delitos informáticos
Nro. 30171	10/03/2014	Ley que modifica la ley 30096, ley de delitos informáticos.

Fuente: Elaboración propia a partir de los datos proporcionados por la página oficial del Congreso de la República.

En nuestro país se incorporaron los delitos informáticos en el ordenamiento jurídico de 1991, luego de una larga lista de propuestas normativas sobre la necesidad de regular estos delitos, se logró incorporar en el Título V correspondiente a los delitos contra el patrimonio, el delito informático en el artículo 207-A, el delito de alteración, daño y destrucción de base de datos, sistema, red o programas de computadoras en el artículo 207-B y el delito informático agravado en el artículo 207-C.

Es de público conocimiento que la criminalidad informática nunca dejó de perfeccionarse y continuar especializándose en materia tecnológica en menoscabo y detrimento de los bienes jurídicos más preciados de la sociedad. Es por eso que se modificaron una serie de articulados, así como la incorporación de estos en diferentes títulos de nuestro ordenamiento jurídico.

Todo ello sirvió para que tiempo después se creara la ley de delitos informáticos desarrollada en correlato con el Convenio de Budapest, en la cual se detalló la estructura legal de la norma esquematizada ampliamente. La distribución normativa se repartió de tal forma que se abarcaron los sucesos carentes de solución o con una sensación de carencia de justicia, tal y como se muestra a continuación:

Tabla 15

Ley de delitos informáticos

Capítulo	Texto normativo	Tipificación de las sanciones	
Segundo	Delitos contra datos y sistemas informáticos	Art. 2	Acceso ilícito
		Art. 3	Atentado contra datos
		Art. 4	Atentado contra sistemas informáticos
Tercero	Delitos informáticos contra la indemnidad y libertad sexual	Art. 5	Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos
Cuarto	Delitos informáticos contra la intimidad y el secreto de las comunicaciones	Art. 7	Interceptación de datos informáticos
Quinto	Delitos informáticos contra el patrimonio	Art. 8	Fraude informático
Sexto	Delitos informáticos contra la fe pública	Art. 9	Suplantación de identidad
Siete	Disposiciones comunes	Art. 10	Abuso de mecanismos y dispositivos normativos

Fuente: Elaboración propia a partir de los datos proporcionados por la Ley N° 30096 – Ley de delitos informáticos.

Ahora bien, una de las propuestas más interesantes en el Convenio sobre la Ciberdelincuencia fue lo puntualizado en el artículo 35 sobre la Red 24/7, en el Perú contamos con la Unidad de Cooperación Judicial Internacional y Extradiciones que viene realizando un buen trabajo siguiendo la línea trazada por el Convenio en el sentido de

abastecer de herramientas que faciliten la confrontación de los delitos que traspasen los límites geográficos. En sencillo, viabilizan que nuestras autoridades puedan ser asistidas por sus semejantes en otros países cuando se requiera practicar diligencias en el exterior.

Tabla 16

Ámbito de acción de la Unidad de Cooperación Judicial Internacional y Extradiciones

Libro séptimo	Definición
Extradición	Es la figura jurídica en la cual un Estado entrega a una persona a otro Estado con el propósito de someterse a una investigación, persecución y juzgamiento por la presunta comisión de un hecho delictivo en su territorio.
Asistencia judicial internacional	Es el intercambio de información relevante y la realización de diligencias en el exterior, según las solicitudes emanadas por los jueces o fiscales de diversos Estados.
Traslado de condenados	Es el traslado de un interno que está cumpliendo condena en un Estado determinado para que sea trasladado al Estado del cual es nacional por motivos resocializadores.
Exhorto consular	Es la toma de declaración de un ciudadano peruano en el extranjero, debiendo permitir el país notificado acceder al pedido.
Oficina de recuperación de activos	Es la asistencia mutua en la identificación, el rastreo, la inmovilización, la confiscación y el decomiso de bienes obtenidos o derivados de la comisión de actos delictivos y de los bienes utilizados en dichas comisiones o del producto de dichos bienes.

Fuente: Elaboración propia a partir de los datos proporcionados por la Unidad de Cooperación Judicial Internacional y Extradiciones

Hay un notable avance en cuanto a la adaptación de nuestros órganos institucionales a los convenios internacionales, eso demuestra un enorme compromiso con la sociedad en la lucha constante por la paz mundial. Sin embargo, queda pendiente repotenciar nuestro sistema de justicia, empezando por convertir a nuestras Fiscalías y Juzgados en órganos especializados para el desarrollo de un proceso judicial garantista.

En síntesis, de los resultados obtenidos en el análisis documental, las entrevistas, la doctrina internacional y nacional, así como de la legislación nacional, se detectó que nuestro sistema de justicia vigente resulta inapropiado para realizar el procesamiento de la comisión de los delitos informáticos normados en la Ley N.° 30096 y la Ley N.° 30171, así como los delitos informáticos regulados desde el artículo 207-A al 207-C del capítulo X del Código Penal.

Asimismo, se descubrió que la ausencia de un Juzgado Especializado en Ciberdelincuencia impide que se administre justicia de una forma óptima, considerando que no es suficiente

con integrar una Fiscalía Especializada en Ciberdelincuencia sin que también exista un correlato en el órgano que impartirá justicia, es cierto que los jueces según el Código Procesal Penal del 2004 no se encargan de la instrucción, pero no es menos cierto que en juicio es igual de importante dominar perfectamente los términos que sostendrán las partes durante la audiencia, tener claro el panorama y el modo en que deberá valorarse la prueba digital en todas sus manifestaciones.

Queda claro con base en los resultados que es insuficiente la consultoría que brindará la Unidad Fiscal Especializada en Ciberdelincuencia, teniendo en cuenta que los delincuentes nos llevan la delantera desde hace más de dos décadas, según la doctrina internacional, los países que ratificaron el Convenio de Budapest tiene las puertas abiertas en emular los criterios adoptados en países como Argentina, reforzando los niveles de cooperación internacional, priorizando la volatilidad de la prueba, lo pluriofensivos que resultan estos delitos y la ubicación transnacional de los presuntos delincuentes informáticos.

CAPÍTULO 4. DISCUSIONES Y CONCLUSIONES

4.1. Discusiones

4.1.1. Limitaciones

Al haber logrado el desarrollo de los capítulos precedentes, conviene describir el apartado de las limitaciones en función de las hipótesis plasmadas durante el estudio y análisis del presente trabajo de investigación. Principalmente en dos vertientes, la primera relacionada a los límites que tuvimos que afrontar desde nuestra posición como autores, destacando la limitación teórica, la viabilidad de las fuentes, los recursos económicos y la limitación temporal. La segunda vertiente se vincula a las limitaciones propias de la investigación, entre los más relevantes podemos mencionar el contexto de la población, los recursos humanos y la circunscripción geográfica, los cuales se expusieron en los siguientes párrafos.

4.1.1.1. Limitaciones de los autores

Sobre la limitación teórica corresponde comentar que la literatura en el ámbito nacional fue escueta, ya que el cibercrimen a pesar de ser un delito añejo, en nuestro país recibe un tratamiento que demuestra poca importancia por nuestros legisladores. Sin embargo, los autores con el ánimo de promover la novedad de la investigación en cuanto a las últimas decisiones adoptadas por los países referentes en esta materia, se logró extraer valiosos testimonios de especialistas nacionales e internacionales, abarcando países como Argentina, España, Colombia y Ecuador, lo cual constituye una fuente documental directa y enriquecedora para el desarrollo del presente trabajo.

En relación a la viabilidad de las fuentes obtenidas se puede resaltar que gran parte de la información se encuentra contenida en los repositorios de las universidades nacionales y extranjeras, en las revistas e informes más rigurosos, así como en tiendas virtuales en las que se ofrece la venta de ebooks, también conocidos como libros digitales, electrónicos y ciberlibros. No obstante, hubiese sido esplendido revisar libros físicos relacionados a la materia objeto de esclarecimiento y análisis, de este modo se habría logrado visitar las bibliotecas más importantes del país.

En lo correspondiente a la limitación de los recursos económicos se detalla que, al no haber conseguido el reporte de los 34 distritos fiscales a nivel nacional, se proyectó un viaje a Tumbes para recabar la información sobre los delitos informáticos atendidos

desde el año 2015 hasta el 2020, siendo imposible concretarse por causa de la covid-19, la imposibilidad de realizar viajes y lo improbable que resultaba ingresar a tal distrito fiscal. A pesar de ello, los resultados obtenidos fueron óptimos y lograron mitigar la ausencia de la data restante.

En lo que respecta a la limitación temporal se expresa que el curso taller de titulación cuenta con una duración de 8 semanas para la presentación del producto final, a simple vista el plazo es menudo, pero no imposible de ejecutar con un adecuado cronograma de aplicación, tal y como se desarrolló en el presente trabajo de investigación. Es así que los autores, empezaron con la elaboración del plan de tesis con meses de antelación, siguiendo el conducto regular para lograr concretar las entrevistas con los ponentes internacionales y nacionales, así como para la obtención de los documentos por parte del Ministerio Público y Poder Judicial, los cuales fueron analizados en el apartado de resultados y serán discutidos en el acápite de interpretación comparativa.

4.1.1.2. Limitaciones de la investigación

En cuanto al contexto de la población, una de las principales limitaciones para realizar las entrevistas fue el rechazo liminar de los jueces por tratarse de temas comprometedores derivados de la falta de especialización y preparación en los temas vinculados a la ciberdelincuencia, y sobre la respuesta por parte de ellos ante la ausencia de Juzgados Especializados. Razones por los cuales, algunos jueces se negaron a brindarnos dichas entrevistas y en otros casos, no se logró obtener respuesta afirmativa que coadyuve a nuestro tema de investigación.

En lo referido a los recursos humanos, se puede mencionar la respuesta tardía de una especialista nacional en ciberdelincuencia, quien indicó que, por un tema de tiempo o por el estado de emergencia producido por la COVID-19, desafortunadamente, nos respondió el correo electrónico de invitación a la entrevista durante la etapa final de la redacción de la tesis, esto es, después de 60 días de espera, considerando que estamos contra el tiempo por el plazo de presentación de los entregables semanales, la rigurosidad de la información obtenida y la fecha de entrega final, no se pudo concretar la reunión pese a nuestra constante insistencia a través de los medios de comunicación electrónicos.

Continuando con las limitaciones surgidas durante la investigación, corresponde explicar sobre el acceso al lugar en el que se encontraban los encuestados elegibles,

porque tras el inicio de la pandemia nos vimos indispuestos a llevar a cabo dichas encuestas, a fin de evitar el contacto directo con la población que se pensaba encuestar y así garantizar nuestra salud. En ese sentido, con el propósito de brindar información transparente e irrefutable, se descartó el registro de datos o muestras mediante el uso de encuestas virtuales, puesto que no genera convicción o certeza de la información y es susceptible de manipulación, motivo por el cual no se incluyeron las encuestas como instrumento de recolección de datos.

4.1.2. Interpretación comparativa

La interpretación comparativa comprende la discusión de los resultados en sus 4 enfoques, estos son, el análisis de las entrevistas, los documentos, la doctrina y la legislación. Este apartado permitió que se puedan interpretar los hallazgos con los estudios antecesores, así como la interconexión con los objeticos y las hipótesis de la investigación; y la integración de las ideas críticas propuestas por los autores en beneficio de la comunidad jurídica, tal y como se muestra a continuación:

OG: Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos.
HG: El Sistema de Justicia del Perú resulta inapropiado para procesar los delitos informáticos, en la medida que carece de Fiscalías y Juzgados Especializados en Ciberdelincuencia.

Sobre el sistema de Administración de Justicia del Perú

Con base a los resultados obtenidos se pudo encontrar que, el MINJUS (2020) presentó un diagnóstico a nivel multisectorial sobre el estado de la delincuencia informática en el que se concluyó que las capacidades y conocimientos con los que cuentan los interventores principales de nuestra Administración de Justicia son insuficientes, en la medida que el trabajo debe ser copulativo e involucrar a las tres instituciones estatales con el mismo nivel de especialización, lo cual en la práctica es desproporcional porque solo contamos con una división policial involucrada directamente en la persecución por delegación de esta clase de investigaciones, mientras que el Ministerio Público y el Poder Judicial, mantienen una postura restrictiva y continúan apostando por cursos, talleres y seminarios esporádicos, creyendo erróneamente que es la solución idónea.

Esta idea sigue la noción cognoscitiva de Lamperti, Rincón y Temperini (2020) cuando mencionan que una solución oportuna sería emular a los países de la región en cuanto a la incorporación de Fiscalías Especializadas, pero teniendo en consideración que no basta

con su creación y centralización en la ciudad capital, sino que debería implementarse progresivamente en todos los departamentos del país, pues es lógico que la idea no se trata de recargar de trabajo, congestionar la carga y evitar contribuir con la celeridad procesal que es el anhelo de todos los ciudadanos, por el contrario se busca brindar soluciones inmediatas por medio del personal especializado y con los recursos tecnológicos más sofisticados para tal fin.

En sentido contrario, los doctores Carretero, García y Acurio (2020) sostienen que la solución está vinculada a las capacitaciones, empero haciendo la salvedad de que no todo debe estar centrado al campo teórico, pues es igual de importante el campo práctico, principalmente porque los fiscales encargados de esa labor deben empezar por tener clara la idea de cómo deben investigar sus casos, pues las propuestas de diligencias a nivel preliminar son determinantes al igual que la conservación de la prueba digital por su volatilidad y el manejo de las herramientas tecnológicas, así como los mecanismos de colaboración 24/7, vitales para la identificación del presunto criminal informático.

Esta situación pude verse reflejada en los resultados de las investigaciones realizadas por el persecutor penal no especializado, en los distritos fiscales de Lima, Lima Sur, Lima Norte, Lima Noroeste y Lima Este, lo cual arrojó un total de 10 731 casos registrados desde el año 2015 hasta el 2020, indicándose claramente que 10 611 casos fueron archivados por distintas razones, pero todas ellas vinculadas a propuestas de investigación fiscal deficientes y solo 120 fueron sentenciados, lo cual a todas luces muestra que nuestro actual sistema de justicia resulta inapropiado para el procesamiento de estos delitos.

Una idea distinta a las expuestas anteriormente fue desarrollada por el Dr. Maza (2020) al señalar que una solución eficaz y trascendente es el uso correcto de los medios tecnológicos, tanto los jueces como los fiscales tienen serios problemas en el manejo y dominio de programas tan básicos como los procesadores de datos e información. En esa misma línea, el Dr. Guerrero (2020) refiriere que, si bien se realizó la distinción conceptual entre los delitos informáticos y los delitos patrimoniales mediados por la tecnología, el problema persiste al no corregir sustancialmente la deficiencia en cuanto al manejo de estas herramientas.

Los doctores Elías y Cuadros (2020) apuestan por repotenciar los conocimientos teórico prácticos del tratamiento de la evidencia digital, esto es, desde la obtención, la custodia y la conservación hasta la etapa de juzgamiento, en donde se actuará como medio probatorio. Con lo que se incrementaría la satisfacción de la sociedad afectada por este

delito pluriofensivo, lo que se expresaría en el cuadro de personas condenadas por estos delitos, los resultados no reflejan la verdadera situación en la que vivimos, pues desde el año 2016 hasta el 2020 solo se condenaron un total de 392 casos de delitos informáticos y 48 casos de delitos contra el patrimonio regulados en los artículos 185 al 208 del Código Penal.

En relación al procesamiento de los delitos informáticos

Nuestros referentes internacionales, entre ellos los doctores Carretero, Lamperti, Migliorisi y Acurio (2020) coinciden en que el problema medular durante el procesamiento de los delitos informáticos estuvo relacionado al tema probatorio, específicamente a la evidencia digital, pero habría que precisar que no basta con evitar nulidades contra este medio probatorio, sino que es necesario que se puedan identificar a los presuntos responsables, su ubicación geográfica y su extradición al país en el que se cometió el delito para ser investigado y juzgado conforme a las normas vigentes. De no ser así, la investigación preparatoria no se formalizará o en el mejor de los supuestos, la causa termina desestimándose por insuficiencia probatoria.

En oposición a la postura predecesora, los doctores Herrera (2018) y Rincón (2020) discrepan con sus colegas y exponen que el motivo que obstaculiza un adecuado procesamiento de estos delitos se ubica en la raíz de la investigación fiscal, esto es, en la tipicidad. Dicho de otro modo, es la coincidencia entre el resultado de la corroboración del hecho real y lo descrito en el tipo penal. Un caso elegible para ejemplificar un hecho concreto es cuando un sujeto clona una tarjeta de débito o crédito y erróneamente se subsume el hecho al tipo penal de clonación de tarjetas, cuando debió investigarse por vulneración de datos personales.

