INFORME DE ANÁLISIS N°04

CIBERDELINCUENCIA EN EL PERÚ: PAUTAS PARA UNA INVESTIGACIÓN FISCAL ESPECIALIZADA

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

OFAEC OFICINA DE ANÁLISIS ESTRATÉGICO CONTRA LA CRIMINALIDAD

INFORME DE ANÁLISIS N°04

CIBERDELINCUENCIA: PAUTAS PARA UNA INVESTIGACIÓN FISCAL ESPECIALIZADA

OFICINA DE ANÁLISIS ESTRATÉGICO CONTRA LA CRIMINALIDAD

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

INFORME DE ANÁLISIS N°04
CIBERDELINCUENCIA: PAUTAS PARA UNA INVESTIGACIÓN FISCAL ESPECIALIZADA

ZORAIDA ÁVALOS RIVERA
Fiscal de la Nación

Comisión encargada de evaluar técnicamente la creación de un Piloto de Fiscalía Especializada o Unidad Especializada en Ciberdelincuencia del Ministerio Público (Resolución de Fiscalía de la Nación N°1025-2020-MP-FN)

Oficina de Anális Estratégico contra la Criminalidad-OFAEC

Ministerio Público
Av. Abancay cuadra 5 s/n Sede Central. Lima- Perú.
Central telefónica 625-5555
Anexos 5786-5787-5788
www.mpfn.gob.pe
Febrero 2021
Foto de portada: Freepik

CONTENIDO

PRESENTACIÓN

I. ANÁLISIS NORMATIVO.....PÁG. 6

1.1 INSTRUMENTOS NORMATIVOS
1.2 MARCO PENAL ACTUAL Y CONCEPTOS RELEVANTES

II. ESTADÍSTICAS OFICIALES.....PÁG 19

2.1. DENUNCIAS REGISTRADAS POR LA DIVISIÓN DE DELITOS DE ALTA TECNOLOGÍA
2.2 DENUNCIAS REGISTRADAS POR EL MINISTERIO PÚBLICO
2.3. FISCALÍAS ESPECIALIZADAS CONTRA LA CRIMINALIDAD ORGANIZADA
2.4. OFICINA DE PERITAJES DEL MINISTERIO PÚBLICO: ÁREA DE ANÁLISIS DIGITAL FORENSE
2.5. UNIDAD DE COOPERACIÓN JUDICIAL INTERNACIONAL Y EXTRADICIONES
2.6. ESCUELA DEL MINISTERIO PÚBLICO

III. ENTREVISTAS A ACTORES DEL SISTEMA.....PÁG. 34

3.1. REPRESENTANTES DE LAS FISCALÍAS CON MAYOR INCIDENCIA DE DELITOS INFORMÁTICOS.
3.2. PERITOS DEL ÁREA DIGITAL FORENSE DE LA OFICINA DE PERITAJES DEL MINISTERIO PÚBLICO

IV. ANÁLISIS COMPARADO DE UNIDADES ESPECIALIZADAS.....PÁG 47

4.1. ESPAÑA
4.2. PORTUGAL
4.3. CHILE
4.4. PARAGUAY
4.5. COLOMBIA
4.6. COSTA RICA
4.7. ARGENTINA

V. UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DEL MINISTERIO PÚBLICO.....PÁG 61

CONCLUSIONES.....PÁG 65
RECOMENDACIONES.....PÁG 67

BIBLIOGRAFÍA.....PÁG 69

PRESENTACIÓN

El auge de la ciberdelincuencia está estrechamente vinculado al desarrollo tecnológico informático. Según la ONU (2019) las tecnologías de la información y comunicación crearon oportunidades para los delincuentes y dieron lugar a un aumento de la tasa y la diversidad de los delitos cometidos en el mundo digital y a través de él. Si bien no se cuenta con cifras oficiales que reflejen las consecuencias de este delito, la OEA estima que la ciberdelincuencia ocasiona costos de aproximadamente 575,000 millones de dólares al año, suma que llega a representar el 0.5% del Producto Bruto Interno mundial y considera que en América Latina y el Caribe estos costos son de aproximadamente 90,000 millones de dólares anuales. (OEA 2016, p. IX).

En nuestro país las cifras del Ministerio Público evidencian que las denuncias por delitos informáticos se incrementan aceleradamente año a año. De octubre de 2013 a julio de 2020, las fiscalías penales y mixtas registraron 21,687 denuncias, de las cuales el 40% proviene del 2019. Sin embargo, en ese mismo periodo se archivó el 58% de las mismas y se emitieron tan solo 108 sentencias, generando una importante carga fiscal y una sensación de impunidad e inseguridad.

Dada esta situación, desde el Ministerio Público se propuso desarrollar un estudio descriptivo que, con información policial y fiscal, tanto cualitativa como cuantitativa, permitiese reconocer las fortalezas y debilidades de la capacidad estatal para abordar este problema de política pública. Como insumo teórico y normativo se tomó en cuenta los preceptos y recomendaciones del Convenio de Budapest suscrito por el Estado peruano en el año 2019, y las definiciones y disposiciones de la Ley de Delitos Informáticos (Ley N° 30096) vigente desde el 2013. Como resultado se obtuvo este informe que es actual y relevante, a sabiendas que aún vivimos una pandemia mundial por COVID-19 en donde nuestro país es uno de los más afectados y los delitos cibernéticos se vuelven más recurrentes dejando entre sus víctimas ciudadanos de diversas edades, así como instituciones públicas y privadas.