Una postura que no pretende estar a favor o en contra de las ideas esgrimidas en los párrafos anteriores es la postulada por el Dr. Temperini (2020) cuando reflexiona diciendo que en Latinoamérica existe una cifra negra bien marcada de casos que no fueron investigados o en el peor supuesto, las personas no interpusieron denuncias porque perdieron la confianza en el sistema y conocen que de haberlo realizado no hubiesen obtenido un mínimo de eficacia.

Desde una óptica vinculada a los policías cibernéticos y el procesamiento de los delitos informáticos, el Dr. Elías (2014) refiere que en nuestro país una de las pocas instituciones en lograr un paso agigantado en especialización fue la División de Investigación de

Delitos de Alta Tecnología, lo cual trajo una serie de resultados positivos en favor de la sociedad que fue o será víctima de esta clase de delitos, entre los más destacables podemos seleccionar la claridad y seguridad que ha logrado en el pensamiento de la gente y la recuperación de la confianza en denunciar con la convicción de que el resultado los beneficiará.

En relación a las medidas que debe adoptar el Estado para una investigación eficiente

Se plantearon múltiples propuestas desde la experiencia internacional sobre los cambios que debería realizar nuestro país para fortalecer las investigaciones y pasar de un nivel de desconcierto a uno con certeza y eficiencia. Para ello, Temperini y Carretero (2020) explican que la investigación en sede policial o fiscal en ningún supuesto debe vulnerar o restringir derechos sin autorización expresa, porque de no ser así el proceso judicial puede ser objeto de nulidades que en su conjunto impedirán su continuación. Además, los especialistas mencionan que hay desaciertos al momento de proponer las pericias que deberían practicarse, para eso se debe capacitar sobre los puntos de pericias que deben solicitarse para aprovechar al máximo los dispositivos incautados.

Desde una perspectiva diferente, García (2020) propone que se debe repotenciar la comunicación entre países a efectos de obtener una respuesta inmediata sobre el paradero de los presuntos responsables o de cualquier vestigio que permita avanzar con el decurso de la investigación. Asimismo, en la medida que estamos en un mundo de constante evolución tecnológica y que el derecho no puede verse superado por la realidad es necesario que se incorporen reformas procesales en el ordenamiento jurídico que contenga normas obsoletas o inaplicables, de ser necesario, en favor de lograr una investigación eficiente.

El Dr. Migliorisi (2020) postula que una de las falencias persistentes está relacionada a la infraestructura y logística con la que cuenta nuestro sistema de administración de justicia, en sus tres principales representantes, estos son, el Poder Judicial, el Ministerio Público y la Policía Nacional del Perú – DIVINDAT. Ante ello, se debería invertir en mejores herramientas tecnológicas, suscribir acuerdos de colaboración con los representantes de las redes sociales más poderosas del mundo como Facebook, Instagram, WhatsApp y YouTube, para acceder a la información de las cuentas de los presuntos responsables.

Desde otro parecer, los doctores Acurio y Rincón (2020) refieren que debemos impulsar la incorporación en los planes escolares y universitarios, diversos programas de formación en el uso seguro de las tecnologías para evitar posibles ataques cibernéticos. Está claro que no se logrará erradicar la comisión de este delito, pero se podrá concientizar a la población en general sobre el uso responsable de las tecnologías de la información y comunicación.

Por su lado, el Dr. Elías (2020) insiste en que debe aminorarse el tiempo de respuesta por parte del Ministerio Público con base al principio de diligencia fiscal, dado que, en la práctica, entre la presentación de la denuncia y la emisión de la primera disposición fiscal puede tomar 28 días en el mejor de los supuestos y en el peor escenarios 290 días. Por otro lado, Cuadros (2020) resalta que se tiene que destinar un presupuesto adicional para no solo crear un Fiscalía Especializada en Cibercrimen, sino la creación de un subsistema especializado en la materia emulando los excelentes resultados que hemos evidenciado con los subsistemas previamente incorporados como en los delitos de Crimen Organizado y Corrupción de Funcionarios.

OE_1: Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.
HG_1: La ausencia de las Fiscalías Especializadas en Ciberdelincuencia incide negativamente en los actos de investigación fiscal, imposibilitando una representación idónea y generando un estado de indefensión de las víctimas y de la sociedad.

En lo que respecta a los archivos de las investigaciones fiscales

Es asombroso lo que se puede encontrar en los fundamentos de los archivos de las investigaciones en etapa preliminar. En palabras de Elías (2020) el principal fundamento radica en que no se cuenta con los datos suficientes para identificar a los presuntos autores de los hechos materia de disputa, lo cual no resulta lógico porque se le estaría exigiendo al agraviado o la persona que realiza la denuncia una condicionante, esta es, en caso no nos brindes elementos probatorios suficientes para identificar al agresor, archivaremos la causa. Lo más alarmante según nuestro referente es que la gran mayoría de propuestas de diligencias fueron planteadas por la parte agraviada.

Lo anterior puede ser reforzado con los reportes fiscales desarrollados en los resultados de la presente investigación, los mismos que describen que desde el año 2015 hasta el 2020, 1954 causas representaron un total de 31.1 % de los casos evaluados, los cuales concluyeron en la etapa de calificación de la denuncia. En esa línea temporal, 4017 casos

que representan el 64 % fueron archivados en la etapa de investigación preliminar y solo 104 de 6274 casos llegaron a etapa de juzgamiento.

Haciendo un paragón con el parágrafo anterior, desde el año 2016 hasta el 2020 solo en 392 casos se emitieron sentencias condenatorias por delitos informáticos regulados en la Ley N° 30096 y en el mismo lapso se emitieron sentencias condenatorias en 48 casos por delitos contra el patrimonio regulados en el Título V del Código Penal. Entonces, es lógico pensar que por errores cometidos en la etapa de investigación gran parte de los casos son archivados y los pocos que llegan a juicio podrían correr con la misma suerte porque hay carencias en cuanto a la especialización y los conocimientos técnicos de los jueces que resuelven la causa.

En palabras de los autores, es notable los esfuerzos que se han realizado hasta el momento, entre los más resaltantes, la incorporación de un marco normativo integral, una órgano consultor y recopilador de información, pero seguirán siendo insuficientes en la medida que las investigaciones en etapa preparatoria no se refuercen con personal especializado tanto en la persecución del delito como en la representación en juicio.

Además, es necesario que cuenten con una cantidad razonable de peritos en cibercrimen y con asistentes en función fiscal que cuenten con un nivel de especialización deseable en la materia. Lo propio deberá realizar el Poder Judicial para estar a la altura de la situación, pues de qué sirve todo ello, si al momento de valorar los medios probatorios, no se cuenta con el conocimiento suficiente para despejar la duda razonable al momento de resolver la causa.

En lo correspondiente a la ausencia de Fiscalías Especializadas en Ciberdelincuencia

Según la opinión de la DIVINDAT representada en esta oportunidad por el efectivo policial Jiménez (2020) sostiene que la comunicación entre las instituciones que conforman el Sistema de Justicia debe ser la misma, también resalta que indistintamente de la posición que ostenten, todos deben contar con conocimientos en informática. Los doctores Elías y Guerrero (2020) concuerdan en que la capacitación en el uso de herramientas informáticas es determinante, ya que dentro de la diversidad de formas de obtener información está la búsqueda de fuente abierta OSIM y no puede pasar por desapercibido el modo de obtención y seguramiento de la prueba digital. Ambos coinciden en que deben implementarse Fiscalías por la complejidad que demanda la atención de estos casos.

Por el contrario, el Dr. Cuadros (2020) expone que nuestra actualidad exige que no solo los jueces, fiscales o policías cuenten con conocimientos especializados en tecnología, sino que en ese grupo también estén los abogados que ejercen la defensa privada, defensores públicos y la ciudadanía en general, este último en menor intensidad cognoscitiva. A su vez, agrega que podremos estar en iguales o superiores condiciones frente a los ciberdelincuentes con la incorporación de una Fiscalía Especializada, dado que se obtendrán mejores resultados a corto y mediano plazo en cuanto a las investigaciones y se trasladará un mensaje positivo y de confianza a la sociedad.

La ausencia de estas Fiscalías Especializadas causó un grado significativo de desprotección de las víctimas en nuestro país, según la declaración de Tenorio (2018) y LP Pasión por el Derecho (2020) cuando mencionan que es medular el factor humano especializado tanto a nivel fiscal como judicial puesto que permitirá alcanzar un avance integral. Al igual que en nuestro país, en México, Vásquez (2019) refiere que también existe escasez de entidades especializadas para el adecuado tratamiento de estos delitos.

En Uruguay, Jackson y Scrollini (2020) sostienen que se adoptó una medida temporal ante la ausencia de las Fiscalías y Juzgados, esto fue la implementación de un sector que priorizó la creación de una serie de protocolos en los que se desarrollaron recomendaciones para el Estado y el modo en que deben enfrentar al cibercrimen. Por su lado, Prieto y Vargas (2020) comentan que la ausencia de estas Fiscalías otorga impunidad a los ciberdelincuentes en la medida que en cuestión de investigación llevan la delantera y la única manera de contrarrestarlos es contando con aparatos tecnológicos de primer nivel operados por fiscales y colaboradores especializados en tecnologías de la información y comunicación.

En síntesis, es idóneo incorporar órganos especializados para la atención de delitos informáticos, la tecnología continúa avanzando constantemente, así como los delincuentes que la utilizan para causar un daño al patrimonio de las personas, cada día logran una mayor sofisticación, la idea de generar alianzas con los hackers, quienes son totalmente distintos a los crackers como se explicó al inicio de la investigación, sería una idea novedosa y traería buenos resultados en cuestiones tan relevantes como la ubicación del ordenador o dispositivo en donde se estaría cometiendo el presunto hecho ilícito penal, el paradero de los presuntos responsables y demás información que con los conocimientos sofisticados con los que cuentan nos podrían brindar.

Sobre la incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia

De la información recogida, el Ministerio Público señala mediante la Resolución de la Nación N.° 1503-2020-MP-FN que la incorporación de la UFEC atenderá casos realizando su labor como órgano informativo y consultor, sin embargo, la población está en desacuerdo debido al tiempo de espera que tomó su creación, también por las limitadas funciones que desempeñará, y sobre todo por la recarga de casos a los fiscales comunes con temas ligados a delitos informáticos. En contraposición al párrafo anterior, La Unidad Fiscal Especializada en Ciberdelincuencia de Argentina incorporó dicho órgano con la finalidad de atender puntos principales de toda investigación, tales como la detección, persecución y represión de la criminalidad organizada.

En tal sentido, al analizar el presente resultado, podemos inferir que la implementación de la UFEC permitirá que las demás Fiscalías trasladen consultas ligadas a la ciberdelincuencia, siendo un avance para la sociedad. No obstante, el tiempo juega un rol importante porque los ciudadanos esperan que los órganos de la Administración de Justicia se pronuncien en la medida de los acontecimientos negativos que suceden en la realidad y esperan que dichas medidas adoptadas sean óptimas para salvaguardar tanto los intereses personales como colectivos. Por ello, es hora de rescatar los aciertos de los demás países vecinos e intentar perfeccionarlos, como en este caso, el país de Argentina y la incorporación de Fiscalías Especializadas actuando como un órgano completo, esto es, desde la etapa de investigación hasta la etapa de juzgamiento.

Bajo esa misma lógica en el ámbito internacional, los doctores Carretero, García, Lamperti, Migliorisi y Temperini (2020) llegaron a concluir que la incorporación de las Fiscalías Especializadas en Argentina lograron encausar los procesos, se mejoraron los niveles de atención de los denunciantes, se esclarecieron las diferencias entre la evidencia física y digital, así como el perfeccionamiento en el tratamiento de los procesos, la identificación de los casos que requieren una atención inmediata y el lugar donde sucede frecuentemente esta clase de delitos. Asimismo, agregan la importancia de conocer el lugar donde las víctimas pueden denunciar y medularmente contar con el personal especializado que permita un mayor grado de cooperación nacional e internacional.

Esto quiere decir que, la implementación de Fiscalías Especializadas permitió un avance significativo en cuanto al mejoramiento de las investigaciones, poder diferenciar términos para que posteriormente el personal tenga el pleno dominio del tema en cuestión, así como brindar un mejor trato y atención a las víctimas de los ciberdelincuentes pudiendo obtener una estadística o balance en cuanto a la comisión de estos delitos intensifica la necesidad

en la incorporación de Fiscalías Especializadas en Ciberdelincuencia a fin de luchar contra el aumento desmedido de los ciberataques.

Frente a lo mencionado los especialistas, Rincón, Maza, y Acurio (2020) refieren que pese a la ausencia de Fiscalías Especializadas en Ciberdelincuencia consideran necesario que se implementen a corto plazo, porque la dinámica de los ciberdelincuentes obliga a que las autoridades actúen con un nivel superior de asertividad y trabajen de forma conjunta; y sobre todo logren una recolección de la evidencia digital de forma más segura, evitando posteriores nulidades por el modo de obtención de las mismas y salvaguardando su actuación en juicio.

De lo señalado en el párrafo anterior, podemos advertir que la necesidad de implementar Fiscalías Especializadas no es un tema ajeno a la realidad, puesto que, el incremento de los ciberataques cada vez es mayor y la demora de los Estados hace que los ciberdelincuentes sigan perfeccionando sus actuaciones delictivas dejando atrás a los fiscales provinciales carentes de especialización en delitos informáticos, por ello, la creación de Fiscalías, el trabajo en conjunto y continuo permitirá desarrollar una mejor labor en relación a la custodia de la evidencia digital, caso contrario, la demora en recabar la evidencia posibilita que se diluya o pierda certeza.

Seguidamente en lo examinado por los especialistas nacionales, Guerrero, Elías y Cuadros (2020) concuerdan en que la creación de la Unidad Fiscal Especializada es un gran acierto en función al alcance del presupuesto. A pesar de que inicialmente asumió el rol de órgano mentor y solo se dedicará a conocer la data sobre los lugares de mayor incidencia de los delitos informáticos, sin embargo, son supuestos que siguen siendo insuficientes ante el constante crecimiento de los ciberataques.

Se colige que, la reciente incorporación de la UFEC permitirá algunos avances vinculados a la absolución de consultas y ligados al traslado de información, siendo supuestos que coadyuvarán de una u otra forma a las demás Fiscalías Especializadas. No obstante, este progreso es poco significativo en comparación con el avance de los ciberdelincuentes. Por ello, se debe continuar insistiendo a nuestras autoridades para que en poco tiempo se llegue a incorporar una Fiscalía Especializada como tal, esto es, cumplimiento el rol de representar a la sociedad durante todo el proceso judicial y prejudicial.

OE_2: Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

HG2: La inexistencia de los Juzgados Especializados en Ciberdelincuencia inciden negativamente al valorar y resolver con base a los medios probatorios aportados por las partes, afectando la predictibilidad de las resoluciones judiciales y el equilibrio del Sistema de Justicia del Perú.

Respecto a la ausencia de Juzgados Especializadas en Ciberdelincuencia

Se recabó data que demuestra una vez más la minoritaria cantidad de casos por delitos informáticos desde el año 2016 al 2020, obteniéndose 392 procesos judiciales con sentencia por delitos de acceso ilícito, el cual representa un porcentaje de 1.8 %, así como delitos de atentado a la integridad de datos y sistemas informáticos, los cuales indican un porcentaje de 2.0 %.

Asimismo, se evidencia con mayor impacto los delitos de fraude informático y proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, los cuales tienen una expresión porcentual equivalente a 69.4 % y 22.2 %, respectivamente. Siendo así, los últimos delitos evaluados son la interceptación de datos informáticos y el delito de suplantación de identidad, copulativamente equivalen a un porcentaje de 4.6 % de la información total, situación que pone en evidencia la desproporción de casos registrados en sede fiscal en comparación a los casos resueltos en sede judicial.

De lo revisado en los antecedentes, el MINJUS (2020) remarca la necesidad de consolidar la información y reforzar las capacidades del personal tanto de las Fiscalías como de los Juzgados a fin de lograr brindar un servicio de atención óptimo y oportuno en los casos de ciberdelincuencia. Asimismo, agrega la importancia de la incorporación de los Juzgados Especializados porque permitirá contar con un registro sofisticado de las denuncias interpuestas y sobre todo se realizará un trabajo de concientización de la sociedad.

En ese contexto, el parecer anterior se refuerza con la tabla 6 referente a las personas con sentencia condenatoria registrada según delitos informáticos y contra el patrimonio relativo a delito informático a nivel nacional, durante el periodo 2016 – 2020, datos que demuestran la necesidad de implementar dichos Juzgados con conocimientos técnicos y preparados para una adecuada valoración de los medios de prueba y la resolución de casos.

En ese sentido, la importancia de contar con una información uniforme sobre el tratamiento de los casos de ciberdelincuencia y fortalecer las capacitaciones del personal

del Sistema de Justicia permitirá masificar el dominio de las actuaciones, inclusive se podría lograr proyectar una guía de los procedimientos útiles durante la investigación fiscal, dejando el panorama más claro sobre las situaciones que podrían considerarse como delitos, así como brindar información a los ciudadanos de los lugares donde pueden acudir o qué hacer para salvaguardar los posibles elementos probatorios u otro medio que permita la continuidad del proceso, escenarios que coadyuvarán con la investigación, siempre que se cuente con jueces especializados que al recibir los medios de pruebas sepan valorar y resolver con base a la objetividad y transparencia.

Continuando la discusión respecto a la ausencia de Juzgados Especializados, desde el punto de vista internacional, los doctores Carretero, Lamperti y Migliorisi (2020), coinciden en que la exigencia de contar con conocimientos tecnológicos debe ser orientado a quienes conforman la Administración de Justicia, esto es, fiscales, jueces y personal que coadyuve con el tratamiento de los casos de ciberdelincuencia dada su complejidad. Igualmente, indican la importancia de las capacitaciones constantes hacia los jueces, así como el hecho de que ellos conozcan y entiendan la actuación realizada por los fiscales y a partir de ello, se comprenda la producción de la prueba y se decida la culpabilidad de un procesado dentro de un juicio penal en el que se respeten todas las garantías.

Es importante que el conocimiento y comprensión de los medios tecnológicos sean exigidos a todos los órganos que conforman la Administración de Justicia dada la gran complejidad que conlleva la atención y tratamiento de los casos de ciberdelitos, así como promover las capacitaciones a los jueces y que los mismos entiendan de forma clara la actuación de los fiscales desde la etapa de investigación, los medios de prueba y la actuación en la etapa de juzgamiento, todo ello, con la finalidad de evitar la dilación de los procesos por factores relacionados a la falta de capacitación, actualización, entre otros.

Siguiendo el mismo sentido, los especialistas Rincón y Maza (2020) concuerdan que la ausencia de Juzgados Especializados son un problema por el impacto que pueden ocasionar ante la comisión de un fraude informático a uno de los sistemas del Estado. A su vez, el desconocimiento de las nuevas tecnologías genera que los jueces no tengan esa inmediación y empatía con los casos, siendo un problema actual y de necesidad inmediata. Por ello, la insistencia de contar con jueces conocedores y expertos en altas tecnologías coadyuvará a mejorar la designación de casos según su especialización.

En tal sentido, la ausencia de Juzgados Especializados trae consigo diversos problemas entre ellos, la posibilidad de la comisión de un fraude informático en perjuicio del Estado, vulnerando aspectos económicos, sociales e inclusive acuerdos internacionales. Por ello, las políticas de prevención que debe fomentar el Estado ante los avances tecnológicos debe ser un punto de agenda a tratar en el menor tiempo posible. Por otro lado, se aspira que los jueces cuenten con los conocimientos especializados en delitos informáticos para un mejor análisis en función a la inmediación y celeridad de los procesos porque se conocerá la afectación directa e indirecta en perjuicio de la víctima y su impacto en la sociedad.

En contrapropuesta a las ideas expuestas anteriormente, Acurio y Temperini (2020) plantean que los términos tecnológicos deben ser aterrizados a un lenguaje simple para que pueda ser entendido por el juez, porque no se le puede exigir a los fiscales y jueces ser expertos en ingeniería de sistemas, sino que al menos cuenten con una formación en derecho informático. Así también, involucra la habilidad del abogado que sustenta el caso ante el juez, será vital la sencillez con la que traslade la información.

En ese sentido, la exigencia de conocer a las altas tecnologías se direcciona exclusivamente al fiscal, porque es quien inicia la investigación y respecto al juez que debe tener el pleno conocimiento sobre el derecho; y la noción sobre la ciberdelincuencia, pero no reiterar la exigencia de una especialización en tecnología. En esa perspectiva, el Dr. Elías (2020), agrega que se necesita capacitar a los operadores de justicia en aspectos básicos sobre los medios tecnológicos porque en todos los casos se requiere la autorización del juez para el levantamiento del secreto de las telecomunicaciones y de esa forma se acceda a los móviles u otro medio electrónico.

En consideración a lo anterior, la explicación de las actuaciones que realiza el fiscal, perito, abogado, entre otros, debe ser transmitido al juez en un lenguaje sencillo para garantizar el pleno conocimiento de los casos de ciberdelincuencia. Por ello, consideramos que los fiscales, jueces y personal autorizado deben contar con formación en derecho informático, para que exista una uniformidad de la información y que ante cualquier vulneración, hechos inusuales o términos nuevos puedan ser discutidos en igualdad de condiciones. Reiteramos que contar con una especialización en informática no lo es, ni será suficiente ante el desmedido avance de la tecnología, por tanto, es necesario que los operadores del derecho sigan en constante capacitación y actualización sobre los medios digitales.

En relación a las propuestas para potenciar nuestro sistema de justicia

De lo revisado en las entrevistas internacionales, los autores Carretero, García, Lamperti y Migliorisi (2020) consideran que la aplicación de una competencia en función de la materia, así como el trabajo en conjunto de las Fiscalías y Juzgados Especializados permitirá brindar una mejor atención de los casos de ciberdelincuencia y así lograr una similitud de conocimiento jurídico y técnico en todas las instituciones que lleven adelante estos casos complejos. En ese sentido, el conocimiento integral permitirá que los jueces sepan actuar ante los casos ligados directamente a delitos informáticos e indirectamente en los casos mediante el uso de la tecnología. Por esa razón, se deben fomentar las capacitaciones de los organismos antes descritos, sobre el uso de los medios tecnológicos debido al avance de la tecnología y sus implicancias en la sociedad.

Considerando las posturas comentadas líneas atrás, la cooperación entre los distintos órganos que involucra el Sistema de Justicia es uno de los aspectos más relevantes para mejorar la atención y el tratamiento de los delitos informáticos. Asimismo, el conocimiento jurídico y técnico uniforme permitirá contar con un personal idóneo para la absolución de consultas ligadas a los delitos informáticos y los cometidos mediante el uso de la tecnología, porque en la realidad vemos casos que no necesariamente serán de fácil entender o de simple identificación del presunto ciberdelincuente. Por ello, la exigencia de entender sobre informática y derecho, sumado a las capacitaciones es un tema urgente y de inmediata atención.

En relación a lo anterior, los doctores Rincón, Maza, Acurio y Temperini (2020) agregan la importancia de la previsión y difusión de la información sobre la identificación de conductas que pueden configurar como delito, porque si los ciudadanos conocen sobre estos temas no dudarán en denunciar y más aún no se dejarán influenciar. Cabe mencionar que la incorporación de las Fiscalías y Juzgados Especializados sería una garantía para los ciudadanos respecto a las expectativas de los procesos. A su vez, advierten la necesidad de establecer un marco de cooperación con la finalidad de mantener una comunicación sumamente activa y fluida en relación a la información obtenida durante el procesamiento de la investigación.

Conjuntamente pensamos que el Estado debe concentrar sus actividades en la prevención de la comisión de los delitos y evitar un esfuerzo innecesario para mitigar sucesos que en su oportunidad se pudieron evitar. Otro punto importante es que, el Estado debe fomentar la difusión de información necesaria sobre las formas en las que se puede configurar un

delito y cómo se debe actuar frente a ello, empleando un lenguaje simple para que las víctimas entiendan de forma inmediata las acciones que deben seguir y evitar llenarlas de dudas o ambigüedades que finalmente concluirán en la desconfianza y rechazo de las víctimas al Sistema de Justicia.

En otra línea argumentativa, Guerrero (2020) sostiene la importante labor que viene realizando la DIVINDAT en la atención de los delitos informáticos, sin embargo, a medida que pasa el tiempo surgieron algunos problemas respecto a la atención de delitos cometidos mediante el uso de las tecnologías y el desabastecimiento de los casos por ser una sola entidad en la capital la encargada de la recepción de todas las denuncias, por ello, es necesario que la Unidad recientemente incorporada capacite al personal sobre el tratamiento de los delitos informáticos y los cometidos mediante uso de la tecnología.

Siguiendo esa línea de pensamiento, Elías (2020) añade que, los Juzgados deben ser incorporados a un mediano plazo porque es necesario diferenciar la atención de los casos ordinarios respecto de los que requieren mayor esfuerzo cognoscitivo y dominio del entorno digital. Por último, Cuadros (2020) señala que, no solo la ciberdelincuencia involucra el dominio de conocimientos teóricos sino también prácticos, que son obtenidos únicamente con la experiencia en el campo laboral, por ello contar y fortalecer el sistema especializado en ciberdelincuencia permitirá volcar los conocimientos en la identificación o prevención de la comisión de los ciberdelitos.

Sin desmerecer la ardua labor que vienen realizando los distintos órganos encargados de la atención y tratamiento de los casos de ciberdelincuencia, es necesario conocer las falencias y carencias de estas entidades a fin de mejorar, perfeccionar o incorporar unidades de apoyo ante los casos que durante la pandemia han tomado un impulso significativo, así como tener la confianza que el personal encargado de los ciberdelitos cuenta con los conocimientos sólidos en cuanto a la diferenciación de los casos ordinarios con los de mayor complejidad, sería un avance transcendental, ampliando el aspecto cognoscitivo con la experiencia adquirida durante el tiempo.

En lo referido a las sugerencias o recomendaciones sobre delitos informáticos

De lo examinado en las entrevistas internacionales, Carretero (2020) recomienda que, el simple hecho de ingresar al mundo virtual, trae consigo implicancias que la mayoría de personas desconoce o no le otorga la importancia debida, por ello, la responsabilidad digital es un factor importante que dependerá de uno mismo. En relación a la postura

anterior, García y Maza (2020) sostienen sobre la concientización del uso de las contraseñas que los usuarios deben activar la capa de seguridad personal, es decir el control de identidad en dos pasos, así como fomentar el diálogo y seguimiento responsable de los padres hacia los menores, cumpliendo el rol de guías permanentes al interactuar con la tecnología, por ello la prevención del uso de la informática será la mejor solución para disminuir la comisión de los delitos informáticos. Reforzando la idea, la especialista Sabrina (2020) añade que el Estado debe promover la información, cursos de capacitaciones relacionados a la ciberdelincuencia y aquellos integrantes más jóvenes dentro de una familia puedan facilitar la información a los más adultos con el fin de prevenir ser víctimas de los ciberdelincuentes.

La inserción de la persona al mundo digital es un tema de sumo cuidado porque indirectamente los usuarios mediante sus publicaciones u otras conductas en los medios electrónicos divulgan su información personal, dejando entrever situaciones que algunas veces no son reales, pero a la vista de terceros podría generar interés. En ese sentido, la prevención de los delitos, incentiva a que los usuarios coloquen claves más seguras y sobre todo la comunicación en los hogares será un factor determinante para que los usuarios estén pendientes a la recepción de correos, mensajes u otros medios maliciosos y sepan cómo actuar de forma inmediata ante alguna sospecha o maniobra temeraria cibernética. Por ello, el rol del Estado debe ser enfocado en la difusión de las capacitaciones en ciberdelincuencia que sean de fácil entender, actuación que será crucial para coadyuvar en la prevención de estos delitos.

En concordancia con la idea anterior, el Dr. Migliorisi (2020), afirma que el buen uso de las tecnologías será la mejor arma para prevenir la comisión de los delitos informáticos, postura respaldada por los expertos, Rincón, Acurio y Temperini (2020) quienes hablan sobre la responsabilidad de los usuarios en el uso de la tecnología y la prioridad que se incentive en la sociedad para evitar futuros ataques. El hecho de desconfiar de la tecnología o de los beneficios que muestra, tales como, envíos de correos electrónicos maliciosos, facilidad de crédito bancario u ofrecimiento de productos, es un punto a favor porque permitirá que se repregunte la veracidad del contenido, así como dudar de la procedencia de la información, todo ello, será posible en la medida que se ponga en práctica el pensamiento crítico y ser conscientes de la inseguridad cibernética.

Es importante el uso adecuado de los medios tecnológicos porque se podrá evitar la comisión de los delitos informáticos, básicamente es la responsabilidad de cada usuario

al aceptar los términos y condiciones de un determino servicio. Por otro lado, la desconfianza de los usuarios ante la llegada de mensajes, correos, llamadas desconocidas permitirá ganar tiempo para repensar el proceder del ciberdelincuente y ante estos hechos el usuario sepa qué hacer y a dónde acudir. El pensar más allá de lo evidente, puede resultar más efectivo y en ocasiones permita evitar la comisión de los delitos cibernéticos.

Desde una perspectiva nacional, los especialistas Guerrero, Elías, Cuadros y el suboficial Jiménez (2020) concluyen en trasladar las prácticas de la realidad a las del mundo digital, desconfiando de personas sin identificación cierta y veraz. Asimismo, es importante que ante sucesos inesperados relacionados a los delitos cibernéticos sepan sobre la existencia de entidades encargadas de la atención e investigación de estos casos. Ahora bien, un método acertado para la prevención de los ciberdelitos es reforzar las contraseñas personales y evitar el uso de una sola clave para distintas redes sociales y cuentas bancarias. Por ello, si se llegase a ser víctimas no duden en denunciar y llegar hasta la última etapa de la investigación porque muchas veces se puede tener impactos más gravosos que los realizados en el mundo real. Por último, contar con el conocimiento y saber los riesgos antes de que ocurra la comisión del delito, siempre será un buen indicador para reforzar y perfeccionar la prevención de esta clase de delitos.

La importante labor que debe cumplir el Estado es promover cursos, charlas o programas referente a los casos de delitos informáticos porque garantizará que los usuarios conozcan un poco más sobre el proceder de los ciberdelincuentes y no caer en chantajes o extorsiones. Asimismo, el hacer caso omiso cuando poco o nada los medios de comunicación o por consejos de terceros señalan que las claves o contraseñas deben ser colocadas con criterio porque en la realidad se ven múltiples casos en el que los usuarios por temas de tiempo o por el famoso dicho —no creo que me pase — se confían, dejando atrás los innumerables riesgos que podría generar el hecho de no haberse tomado un tiempo adicional para insertar o modificar las claves de las redes sociales y cuentas bancarias. Lastimosamente, uno no mide el riesgo hasta que le ocurre y por pequeñas cosas que se pudo prevenir en su debido tiempo, se vean afectadas en pérdidas materiales, económicas o en el peor escenario se vulnere el honor y reputación de la persona.

4.1.3. Implicancias

En este acápite se redactaron las implicancias, conocidas en la doctrina como implicaciones, con base en los objetivos de la investigación tomando en cuenta para su desarrollo tres enfoques, estos son, la implicancia práctica, teórica y metodológica. Esto

nos permitirá difundir a la comunidad jurídica y sociedad civil, la importancia de nuestra investigación.

4.1.3.1. Implicancia práctica

En lo que respecta a la implicancia práctica, iniciaremos por comentar que este trabajo contribuirá al Sistema de Administración de Justicia a resolver dos problemas reales, el primero vinculado a la incorporación de una Fiscalías Especializada en Ciberdelincuencia y el segundo relacionado a la implementación de un Juzgado Especializado en Ciberdelincuencia. Ambas están lejos de ser propuestas antojadizas de los autores, pues cuentan con el respaldo de la doctrina, la jurisprudencia, el análisis documental recabado y medularmente con base a las entrevistas obtenidas.

Simultáneamente, la implicancia anterior es trascendental para mejorar diferentes subproblemas que se desprenden de un despliegue limitado de nuestras autoridades, por mencionar algunos de ellos, la obtención, custodia y preservación de la prueba digital, propuestas de diligencias pertinentes para esclarecer los hechos y a los presuntos responsables, las pericias que realmente deberían solicitarse, un mejor entendimiento en aspectos técnicos entre el juez, el fiscal, los peritos y demás intervinientes.

4.1.3.2. Implicancia teórica

En lo referido a la implicancia teórica se puede mencionar que los resultados obtenidos servirán para incrementar el acervo de información en la materia de ciberdelincuencia y apoyará múltiples propuestas de diferentes autores nacionales y extranjeros sobre el perjuicio que se causa a la sociedad al no contar con órganos especializados para combatir la delincuencia informática. Asimismo, insistimos en que es errado el análisis al que se arriba en el tratamiento judicial del ciberdelito elaborado por el Consejo Ejecutivo del Poder Judicial, porque apoyando postulados de autores referentes a nivel nacional, los esfuerzos tienen que ser copulativos desde el persecutor de la acción penal pública hasta la autoridad que tiene bajo su responsabilidad juzgar la causa.

Con el análisis documental se ofrecieron resultados que eran desconocidos por la comunidad en general, como es el detalle de los casos investigados en sede fiscal en donde se expuso que nuestros Fiscales y Jueces no están preparados para investigar y juzgar dichos casos, respectivamente, en principio porque no cuentan con los conocimientos especializados, así como las herramientas tecnológicas, logísticas e infraestructurales para ejecutar con eficiencia dicha labor, con ello no solo se busca

resaltar solo las deficiencias, sino por el contrario se propone una medida necesaria que fue impulsada e incorporada por los países de nuestra región y que ha demostrado resultados positivos en todas sus aristas. Esperamos que las ideas plasmadas en el decurso de la investigación puedan ser utilizadas en futuros estudios jurídicos con la seriedad y rigurosidad que amerita.

4.1.3.3. Implicancia metodológica

En lo correspondiente a esta implicancia, se puede rescatar que la utilidad metodológica permite analizar reportes con el tratamiento del análisis documental. Es decir, el instrumento de recolección de datos seguirá siendo el análisis de documentos, sin embargo, se podrán analizar los datos recabados en el programa Excel a través de las tablas y gráficos dinámicos en dicha plataforma de manera útil y clara. Dichos resultados podrán ser presentados en figuras inteligibles para un óptimo entendimiento por parte de los lectores tal y como se utilizó en la presente investigación.

Asimismo, esta propuesta sugiere al investigador cómo podría estudiar dos poblaciones y cinco muestras incrementando la calidad de la tesis. Dicho en otras palabras, el autor bajo el criterio de muestreo no probabilístico por conveniencia puede definir una población conformada por abogados y policías; y tres muestras integradas por 11 abogados y 1 policía para aplicar la técnica de la entrevista y utilización del instrumento de recolección de datos de la guía o cuestionario de entrevista. A su vez, se puede conformar una base de datos conformada por casos en sede fiscal y judicial sobre delitos informáticos y dos muestras integradas por un reporte fiscal con 15 548 casos y otro reporte con 440 sentencias condenatorias. Todo esto dependerá de los objetivos que se haya trazado en la investigación, así como el nivel de aporte que desee incluir el investigador.

4.2. Conclusiones

En esta sección del presente estudio se proporciona la interpretación general a la que arribaron los autores según el análisis de los datos vinculados a los problemas y objetivos, así como los fragmentos teóricos que retoma el problema y confirma las hipótesis de la investigación.

Primero:

Como resultado de la investigación se obtuvo que nuestro actual Sistema de Administración de Justicia conformado principalmente por el Ministerio Público

(Unidad Fiscal Especializada en Ciberdelincuencia), el Poder Judicial y la Policía Nacional del Perú (División de Investigación de Delitos de Alta Tecnología) no resultan apropiados para procesar la comisión de los delitos informáticos y delitos tradicionales cometidos en medios tecnológicos porque existen carencias en el personal, la infraestructura y la logística.

Segundo:

La falta de una Fiscalía Especializada en Ciberdelincuencia que no cuente con fiscales, asistentes en función fiscal y personal administrativo con conocimientos en derecho y tecnología, dedicada únicamente a la atención de delitos informáticos y delitos tradicionales cometidos en medios tecnológicos, incide negativamente en los actos de investigación fiscal, imposibilitando una representación idónea y generando un estado de desconfianza en las víctimas.

Tercero:

Finalmente, podemos concluir que la ausencia de un órgano igualmente instruído como un Juzgado Especializado en Ciberdelincuencia que resuelva la causa con conocimientos técnicos y jurídicos que le permitan valorar la evidencia convertida en prueba digital durante la sustentación en juicio y al no contar con un órgano avocado únicamente al conocimiento de delitos informáticos y delitos tradicionales cometidos en medios tecnológicos, afecta la potestad jurisdiccional y atenta contra el equilibrio del Sistema de Justicia.

4.3. Recomendaciones

En este apartado de la investigación se redactaron las recomendaciones que a nuestro entender podrían tomar en cuenta nuestros legisladores para repotenciar el Sistema de Administración de Justicia, así como cualquier estudiante o profesional visionario y ejercer su iniciativa legislativa promoviendo proyectos de ley que contribuyan a la seguridad informática de la sociedad cibernética.

Primero:

Se recomienda incorporar Fiscalías y Juzgados Especializados en Ciberdelincuencia siguiendo la experiencia de otros países en Latinoamérica, tales como Argentina, Uruguay y España, para perfeccionar nuestro Sistema de Justicia y colocar en un nivel óptimo a nuestras autoridades.

Segundo:

Se recomienda ampliar las potestades de la Unidad Fiscal Especializada en Ciberdelincuencia para que actúe durante toda la investigación fiscal y proceso judicial, así como se refuerce los conocimientos sobre la cadena de custodia de la prueba digital y las propuestas de las diligencias en la investigación preparatoria.

Tercero:

Se recomienda que, la posible incorporación de una Fiscalía Especializada en Ciberdelincuencia cuente con un Juzgado igualmente especializado en la impartición de justicia, evitando así que durante el desarrollo del proceso haya desconocimiento de parte del juzgador sobre los actos de investigación fiscal realizados o la valoración de las pruebas digitales sustentadas en juicio.

REFERENCIAS

A favor de tic (2017). *¿Qué es un ciberdelito?* Recuperado de https://bit.ly/2MJ0oVR

Academia de la Magistratura (2020). *Programa de Actualización y Perfeccionamiento*. Programas Académicos. Recuperado de https://bit.ly/3oAlVx5

Altuna, M. (2018). *Guía de investigación científica 2018*. Revista de la Facultad de Derecho y Ciencias Políticas de la UPN. Recuperado de http://bit.ly/3czqfKN

Álvarez Rodríguez, I. (2018). *Apuntes sobre el Derecho del Ciberespacio*. En Revista de la Escuela de Ingeniería Informática de Segovia. Recuperado de https://bit.ly/39TnqT6

Aranda, V. (2004). *Historia y evolución de Internet*. Autores científico-técnicos y académicos, 01-11. Recuperado de https://bit.ly/3tdft2z

Arias Gonzáles, J. (2020). *Proyecto de Tesis Guía para la elaboración*. Recuperado de http://bit.ly/36Tduaj

Arias Gonzáles, J. (2020). *Técnicas e instrumentos de investigación científica*. Recuperado de http://bit.ly/2YFtw2Y

Baena Paz, G. (2014). *Metodología de la investigación*. Recuperado de ProQuest Ebook Central https://bit.ly/3amcPyJ

Cardozo, R. (30 de agosto de 2019). *Atención al 'vishing': cómo detectarlo y protegerse*. BBVA, Lima, p. A1.

Consejos para protegerse contra el cibercrimen. [Editorial]. (04 de diciembre de 2019). *Kaspersky*, p. A1.

Constitución Política del Perú (1993, 29 de diciembre). Presidencia del Consejo de Ministros. Recuperado de https://bit.ly/2MmuiPB

Cornejo, J. (9 de diciembre de 2020). *¿Qué es el allanamiento en una investigación penal y cuál es el procedimiento para su realización?* Entrevista. Gestión [Archivo de Vídeo]. http://bit.ly/303Coju

Cortes, R. (2015). *Retos de la Administración de Justicia frente a los Delitos Informáticos*. En Universidad Santo Tomas Sede Villavicencio. [En línea]. Recuperado de https://bit.ly/2L6nkhf

Decreto Supremo N° 010-19-RE - MRE. *Ratifican el "Convenio sobre la Delincuencia"* (marzo 09, 2019). Recuperado de https://bit.ly/39BjsOC

Decreto Supremo N° 017-93-JUS – MINJUS. *Texto Único Ordenado de la Ley Orgánica del Poder Judicial* (mayo, 2012). Recuperado de https://bit.ly/3pBKtXQ

Derecho Internacional (2018). *Acuerdo Internacional*. Recuperado de http://bit.ly/2NYcCdK

Díaz, R (2019). *El crecimiento de la ciberdelincuencia*. En Universidad ESAN [En línea]. Recuperado de https://bit.ly/3j4K0Le

Diccionario panhispánico del español jurídico (2020). *Delito informático*. Recuperado de http://bit.ly/3cvyfwf

División de Investigaciones de Delitos de Alta Tecnología (2006). *Bienvenidos a la DIVINDAT*. Recuperado de https://bit.ly/3ozkA9J

Domínguez Cerezo, A., & Cornejo García, R. (2020). *La ciberdelincuencia en España: Un estudio basado en las estadísticas policiales*. *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS, (6), 2.* Recuperado de https://bit.ly/36MsEOm

El Centro Curtis E. LeMay para el Desarrollo y la Educación de la Doctrina (2011). *Introducción a las Operaciones Ciberespaciales*. Recuperado de https://bit.ly/3pAwZf3

Elías, R. (2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú*. En Revista Hiperderecho. Recuperado de https://bit.ly/3ara0Nc

Elías, R. (2020, 13 de junio). GADE - *Grupo de Arbitraje y Derecho Empresarial* [Transmisiones]. Recuperado de https://bit.ly/39ApOO9

Fernández Flecha, M., Urteaga Crovetto, P. & Verona Badajoz, A. (2015). *Guía de investigación en Derecho*. En Vicerrectorado de Investigación de la Pontificia Universidad Católica del Perú. Recuperado de https://bit.ly/3tdR0tV

Flores, M. (2018). *Tecnología y violencia en Perú. En Hiperderecho*. [En línea]. Recuperado de https://bit.ly/3oJbmbf

García, V. (2019). *¿Cómo está avanzando la Ciberseguridad en el Perú? Breve Aproximación al Marco Normativo*. Actualidad Jurídica. Recuperado de https://bit.ly/2NTBBik

Guerrero, C. (2018). *De Budapest: Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia impacto en el corto, mediano y largo plazo*. Derechos Digitales América Latina. [En línea]. Recuperado de https://bit.ly/3pAQQL9

Hernández Sampieri, R. & Mendoza Torres, C. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* (Primera Edición). México: Ciudad de México. Recuperado de https://bit.ly/39yBYXL

Hernández, R. (2014). *Metodología de la investigación.* (Sexta Edición). México: Ciudad de México. Recuperado de https://bit.ly/3uDuZVY

Hernández, R., Fernández, C. & Baptista, P. (2010). *Metodología de la investigación.* (Quinta Edición). México: Ciudad de México. Recuperado de http://bit.ly/3pDs90i

Herrera Ursua, L. (2018). *Eficacia de la Ley de Delitos Informáticos en el Distrito Judicial de Huánuco 2017*. (Tesis para optar Título Profesional). Universidad de Huánuco, Perú.

Jackson, M. & Scrollini, F. (2017). *Apuntes sobre Delitos Informáticos en Uruguay (Notes on Computer Crimes in Uruguay)*. En DAT&SOC. [En línea]. Recuperado de https://bit.ly/3cAljoC

La Ley (13 de febrero de 2019). *El Perú aprobó el Convenio sobre la Ciberdelincuencia: estos son los nuevos delitos.* El Ángulo Legal de la Noticia. Recuperado de https://bit.ly/3cAli42

Ley N° 26335 - CR. *Ley Orgánica de la Academia de la Magistratura* (julio 21, 1994). Recuperado de https://bit.ly/3r8o6JN

LP Pasión por el Derecho (14 de agosto de 2019). *Cibercrimen y nueva teoría del delito*. Entrevista al profesor Ricardo Posada [Archivo de Vídeo]. YouTube. https://bit.ly/3rbdCts

LP Pasión por el Derecho (2020). *La ciberdelincuencia: ¿quién nos protege?* Recuperado de https://bit.ly/3pF4AUU

Marchal Gonzáles, A. (2016). *La ciberdelincuencia ¿Estamos preparados para perseguir este tipo de delitos?* En Revista de Criminología creada por el Departamento de Criminología y Seguridad de la Facultad de Derecho y Economía n.° 4. Recuperado de https://bit.ly/3pF0w7d

Martínez Ruíz, H. & Benítez Ontiveros, L. (2015). *Metodología de la investigación social* I. México: Querétaro. Recuperado de https://bit.ly/2NTHMmw

Mesa Millán, A. (2017). *La ciberdelincuencia y sus consecuencias jurídicas.* (Tesis de Grado en Criminología). Universidad de Valladolid, España.

Ministerio de Economía y Finanzas (2021). *Conoce el proceso de desarrollo del Presupuesto Público 2021*. Recuperado de http://bit.ly/2MFNUhZ

Ministerio de Justicia y Derechos Humanos (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú.* Observatorio Nacional de Política Criminal. Recuperado de https://bit.ly/2YyCuiu

Ministerio Público Fiscal (2021). Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). Recuperado de http://bit.ly/3cvCkjQ

Ministerio Público Fiscal de la Provincia de Salta. (2020). *Ciberdelitos: el miedo a la modernidad ayuda a una sociedad indecente.* [En línea]. Recuperado de https://bit.ly/39AcCsP

Ministerio Público Fiscalía de la Nación (2017). *Manuel de Evidencia Digital*. Recuperado de https://bit.ly/3apN40x

Ministerio Público Fiscalía de la Nación (2017). *Manuel de Evidencia Digital*. Recuperado de https://bit.ly/3apN40x

Ministerio Público Fiscalía de la Nación (2020). *Boletín Estadístico del Ministerio Público. Boletín - N° 7*. Recuperado de https://bit.ly/39Bi1Qe

Ministerio Público Fiscalía de la Nación del Perú (2020). *¿Qué hacemos?* Gob.pe. Plataforma digital única del Estado Peruano. Recuperado de https://bit.ly/3r9WoMY

Ministerio Público Fiscalía de la Nación del Perú (2020). *Fiscalías Especializadas*. Sistema Fiscal. Recuperado de https://bit.ly/2NOvZFX

Morachimo, M. (2019, 12 de febrero). *Sentido común frente a la Convención de Budapest.* CE Think Tank Newswire. Recuperado de http://bit.ly/3uVOVnr

Organización de los Estados Americanos (1969). *Convención de Viena sobre el derecho de los tratados*. Recuperado de https://bit.ly/3j6SMZc

Organización Internacional de Policía Criminal - Interpol (2021). *Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad*. Recuperado de http://bit.ly/3j8ENSz

Organización Mundial de la Propiedad Intelectual (1969). *Glosario*. Recuperado de http://bit.ly/39Ejc1x

Perú se adhiere a Convenio de Budapest sobre Ciberseguridad y Ayuda Judicial [EFE News Service]. (04 de febrero de 2019). EFE News Service, párr. 6. Recuperado de https://bit.ly/3r5S80Q

Perú. Ministerio Público Fiscalía de la Nación del Perú (2003). *Resolución de la Fiscalía de la Nación N° 714-2003-MP-FN: Creación e Implementación de la Escuela del Ministerio Público.* Recuperado de https://bit.ly/3r3xT3K

Perú. Ministerio Público Fiscalía de la Nación del Perú (2004). *Resolución de la Fiscalía de la Nación N° 1234-2004-MP-FN: Reglamento de Organización y Funciones de la Escuela del Ministerio Público «Dr. Gonzalo Ortiz de Zevallos Roedel»*. Recuperado de https://bit.ly/2NSJioZ

Portal del Consejo de Europa (2020, 22 de noviembre). *Cuadro de firmas y ratificaciones del Tratado 185 Convenio sobre Ciberdelincuencia*. Recuperado de https://bit.ly/3akKdWL

Presidencia del Consejo de Ministros (2019, 01 de febrero). *Perú se adhiere al Convenio de Budapest para luchar contra la ciberdelincuencia.* Oficina de Prensa e Imagen Institucional. Recuperado de https://bit.ly/2L3Szt8

Prieto, N. & Vargas, G. (2020). *Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informáticos*. (Tesis de grado en Maestría). Universidad de Guayaquil, Ecuador.

Proaño Reyes, G. (2018). *La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana*. En Revista de Derecho Iuris Dictio. Recuperado de http://bit.ly/3tqAJlD

Proyecto de Ley N° 4643/2019 – CR. *Ley que declara de interés nacional y necesidad pública la creación de la fiscalía especializada en delitos informáticos* (agosto 02, 2019). Recuperado de https://bit.ly/2MELyPZ

Ramírez Gonzáles, A. (2004). *Metodología de la Investigación Científica*. Recuperado de http://bit.ly/3j3Y1Jb

Resolución de la Fiscalía de la Nación N° 1503-2020 - FN. *Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima*. (diciembre 12, 2020). Recuperado de http://bit.ly/2YBqmNC

Resolución Legislativa N° 30913 - PCM. *Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia* (febrero 12, 2019). Recuperado de https://bit.ly/3amx0gc

Resolución Nº 024-2020-MP-FN-JFS - FN. *Crean fiscalías, despachos y plazas fiscales en el Distrito Fiscal de Lima, con motivo de la Implementación del Código Procesal Penal, correspondiente al Primer Tramo* (junio 24, 2020). Pág. 2. Presidencia de la Junta de Fiscales Supremos de la Fiscalía de la Nación. Recuperado de http://bit.ly/3jkzjV0

Rico, M. (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos*. Revista IUS, 7(31) pp. 207-222. Recuperado de https://bit.ly/3cINLEX

Supo, J. (2015). *Cómo empezar una tesis: tu proyecto de investigación en un solo día. En revista Bioestadístico*. Obtenido de https://bit.ly/39zNzpG

Taylor, J. & Bogdan, R. (1994). *Introducción a los métodos cualitativos de investigación. Ediciones Paidón Ibérica S.A.* España: Barcelona. (Reimpresión). Recuperado de http://bit.ly/3r0HVCo

Tenorio Pereyra, J. E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*. (Tesis de grado en Maestría). Academia Diplomática del Perú, Perú.

Vásquez Sarmiento, A. L. (2019). *Falsos portales que conectan a México con el cibercrimen transnacional: ciberdelincuentes ya no asaltan bancos ni casas; con internet y un click atacan a sus víctimas, esta amenaza por los cibernautas apenas empieza.* (Tesis de grado en Maestría). Centro de Investigación y docencias económica, México.

Vera, P. (2021). *Manual de introducción a la metodología de la investigación*. (Primera Edición). Recuperado de https://bit.ly/2NNCF7b

Villanueva Benites, Luis. (2011). *Diseño del proyecto e informe de investigación*. Recuperado de http://bit.ly/3j4j3Ye

Zeas Martínez, R. (2011). *Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark.* (Tesis de Licenciatura). Universidad Israel, Quito, Ecuador.

ANEXOS

Anexo 1. Denuncias recibidas en la DIVINDAT por delitos informáticos desde el 2015 hasta el 2020

DIVINDAT DIRINCRI <divindat.dirincri@gmail.com> lun, 9 nov 2020 23:09

para mí

Buenas noches,
Sr. Bertho Arturo Menacho Ortega
Se remite la información solicitada en formato excel, según lo coordinado en el email anterior, respecto a la entrevista se coordinará y se le dará el contacto por este medio, si tiene alguna duda respecto al cuadro no dude en hacer la consulta.

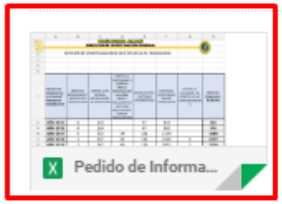
Dios Guarde a Ud.

CAP PNP
Teresa Milagros CHANG MORÁN
Área de Estadística-DIVINDAT- DIRINCRI-PNP

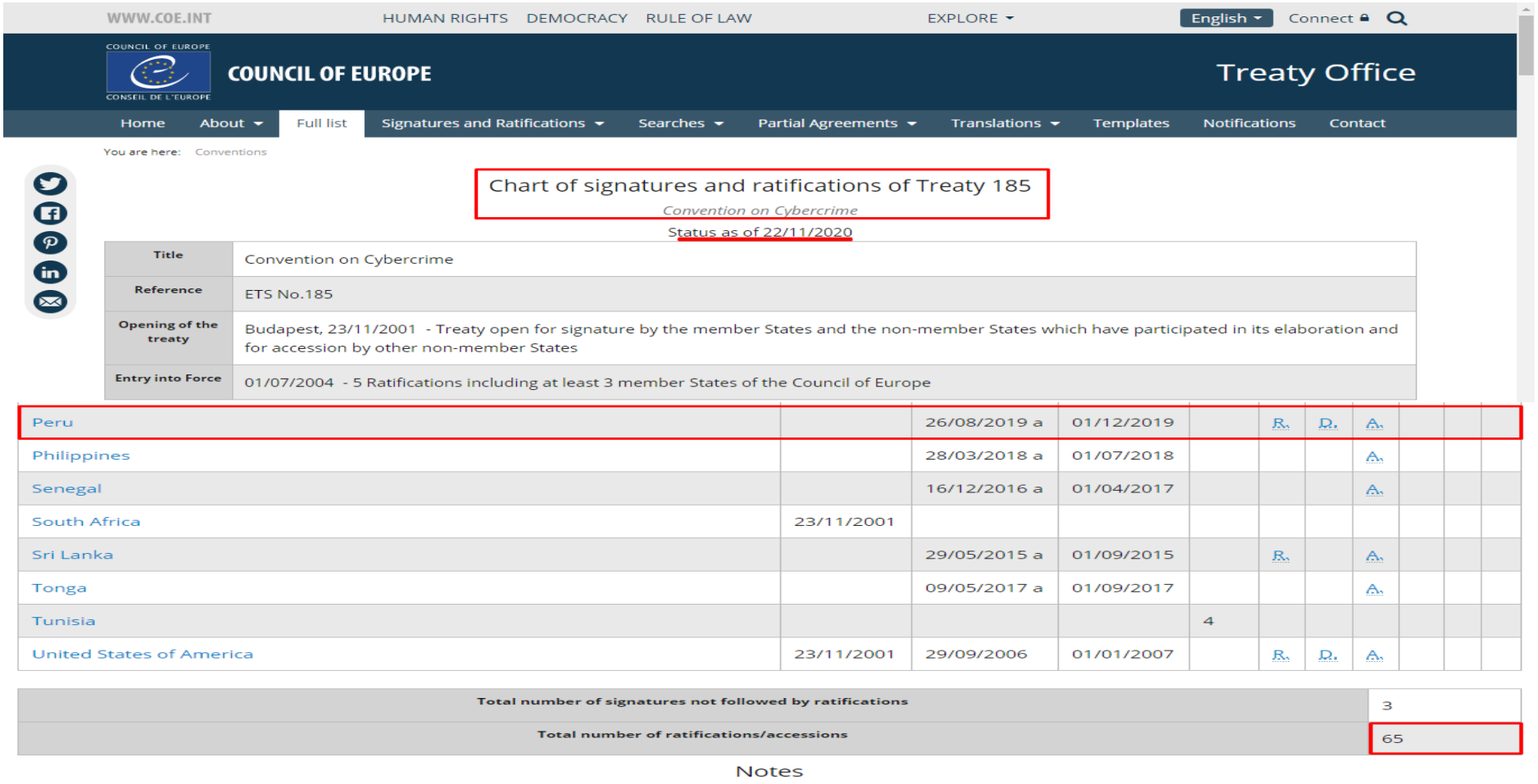
•••
--

ACUSAR RECIBO.
_____
ÁREA DE ESTADÍSTICAS
DIVINDAT-DIRINCRI PNP

CORREO INSTITUCIONAL: divindat.est@policia.gob.pe



Anexo 2. Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime, cuya traducción en castellano es: Cuadro de firmas y ratificaciones del Tratado 185 Convenio sobre Ciberdelincuencia



WWW.COE.INT HUMAN RIGHTS DEMOCRACY RULE OF LAW EXPLORE English Connect

COUNCIL OF EUROPE

COUNCIL OF EUROPE Treaty Office

Home About Full list Signatures and Ratifications Searches Partial Agreements Translations Templates Notifications Contact

You are here: Conventions

Chart of signatures and ratifications of Treaty 185

Convention on Cybercrime

Status as of 22/11/2020

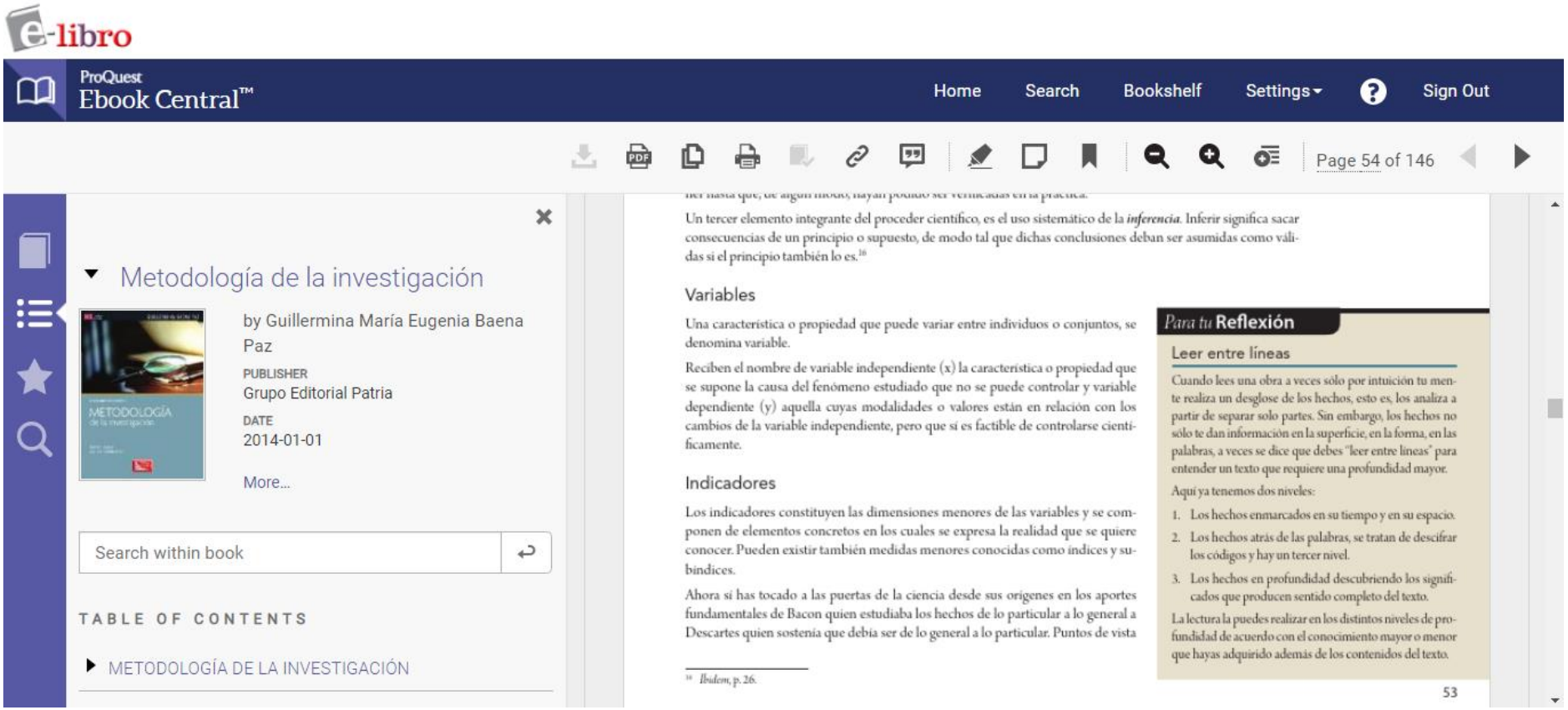
Title	Convention on Cybercrime
Reference	ETS No.185
Opening of the treaty	Budapest, 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
Entry into Force	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe

Peru		26/08/2019 a	01/12/2019		R.	D.	A.		
Philippines		28/03/2018 a	01/07/2018				A.		
Senegal		16/12/2016 a	01/04/2017				A.		
South Africa	23/11/2001								
Sri Lanka		29/05/2015 a	01/09/2015		R.		A.		
Tonga		09/05/2017 a	01/09/2017				A.		
Tunisia				4					
United States of America	23/11/2001	29/09/2006	01/01/2007		R.	D.	A.		

Total number of signatures not followed by ratifications	3
Total number of ratifications/accessions	65

Notes

Anexo 3. Definición de variables e indicadores



Anexo 4. Proyecto de Ley Nro. 05071

Proyecto de Ley Nro : 05071

Fundamentos

Efecto de la Vigencia de la Norma sobre la Legislación Nacional

Analisis Costo Beneficio

Texto del Proyecto

El CONGRESISTA DE LA REPÚBLICA QUE SUSCRIBE, EJERCIENDO EL DERECHO DE INICIATIVA LEGISLATIVA REFERIDO EN EL ARTÍCULO 107° DE LA CONSTITUCIÓN POLÍTICA DEL PERÚ:

CONSIDERANDO:

Que, el desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Que, en los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Que, los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, el presente proyecto se dirige a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países.

Propone el siguiente Proyecto de Ley:

LEY DE DELITOS INFORMATICOS

Artículo único.- *Incorpórase al Código Penal, promulgado por Decreto Legislativo N° 635, el Capítulo XI, Delitos Informáticos, los artículos 208a y 208b; con los siguientes textos:*

Artículo 208 a.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de la libertad no mayor de dos años, o con prestación de servicios comunitario de cincuentidós a ciento cuatro jornadas.

Artículo 209 b.- El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.

Lima, 18 de agosto de 1999

JORGE MUÑIZ ZICHES
Congresista de la República

Anexo 5. Proyecto de Ley Nro. 05132

Periodo:	Periodo de Gobierno 1995 - 2000.
Legislatura:	Primera Legislatura Ordinaria de 1999
Número:	05132
Fecha Presentación:	08/31/1999
Proponente:	CONGRESO DE LA REPUBLICA
Grupo Parlamentario:	
Titulo:	INFORMATICA:PENA DELITOS INFORMATICOS
Sumilla:	Establece como figura típica penal los Delitos Informáticos. El que maliciosamente destruya o inutilice el soporte lógico de un sistema computacional, empleando medios computacionales, será reprimido don pena privativa de libertad no mayor de cuatro años.
Autores(*):	DIAZ DIAZ SUSANA
Seguimiento:	02/09/1999 A Comisión Reforma de Códigos 09/09/1999 En Comisión Reforma de Códigos 12/11/1999 Dictamen Reforma de Códigos Favorable Sustitutorio Mayoria 18/11/1999 Orden del Día 03/05/2000 Aprobado

Anexo 6. Proyecto de Ley Nro. 05326

Periodo:	Periodo de Gobierno 1995 - 2000.
Legislatura:	Primera Legislatura Ordinaria de 1999
Número:	05326
Fecha Presentación:	10/18/1999
Proponente:	CONGRESO DE LA REPUBLICA
Grupo Parlamentario:	
Titulo:	CODIGO PENAL:196-PENA MANIP.INFORMATICA-TRANSFER.PATRIMONIO
Sumilla:	Modifica el artículo 196º del Decreto Legislativo Nº 635. Código Penal. Establece pena para aquel que valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.
Autores(*):	VEGA ASCENCIO ANASTACIO
Seguimiento:	22/10/1999 A Comisión Reforma de Códigos 26/10/1999 En Comisión Reforma de Códigos 12/11/1999 Dictamen Reforma de Códigos Favorable Sustitutorio Mayoria 18/11/1999 Orden del Dia 03/05/2000 Aprobado 08/05/2000 Autógrafa Sobre Nº: 102-99 31/05/2000 Observado 07/06/2000 Vuelve Comisión Reforma de Códigos 08/06/2000 En Comisión Reforma de Códigos 14/06/2000 Dictamen Reforma de Códigos Favorable Sustitutorio Mayoria 14/06/2000 Orden del Dia 21/06/2000 Aprobado 26/06/2000 Autógrafa Sobre Nº: 151-99 17/07/2000 Promulgado Ley Nº: 27309
Iniciativas Agrupadas:	5132, 5071
Número de Ley:	Ley Nº: 27309 07/17/2000 DELITOS INFORMATICOS INCORPORADO AL CODIGO PENAL
Titulo de la Ley:	DELITOS INFORMATICOS INCORPORADO AL CODIGO PENAL
Sumilla de la Ley	Ley que incorpora los delitos informáticos al Código Penal.

Anexo 7. Conversatorio sobre Nuevas Tecnologías y Delitos Informáticos - Situación actual de los Hackers a las cuentas privadas y servidores de las entidades del Estado

Anexo 8. Número de Fiscalías del Ministerio Público por categoría y especialidad, julio 2020

Categoría/ Especialidad	2019 Julio	%	2020 Julio	%
Fiscalía de la Nación	1	0.07	1	0.07
Fiscalías Supremas	7	0.49	7	0.49
Penal	2	0.14	2	0.14
Delitos Cometidos por Funcionarios Publicos	2	0.14	2	0.14
Civil	1	0.07	1	0.07
Contencioso Administrativo	1	0.07	1	0.07
Control Interno	1	0.07	1	0.07
Fiscalías Superiores	268	18.70	276	19.14
Oficinas Desconcentradas de Control Interno	33	2.30	33	2.29
Penal	132	9.21	139	9.64
Nacional Especializada Criminalidad Organizada	3	0.21	3	0.21
Nacional Especializada Anticorrupción	2	0.14	2	0.14
Especializada Anticorrupción	18	1.26	18	1.25
Nacional Especializada en Lavado de Activos	3	0.21	3	0.21
Delitos de Trata de Personas	1	0.07	1	0.07
Penal Nacional	3	0.21	2	0.14
Civil	5	0.35	5	0.35
Contencioso Administrativo	3	0.21	3	0.21
Civil y Familia	36	2.51	36	2.50
Mixta	23	1.61	23	1.60
Familia	2	0.14	2	0.14
Extincion del Dominio	2	0.14	2	0.14
Prevención del Delito	-	0.00	1	0.07
Violencia Contra la Mujer y los Integrantes del Grupo Familiar	2	0.14	3	0.21
Fiscalías Provinciales	1,157	80.74	1,158	80.31
Penal	445	31.05	443	30.72
Supra Provincial	9	0.63	10	0.69
Supra Prov.corp.lavado de Activos	2	0.14	2	0.14
Prov.corp.lavado de Activos	11	0.77	11	0.76
Delitos de Trata de Personas	9	0.63	9	0.62
Transito y Seguridad Vial	7	0.49	6	0.42
Aduanero y Propiedad Intelectual	8	0.56	8	0.55
Supraprovincial Especializada Anticorrupción	1	0.07	1	0.07
Corporativas Especializadas Anticorrupción	43	3.00	43	2.98
Tráfico Ilícito de Drogas	29	2.02	29	2.01
Supra Provincial Criminalidad Organizada	4	0.28	5	0.35
Corporativa Criminalidad Organizada	26	1.81	20	1.39
Mixta	130	9.07	119	8.25
Civil	8	0.56	8	0.55
Civil Y Familia	213	14.86	216	14.98
Familia	41	2.86	38	2.64
Familia Prev. Violencia Género	4	0.28	2	0.14
Turismo	1	0.07	1	0.07
Tributario	1	0.07	1	0.07
Materia Ambiental	41	2.86	43	2.98
Especializada en Violencia Contral la Mujer y los Integrantes del Grupo Familiar	28	1.95	49	3.40
Extincion de Dominio	24	1.67	24	1.66
Prevención del Delito	72	5.02	70	4.85
Total	1,433	100.00	1,442	100.00

Anexo 9. Cuestionario de entrevistas nacionales

Cuestionario de entrevista para ponentes nacionales

Título: *"Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020".*

NOMBRES Y APELLIDOS		GÉNERO	F	M
INSTITUCIÓN				
CORREO ELECTRÓNICO		CELULAR / TELÉFONO		
CARGO				

Objetivo General

Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos

1. ¿Cuáles son los problemas más recurrentes durante el desarrollo del proceso judicial entre una Fiscalía Especializada en Ciberdelincuencia y un Juzgado no Especializado en la materia?

2. ¿Cómo será el proceso de adaptación de la Unidad Fiscal Especializada en Ciberdelincuencia al no contar con Juzgados Especializados en la materia?

3. ¿Qué resultados a nivel investigativo se obtendrán con la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

4. ¿Qué medidas debe adoptar el Estado peruano para una eficiente investigación y administración de justicia en los casos de Ciberdelincuencia?

5. ¿Cómo debería distribuirse la Unidad Fiscal Especializada en Ciberdelincuencia para cubrir las zonas con mayor incidencia delictiva a nivel nacional?

Objetivo Específico 1

Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

6. ¿Qué opina sobre la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia como órgano consultor y no como órgano persecutor de estos delitos?

7. ¿En su opinión ante el aumento de los delitos informáticos fue oportuna la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

8. ¿Por qué es necesario que los fiscales cuenten con conocimientos en derecho y en tecnología para detectar, individualizar y perseguir los casos de Ciberdelincuencia?

9. ¿Cómo deben adaptarse los estudios jurídicos para el ejercicio de una adecuada defensa técnica ante la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia?

Objetivo Específico 2

Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

10. ¿Qué aspectos cree usted que se puedan potenciar en el Sistema de Justicia para la atención idónea de los casos de Ciberdelincuencia?

11. ¿Por qué hasta la fecha no hemos incorporado Juzgados Especializados en Ciberdelincuencia teniendo en cuenta la complejidad de estos casos?

12. ¿Por qué deberíamos incorporar una justicia especializada en Ciberdelincuencia?

13. ¿Alguna sugerencia o recomendación que desee agregar?

_____

Nombres y Apellidos del especialista

Anexo 10. Cuestionario de entrevistas internacionales

UNIVERSIDAD PRIVADA DEL NORTE

"Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020".

Cuestionario de entrevista para ponentes internacionales

Título: *"Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020".*

NOMBRES Y APELLIDOS		GÉNERO	F	M
INSTITUCIÓN				
CORREO ELECTRÓNICO		CELULAR / TELÉFONO		
CARGO				

Objetivo General

Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos

1. ¿Cuáles son las deficiencias de las Fiscalías y Juzgados Especializados en la atención de los casos de Ciberdelincuencia? (Argentina)

2. ¿Qué opina sobre los fiscales que investigan y los jueces que imparten justicia en los casos de Ciberdelincuencia?

3. ¿Por qué la mayoría de los casos de Ciberdelincuencia registrados en los últimos 5 años han sido archivados?

4. ¿Qué medidas debe adoptar el Estado argentino para una eficiente investigación y administración de justicia en los casos de Ciberdelincuencia?

Objetivo Específico 1

Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

5. ¿Qué se ha logrado con la incorporación de las Fiscalías Especializadas en Ciberdelincuencia?

6. ¿En su opinión ante el aumento de los delitos informáticos cómo ha sido la respuesta de las Fiscalías Especializadas en Ciberdelincuencia?

7. ¿Por qué es necesario que los fiscales cuenten con conocimientos en derecho y en tecnología para detectar, individualizar y perseguir los casos de Ciberdelincuencia?

8. ¿Cuáles son las ventajas y desventajas de incorporar Fiscalías Especializadas en Ciberdelincuencia?

9. ¿Qué aspectos cree usted que pueden ser emulados por los países de Sudamérica en base a la experiencia de Argentina con la incorporación de Fiscalías Especializadas en Ciberdelincuencia?

Objetivo Específico 2

Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

10. ¿Qué opina sobre la Administración de Justicia no Especializada en Sudamérica para los casos de Ciberdelincuencia?

11. ¿Qué opina sobre la necesidad de implementar Juzgados Especializados en Ciberdelincuencia como correlato de las Fiscalías Especializadas recientemente incorporadas?

12. ¿Qué recomendaría al Estado peruano para aprovechar la reciente incorporación de la Unidad Fiscal Especializada en Ciberdelincuencia en base a la experiencia argentina?

13. ¿Coméntenos sobre un caso emblemático vinculado a la Ciberdelincuencia que haya tenido que afrontar desde su rol como abogado(a)?

14. ¿Alguna sugerencia o recomendación que desee agregar?

_____

Nombres y Apellidos del especialista

Anexo 11. Cuestionario de entrevista al efectivo policial

Cuestionario de entrevista para el efectivo policial

Título: *"Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020".*

NOMBRES Y APELLIDOS		GÉNERO	F	M
INSTITUCIÓN				
CORREO ELECTRÓNICO		CELULAR / TELÉFONO		
CARGO				

Objetivo General

Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos

1. ¿Considera que la DIVINDAT cuenta con los recursos logísticos suficientes para atender las denuncias a nivel nacional?
2. ¿Cuál es el procedimiento para la atención de una denuncia interpuesta en provincia por la comisión de un presunto delito informático?

Objetivo Específico 1

Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea.

3. ¿A qué se debe el incremento anual de los delitos informáticos?
4. ¿Considera usted que el Fiscal actualmente se encuentra capacitado para investigar plenamente los delitos informáticos?
5. ¿Considera usted la necesaria implementación de Fiscalías Especializadas en Ciberdelincuencia?

Objetivo Específico 2

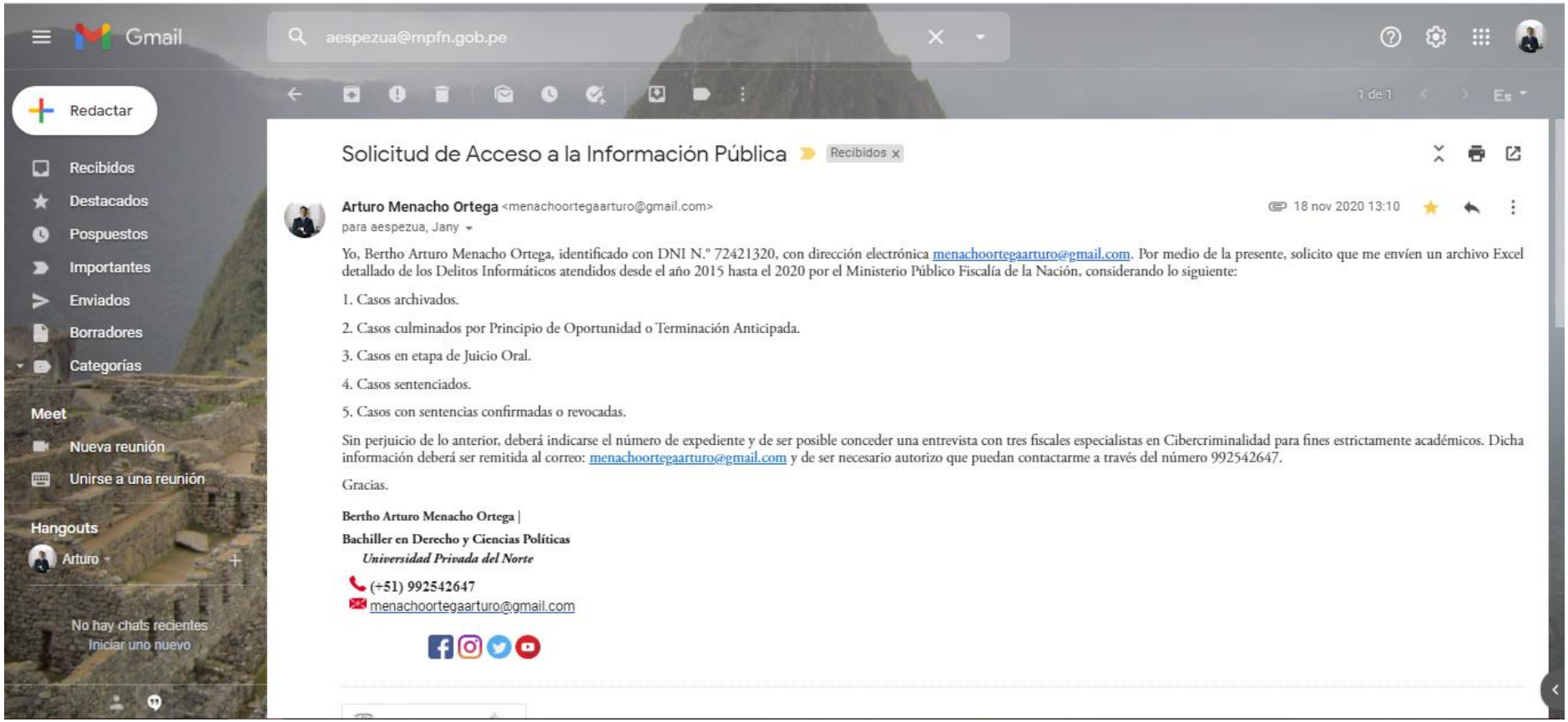
Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.

6. ¿Cuáles son los delitos informáticos más recurrentes en la DIVINDAT durante el 2020?

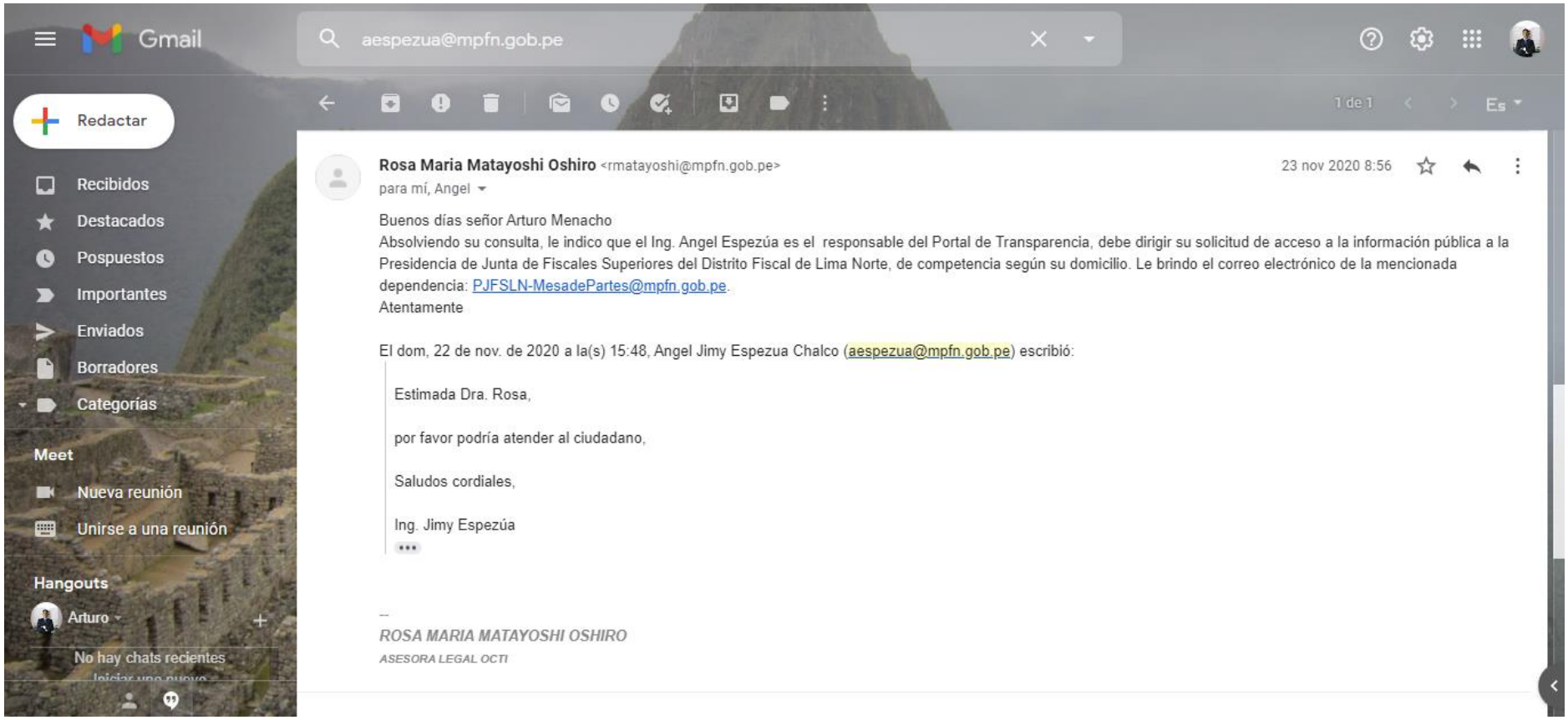
7. ¿Alguna sugerencia o recomendación que desee agregar?

Nombres y Apellidos del especialista

Anexo 12. Solicitud de acceso a la información pública al Ministerio Público



Anexo 13. Aclaración sobre la solicitud de acceso a la información pública al Ministerio Público

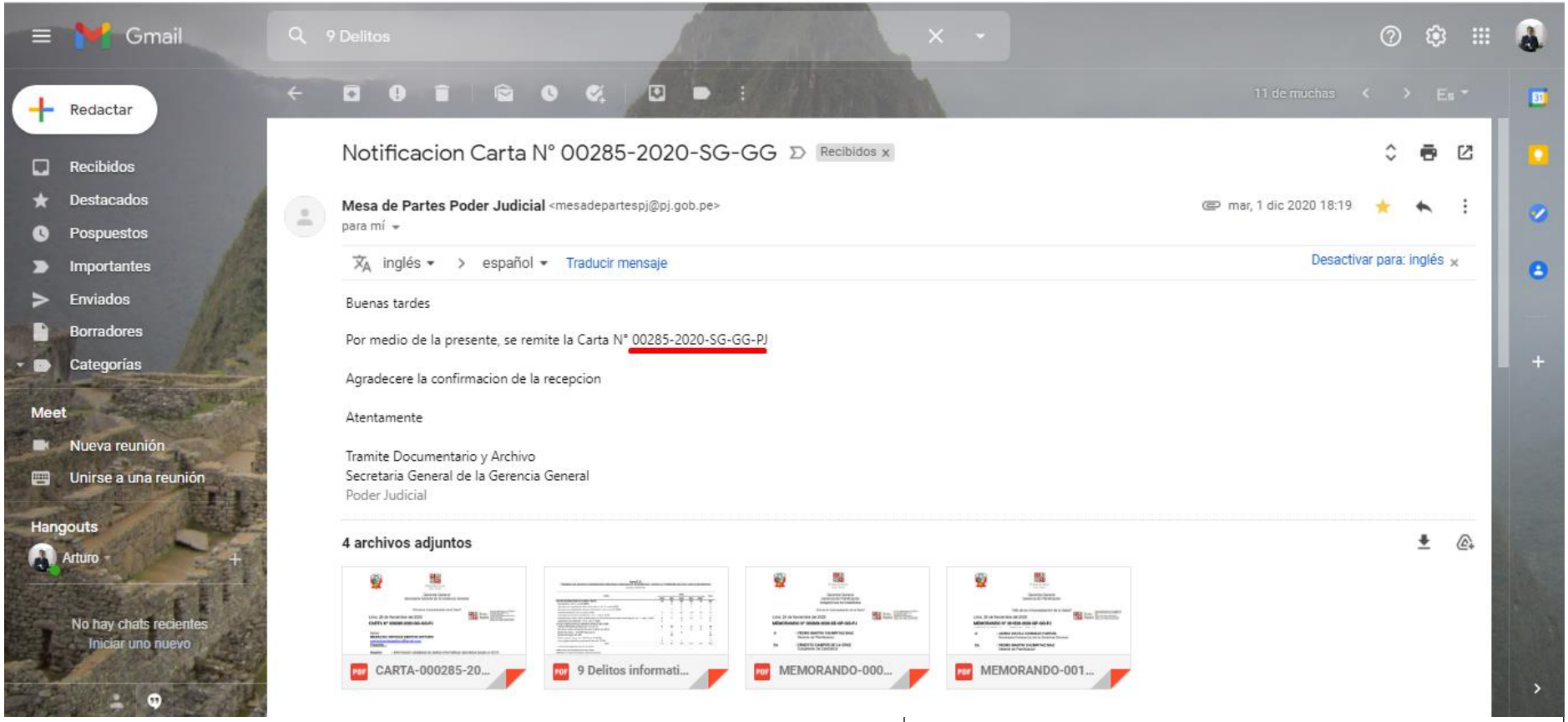


Anexo 14. Atención a la solicitud de acceso a la información pública al Ministerio Público

Link de acceso al material: http://bit.ly/2O3kyKY

Anexo 15. Solicitud de acceso a la información pública al Poder Judicial

Anexo n.° 16. Atención a la solicitud de acceso a la información pública al Poder Judicial



Link de acceso al material: http://bit.ly/3rhfPDU

Anexo 17. Lista de entrevistados internacionales

Especialista	Resumen de hoja de vida	País
Juan Carlos Carretero	Abogado especialista en ciberdelitos Organización de los Estados Americanos y la Universidad de León. Doctorando en ciencias jurídicas por la Universidad de la Matanza, Argentina. Miembro Titular de la Asociación Argentina de Derecho Internacional. Miembro Pleno de la Asociación Americana de Derecho Internacional Privado. Miembro de Asociation Society of Internacional Law. Director de la Carrera de Derecho de la Universidad de Flores.	Argentina
Sabrina Bibiana Lamperti	Abogada especialista en Criminalidad Económica, con tesis especializada en Delitos Informáticos. Maestranda en Ciencia, Tecnología y Sociedad. Detective Judicial en el Ministerio Público Fiscal de la policía de Buenos Aires e integrante del equipo de referentes en investigación digital por el departamento judicial Mar del Plata. Docente de Derecho Informático y de la Diplomatura en Informática Forense en la Universidad FASTA. Docente de la Diplomatura en Cibercrimen y Evidencia Digital de la Universidad Champagnat. Docente del Programa de Actualización en Ciberseguridad y Delitos Informáticos de la Facultad de Ciencias Sociales de la UBA. Investigadora del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense.	Argentina
Fernando Rincón Rodríguez	Abogado por la Universidad Libre de Colombia, Bogotá, Colombia. Director en la Especialización en Auditoría y Administración de la Información Tributaria por la Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Consultor jurídico del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de Universidad Santo Tomás de Aquino, USTA. Docente universitario de pregrado, posgrado y conferencista en las áreas de informática jurídica derecho informático.	Colombia
Santiago Martín Acurio Del Pino	Abogado y Doctor en Jurisprudencia por la Pontificia Universidad Católica del Ecuador. Especialista en Derecho Penal por la Universidad Andina Simón Bolívar. Magister en Tecnologías aplicadas a la Gestión y Práctica Docente por la Pontificia Universidad Católica del Ecuador, fue juez de la Corte Provincial de Justicia. Director de Tecnologías de la Información y la Comunicación de la Fiscalía General del Estado. Es profesor de Derecho Informático y TICS aplicadas al Derecho e Informática Jurídica de las Facultades de Ingeniería en Sistemas y Jurisprudencia de la Pontificia Universidad Católica del Ecuador desde el 2005. Es Profesor del Curso de Derecho Penal Informático, Marco Jurídico de la Seguridad de la ESPOL desde el año 2012. Instructor de Cibercrimen de la Organización de Estados Americanos OEA.	Ecuador
	Abogado por la Universidad Católica de Salta, cuenta con especialización en derecho informático, vivienda y seguridad pública. Es Investigador, conferencista y	

Diego Fernando Migliorisi Parrondo	escritor. Es director de Migliorisi Abogados desde el año 2018. Asimismo, pertenece al Colegio de Abogados del departamento judicial de Zárate-Campana donde colabora en la comisión de informática. Por último, integra las prestigiosas instituciones internacionales como la Asociación Internacional de Derecho Penal, la Federación Interamericana de Abogados, la Asociación Americana de Derecho Internacional Privado, la Technology Law Association (ItechLaw) y la American Society of Comparative Law.	Argentina
Rafael García Borda	Abogado. Director de la Sección Análisis Informático del departamento judicial Quilmes con asiento en Berazategui. Secretario en la Ayudantía Fiscal de Delitos Conexos a la trata de personas, pornografía infantil en internet y grooming. Es investigador digital en cibercrimen y docente universitario.	Argentina
Pablo Maza Correa	Abogado especialista en delitos informáticos y tecnologías e internet. Perito Judicial Informático y Fundador de la firma Intelectual Abogados. Forma parte de la Asociación Balear de Empresas de Software, Internet y Nuevas Tecnologías. Es conferencista nacional e internacional.	España
Marcelo Gabriel Ignacio Temperini	Abogado por la Universidad Nacional del Litoral. Posee una especialización en Cibercrimen y Evidencia Digital, los cuales fueron realizados en la Universidad Internacional de Catalunya - España. Posee una diplomatura en Derecho Informático por la Universidad Nacional de Río Negro. Es Técnico Analista de Seguridad y Vulnerabilidad de Redes de Información. Se encuentra doctorado en Derecho y realizando una investigación sobre Delitos Informáticos y Cibercrimen en el Centro de Investigación de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral. Asimismo, es Socio Fundador de AsegurarTe - Consultora en Seguridad de la Información. Es Cofundador y uno de los directores del Proyecto ODILA: Observatorio de Delitos Informáticos de Latinoamérica.	Argentina

Anexo 18. Lista de entrevistados nacionales

Especialista	Resumen de hoja de vida
Carlos Germán Guerrero Argote	Abogado por la Universidad Nacional de San Marcos (Perú), con estudios de postgrado en Gobernanza y Privacidad de Internet en la Universidad de San Andrés (Argentina). Sus áreas de trabajo son: Gobernanza de Internet, Economía Digital y Derechos Digitales. Es miembro de la ONG peruana Hiperderecho.
Ricardo Nicanor Elías Puelles	Abogado por la Pontificia Universidad Católica del Perú. Maestrando en Razonamiento Probatorio por la Universidad de Girona (España). Socio fundador del Estudio Elías Puelles, presidente del Observatorio Peruano de Cibercriminalidad y del Instituto Peruano de Razonamiento Probatorio y miembro de la Sociedad de Derecho y Empresas Digitales. Ha sido training coordinator del American Bar Asociation - Rule of Law Initiative y es docente en cursos de especialización en la Pontificia Universidad Católica del Perú y en la Universidad del Pacífico.
Javier Martin Cuadros Gutiérrez	Abogado con estudios en maestría en Ciencias Penales por la UNMSM. Con estudios de investigación criminal y Litigación Oral especializada en delitos informáticos – Cybercrime por la American Bar Asociation Rule of Law Initiative. Fiscal Adjunto Provincial de la Primera Fiscalía Provincial Corporativa Especializada en Delitos de Corrupción de Funcionarios de Lima - Sexto Despacho.
Elías Jiménez Gutierrez	Sub oficial de tercera, actualmente se desempeña como efectivo policial de la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional del Perú.

Anexo 19. Entrevista al Dr. Juan Carlos Carretero

Responder Responder a todos Reenviar MI

domingo 27/12/2020 04:34 p. m.

Bertho Arturo Menacho Ortega

Invitación a entrevista de tesis

Para juan_carretero@hotmail.com

CC Jany Giovana Bernal Gallardo

Cuestionario de entrevista de BAMO y JGBG - Ponentes internacionales.pdf
307 KB

Estimado Dr. Carretero:

Previo cordial saludo, esperando que usted y su familia se encuentren bien de salud, le saludamos desde Perú, Bertho Arturo Menacho Ortega y Jany Giovana Bernal Gallardo, Bachilleres en Derecho y Ciencias Políticas con mención en Derecho Empresarial por la Universidad Privada del Norte.

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Por ese motivo, remito el enlace para la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista al Dr. Juan Carlos Carretero

Time: Dec 29, 2020 04:00 PM Bogotá

Join Zoom Meeting

https://us04web.zoom.us/j/71336657834?pwd=WTQxNmQrdkdDZE5VdWhzNk5LUzVpUT09

Meeting ID: 713 3665 7834

Passcode: W57RUU

Atte.

Jany y Arturo.

Argentina

Anexo 20. Entrevista al Dr. Carlos Germán Guerrero Argote

Responder Responder a todos Reenviar MI

domingo 20/12/2020 11:50 p. m.

Bertho Arturo Menacho Ortega

Invitación a entrevista de tesis

Para carlos@hiperderecho.org

CC Jany Giovana Bernal Gallardo

Cuestionario de entrevista de BAMO y JGBG.pdf
249 KB

Estimado Dr. Guerrero:

Previo cordial saludo, esperando que usted y su familia se encuentren bien de salud, le saluda **Bertho Arturo Menacho Ortega** y **Jany Giovana Bernal Gallardo**, Bachilleres en Derecho y Ciencias Políticas con mención en Derecho Empresarial por la Universidad Privada del Norte.

Mediante el presente mensaje, agradeceríamos que nos brinde un espacio de su recargada agenda para poder entrevistarlo a través de la plataforma Zoom en el horario que usted disponga y reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada «***Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020***». Somos testigos de su constante contribución a la Comunidad Jurídica y de su gran aporte en materia de Ciberdelincuencia, por lo que sería un honor contar con su partici

Por último, sugerimos como fecha de entrevista el día domingo 27 de diciembre de 2020, a partir de las 11:00 a. m.

Quedamos atentos a su gentil respuesta.

Atte.

Jany y Arturo.

Perú

Anexo 21. Entrevista al Dra. Sabrina Bibiana Lamperti

Responder Responder a todos Reenviar MI

jueves 31/12/2020 08:58 p. m.

Bertho Arturo Menacho Ortega

Invitación a entrevista de tesis

Para slamperti@ufasta.edu.ar

CC Jany Giovana Bernal Gallardo

Cuestionario de entrevista de BAMO y JGBG - Ponentes internacionales.pdf
306 KB

Estimada Dra. Lamperti:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Considerando la fecha propuesta, hemos programada la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista magistral a la Dra. Sabrina Bibiana Lamperti

Time: Jan 4, 2021 02:00 p. m. Perú – **04:00 p. m. Argentina**

Join Zoom Meeting

https://us02web.zoom.us/j/81690347497?pwd=OHZDaFlDOHlLWFY2MDRYdnlDSFJsZz09

Meeting ID: 816 9034 7497

Passcode: 013606

Le deseamos un próspero año nuevo.

Atte.

Jany y Arturo.

Argentina

Anexo 22. Entrevista al Dr. Fernando Rincón Rodríguez

Invitación a entrevista de tesis

1

Jany Giovana Bernal Gallardo
Mar 29/12/2020 17:15
Para: ferinconr@gmail.com
CC: Bertho Arturo Menacho Ortega

Cuestionario de entrevista de...
325 KB

Estimado Dr. Rincón:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada «***Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020***». Considerando su asentimiento a la fecha propuesta, hemos programada la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista magistral al Dr. Fernando Rincón Rodríguez

Time: Jan 5, 2021 05:00 PM Lima

Join Zoom Meeting

https://us02web.zoom.us/j/82857757038?pwd=NjRrL0Qrd21OZzBIaXYrMnZiWGVWQT09

Meeting ID: 828 5775 7038

Passcode: 924700

Atte.

Jany y Arturo.

Colombia

Anexo 23. Entrevista al Dr. Ricardo Elías Puelles

Responder Responder a todos Reenviar MI

martes 22/12/2020 07:53 p. m.

Bertho Arturo Menacho Ortega

Invitación para entrevista de tesis

Para hola@cibercrimenperu.com

CC Jany Giovana Bernal Gallardo

Estimado Dr. Elías:

Previo cordial saludo, esperando que usted y su familia se encuentren bien de salud, le saluda **Bertho Arturo Menacho Ortega** y **Jany Giovana Bernal Gallardo**, Bachilleres en Derecho y Ciencias Políticas con mención en Derecho Empresarial por la Universidad Privada del Norte.

Mediante el presente mensaje, agradeceríamos que nos brinde un espacio de su recargada agenda para poder entrevistarlo a través de la plataforma Zoom en el horario que usted disponga y reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada «***Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020***». Somos testigos de su constante contribución a la Comunidad Jurídica y de su gran aporte en materia de Ciberdelincuencia, por lo que sería un honor contar con su parti

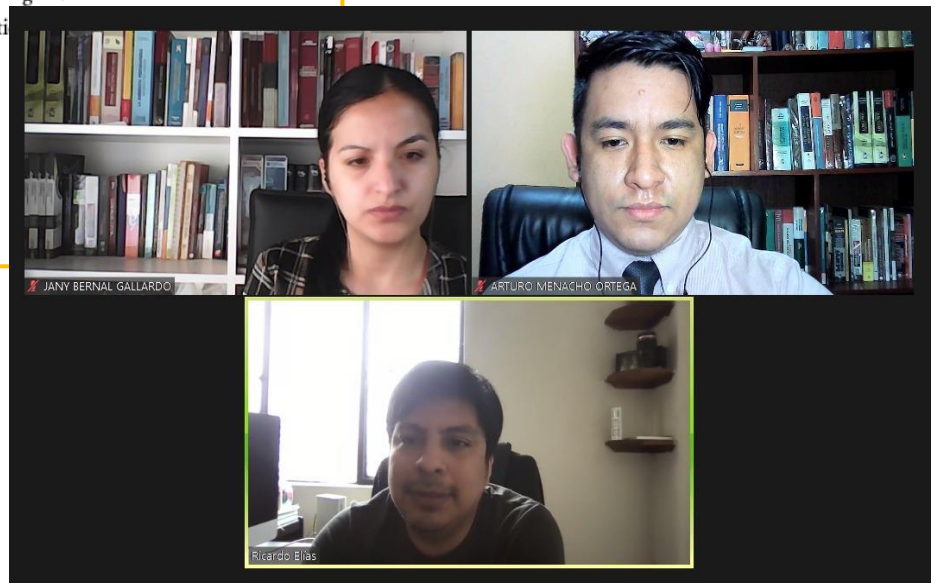
Por último, sugerimos como fecha de entrevista el día sábado 26 de diciembre de 2020, a partir de las 05:00 p. m.

Quedamos atentos a su gentil respuesta.

Atte.

Jany y Arturo.

Perú



Anexo 24. Santiago Martín Acurio Del Pino

Jany Giovana Bernal Gallardo
Lun 28/12/2020 12:54
Para: Santiago Acurio Del Pino <sacurio@hotmail.com>
CC: Bertho Arturo Menacho Ortega

Estimado Dr. Acurio Del Pino:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Considerando la fecha propuesta, hemos programada la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista magistral al Dr. Santiago Acurio Del Pino

Time: Jan 6, 2021 03:00 p. m. Perú - Ecuador

Join Zoom Meeting

https://us04web.zoom.us/j/78444596635?pwd=RHNvbWsrblhRRHhkOWpuSms0QUNLQT09

Meeting ID: 784 4459 6635

Passcode: e6DhhN

Atte.

Jany y Arturo.

Ecuador

Anexo 25. Diego Fernando Migliorisi Parrondo

Jany Giovana Bernal Gallardo
Lun 28/12/2020 9:10
Para: Diego Fernando Migliorisi <diegofernandomigliorisi@gmail.com>
CC: Bertho Arturo Menacho Ortega

Estimado Dr. Migliorisi:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Por ese motivo, remito el enlace para la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista al Dr. Diego Fernando Migliorisi Parrondo

Time: Jan 4, 2021 11:30 AM Lima

Join Zoom Meeting

https://us04web.zoom.us/j/76398855108?pwd=SXEvTStPVXNIUEV5dHBWUlhORWNjdz09

Meeting ID: 763 9885 5108

Passcode: aGfAr8

Atte.

Jany y Arturo.

Argentina

Anexo 26. Rafael García Borda

Responder Responder a todos Reenviar

lunes 28/12/2020 09:55 p. m.

Bertho Arturo Menacho Ortega

Invitación a entrevista de tesis

Para rafaelgarciaborda@gmail.com

CC Jany Giovana Bernal Gallardo

Cuestionario de entrevista de BAMO y JGBG - Ponentes internacionales.pdf
303 KB

Estimado Dr. García:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Considerando la fecha propuesta, hemos programada la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista magistral al Dr. Rafael García Borda

Time: Jan 11, 2021 - 10:00 a. m. Lima – **12:00 p. m. Argentina**

Join Zoom Meeting

https://us04web.zoom.us/j/79896015089?pwd=TTBoM2loSDhKRzZQQk8xaVg1T0dYUT09

Meeting ID: 798 9601 5089

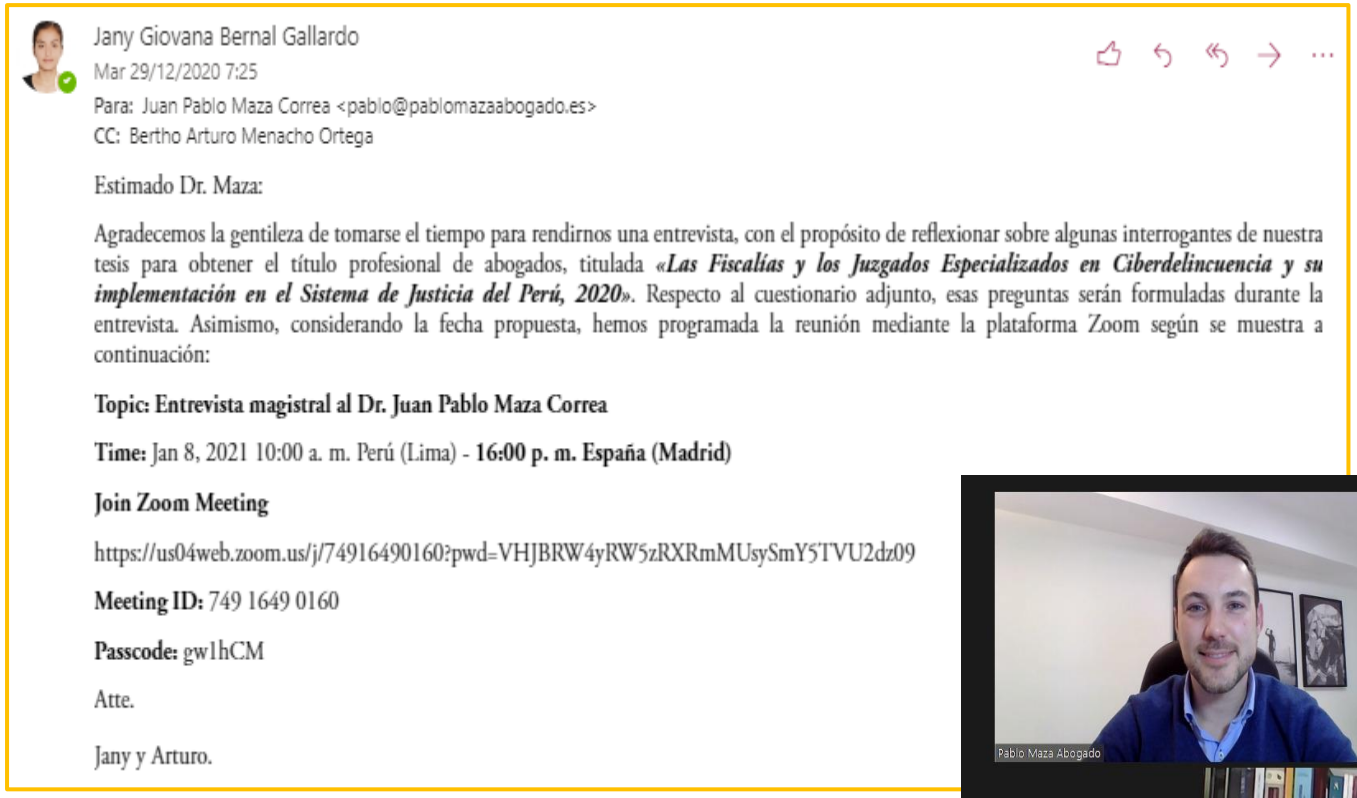
Passcode: dCmF1k

Atte.

Jany y Arturo.

Argentina

Anexo 27. Pablo Maza Correa



Jany Giovana Bernal Gallardo
Mar 29/12/2020 7:25
Para: Juan Pablo Maza Correa <pablo@pablomazaabogado.es>
CC: Bertho Arturo Menacho Ortega

Estimado Dr. Maza:

Agradecemos la gentileza de tomarse el tiempo para rendirnos una entrevista, con el propósito de reflexionar sobre algunas interrogantes de nuestra tesis para obtener el título profesional de abogados, titulada ***«Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia y su implementación en el Sistema de Justicia del Perú, 2020»***. Respecto al cuestionario adjunto, esas preguntas serán formuladas durante la entrevista. Asimismo, considerando la fecha propuesta, hemos programada la reunión mediante la plataforma Zoom según se muestra a continuación:

Topic: Entrevista magistral al Dr. Juan Pablo Maza Correa

Time: Jan 8, 2021 10:00 a. m. Perú (Lima) - **16:00 p. m. España (Madrid)**

Join Zoom Meeting

https://us04web.zoom.us/j/74916490160?pwd=VHJBRW4yRW5zRXRmMUsySmY5TVU2dz09

Meeting ID: 749 1649 0160

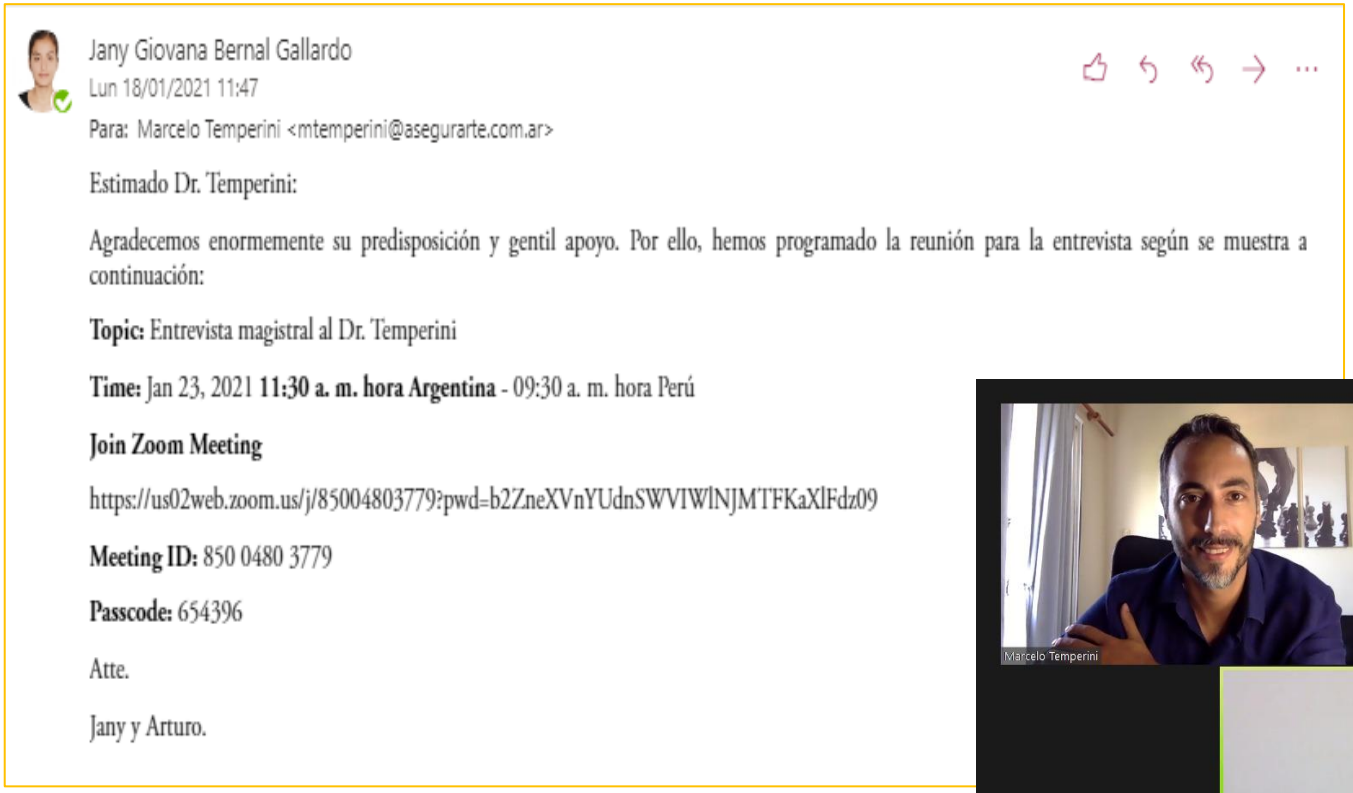
Passcode: gw1hCM

Atte.

Jany y Arturo.

España

Anexo 28. Marcelo Gabriel Ignacio Temperini



Jany Giovana Bernal Gallardo
Lun 18/01/2021 11:47
Para: Marcelo Temperini <mtemperini@asegurarte.com.ar>

Estimado Dr. Temperini:

Agradecemos enormemente su predisposición y gentil apoyo. Por ello, hemos programado la reunión para la entrevista según se muestra a continuación:

Topic: Entrevista magistral al Dr. Temperini

Time: Jan 23, 2021 **11:30 a. m. hora Argentina** - 09:30 a. m. hora Perú

Join Zoom Meeting

https://us02web.zoom.us/j/85004803779?pwd=b2ZneXVnYUdnSWVlWlNJMTFKaXlFdz09

Meeting ID: 850 0480 3779

Passcode: 654396

Atte.

Jany y Arturo.

Argentina

Anexo 29. Javier Martin Cuadros Gutiérrez

Responder Responder a todos Reenviar

miércoles 13/01/2021 08:01 p. m.

Bertho Arturo Menacho Ortega

RE: Invitación a entrevista de tesis

Para Javier Martin Cuadros Gutierrez

CC Jany Giovana Bernal Gallardo

Estimado Dr. Cuadros:

Agradecemos su predisposición y gentil apoyo, entendemos perfectamente su ardua labor en el ejercicio profesional, así como su recargada agenda. Por ello, considerando lo manifestado por usted hemos programado la reunión para la entrevista según se muestra a continuación:

Topic: Entrevista magistral al Dr. Javier Martin Cuadros Gutiérrez

Time: Jan 23, 2021 04:30 p. m. - Lima
Join Zoom Meeting
https://us02web.zoom.us/j/86895017795?pwd=bVdXaTFGZnhCcWJsT1k1TDlXUmd5Zz09
Meeting ID: 868 9501 7795
Passcode: 505485

Atte.

Jany y Arturo.

Perú

Anexo 30. Elías Jiménez Gutierrez

DIVINDAT DIRINCRI <divindat.dirincri@gmail.com> 9 nov 2020 23:09

para mí

Buenas noches,
Sr. Bertho Arturo Menacho Ortega
Se remite la información solicitada en formato excel, según lo coordinado en el email anterior, respecto a la entrevista se coordinará y se le dará el contacto por este medio, si tiene alguna duda respecto al cuadro no dude en hacer la consulta.

Dios Guarde a Ud.

CAP PNP
Teresa Milagros CHANG MORÁN
Área de Estadística-DIVINDAT- DIRINCRI-PNP

•••

--

ACUSAR RECIBO.

_____
ÁREA DE ESTADÍSTICAS
DIVINDAT-DIRINCRI PNP

CORREO INSTITUCIONAL: divindat.est@policia.gob.pe

Perú

Anexo 31. Matriz de consistencia

Problema	Objetivos	Hipótesis	Variables	Dimensiones	Metodología
Problema general ¿El Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos? **Problemas específicos** ¿De qué forma atienden las Fiscalías Provinciales no Especializadas en Ciberdelincuencia en el Sistema de Administración de Justicia del Perú, 2020? ¿De qué manera atienden los Juzgados no Especializados los casos de Ciberdelincuencia en el Sistema de Administración de Justicia del Perú, 2020?	**Objetivo general** Evaluar si el Sistema de Administración de Justicia en el Perú resulta apropiado para procesar la comisión de delitos informáticos. **Objetivos específicos** Detectar si la ausencia de una Fiscalía Especializada en Ciberdelincuencia impide la realización de una investigación idónea. Descubrir si la ausencia de un Juzgado Especializado en Ciberdelincuencia impide la realización de una eficiente Administración de Justicia.	**Hipótesis general** El Sistema de Justicia del Perú resulta inapropiado para procesar los delitos informáticos, en la medida que carece de Fiscalías y Juzgados Especializados en Ciberdelincuencia. **Hipótesis específicas** La ausencia de las Fiscalías Especializadas en Ciberdelincuencia incide negativamente en los actos de investigación fiscal, imposibilitando una representación idónea y generando un estado de indefensión de las víctimas y de la sociedad. La inexistencia de los Juzgados Especializados en Ciberdelincuencia incide negativamente al valorar y resolver con base a los medios probatorios aportados por las partes, afectando la predictibilidad de las resoluciones judiciales y el equilibrio del Sistema de Justicia del Perú.	**Variable independiente** Las Fiscalías y los Juzgados Especializados en Ciberdelincuencia. **Variable dependiente** Sistema de Justicia del Perú.	**Fiscalía Especializada en Ciberdelincuencia** Es el titular de la acción penal pública, defensor de la legalidad de los derechos ciudadanos, persecutor del delito y encargado de representar a la sociedad en juicio en los casos de ciberdelincuencia. **Juzgado Especializado en Ciberdelincuencia** Es aquel órgano jurisdiccional especializado en ciberdelincuencia que imparte justica en una determinada circunscripción geográfica. **Administración de Justicia** Es el aparato del Estado puesto al servicio de la administración de justicia, directa o indirectamente a través del Poder Judicial, el Ministerio Público y otras entidades públicas.	**Propósito:** Básica **Enfoque:** Mixto (Cualitativo y Cuantitativo) **Diseño:** No experimental **Alcance o nivel:** Exploratorio **Método:** Sociológico **Población:** P_1: Especialistas en la materia nacionales e internacionales. P_2: Base de datos de los casos seguidos en sede fiscal y judicial **Muestra:** Muestreo no probabilístico por conveniencia: M_1: 8 abogados especialistas internacionales. M_2: 3 abogados especialistas nacionales. M_3: 1 efectivo policial de la DIVINDAT. M_4: Reporte fiscal con 15 548 casos desde el año 2015 hasta el 2020. M_5: Reporte judicial con 440 sentencias condenatorias desde el año 2016 hasta el 2020. **Técnica de recolección de datos:** Entrevista no estructurada Análisis de documentos **Instrumento de recolección de datos:** Guía o **c**uestionario de entrevista (Enfoque cualitativo) Análisis documental (Enfoque cuantitativo) **Método de análisis de datos:** Tablas dinámicas y gráficos en Excel.