El presente texto empieza con un análisis de la normatividad vigente. Luego presenta estadística descriptiva en base a denuncias. Paso seguido se analizan entrevistas a actores relevantes en la investigación penal. Se incluye también un análisis comparado con otras unidades especializadas a nivel internacional. Hacia el final se dedica un capítulo a la Unidad Fiscal Especializada en Ciberdelincuencia de reciente creación en Perú. Por último se concluye con recomendaciones que tienen como objetivo fortalecer las capacidades institucionales para investigar los delitos informáticos.

Con esta publicación, el Ministerio Público reafirma la importancia de la especialización de la investigación fiscal, la cual no se llegó a priorizar en años previos, pero que ahora se constituye como parte de nuestra política institucional, y que si bien empieza por una Unidad Fiscal Especializada en Ciberdelincuencia con competencia nacional, la consigna es que pueda extenderse, próximamente, a la implementación de fiscalías penales especializadas en los diferentes distritos fiscales a nivel nacional.

I. ANÁLISIS NORMATIVO

1. LOS INSTRUMENTOS NORMATIVOS DE RELEVANCIA

Los instrumentos normativos han sido organizados en instrumentos internacionales, legislación nacional, resoluciones de la Fiscalía de la Nación y en procedimientos de actuación.

Instrumentos internacionales

Siguiendo la metodología planteada para el desarrollo de este informe se recopilaron normas de relevancia internacional en materia de ciberdelincuencia. Cabe resaltar, que no se restringió el análisis a aquellos tratados vinculantes para el Estado peruano, sino que en general se identificaron instrumentos de derecho internacional que brindan lineamientos importantes para la planificación de los diferentes aspectos a considerar para la creación de una Unidad Especializada en la materia.

Entre estos es posible distinguir aquellos surgidos en el marco del Sistema de las Naciones Unidas, tanto tratados internacionales que protegen derechos y libertades básicas como resoluciones que contienen recomendaciones de prevención y persecución de la ciberdelincuencia en sus diversas formas:

- La Resolución 64/211 sobre la Creación de una Cultura Mundial de Seguridad Cibernética y Balance de las Medidas Nacionales para Proteger las Infraestructuras de Información Esenciales, aprobada por la Asamblea General de las Naciones Unidas, el 21 de diciembre de 2009.

- La Resolución 56/121 sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, aprobada por la Asamblea General de las Naciones Unidas, el 19 de diciembre de 2001.

Por otra parte, en el sistema interamericano se cuenta también con convenios de relevancia sobre aspectos procesales para la investigación de delitos informáticos, algunos de estos aún no ratificados, así como también encontramos instrumentos de *soft law* y políticas en materia de ciberdelincuencia como son:

- El Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia (2014), firmado el 28 de mayo de 2014, como parte de las acciones impulsadas por la Conferencia Ministros de Justicia de Iberoamérica (COMJIB). Pendiente aún de ratificación por parte del Estado peruano.

- La Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética: un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética (2004), aprobada por la Asamblea General de la Organización de Estados Americanos, el 08 de junio de 2004 mediante Resolución AG/RES. 2004 (XXXIV-0/04). Insta a los Estados miembros a implementar una serie de recomendaciones en la materia.

- El Protocolo Facultativo Relativo a la Convención Interamericana sobre Asistencia Mutua en Materia Penal (1993), adoptado por la Organización de Estados Americanos el 6 de noviembre de 1993. Entró en vigor el 4 de julio de 2002. No ha sido suscrito por el Perú.

El sistema europeo es el que más avances ha mostrado en la generación de políticas internacionales en la materia, de manera que provee estándares de referencia a nivel internacional, incluyendo tratados internacionales multilaterales abiertos a la adhesión de Estados no miembros, como es el caso del Convenio de Budapest, así como directivas, y otros instrumentos de interés. Entre otros, cabe resaltar:

- La Directiva 2016/680 del Parlamento Europeo y del Consejo de Europa relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos; del 27 de abril de 2016.

- El Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual (2007). En vigor desde el 1 de julio de 2010, luego de su ratificación por parte de cinco países miembros de la Unión Europea. Abierto a la firma de otros países, sin embargo, a la fecha solo ratificado a nivel de la Unión Europea.

- Protocolo Adicional al Convenio sobre Ciberdelincuencia, relativo a la Penalización de Actos de Naturaleza Racista y Xenófoba cometidos por Medio de Sistemas Informáticos (2002), adoptado por el Consejo de Comité de Ministros el 7 de noviembre de 2002. En vigor desde marzo de 2006.

- El Protocolo Adicional al Convenio N°108, relativo a Autoridades de Supervisión y Flujos Internacionales de Datos (2001), adoptado por el Consejo de Europa el 8 de noviembre de 2001.

- El Convenio sobre ciberdelincuencia o Convenio de Budapest (2001), aprobado por el Consejo de Europa el 8 de noviembre de 2001, en vigor desde julio de 2004. El 13 de febrero de 2019, mediante Resolución Legislativa N°30913, el Congreso de la República aprobó la adhesión del Perú a este Convenio, el mismo que fue ratificado mediante Decreto Supremo N°010-2019-RE, el 09 de marzo de 2019.

- El Convenio N°108 del Consejo de Europa para la protección de personas con respecto al tratamiento informatizado de datos personales (1981), adoptado por el Consejo de Europa el 8 de enero de 1981.

Legislación Nacional

En cuanto a los avances logrados a través de nuestra legislación nacional estos involucran, por una parte, el ámbito más global referido a la ciberdefensa:

- Ley N°30999, Ley de Ciberdefensa, aprobado el 26 de agosto de 2019.

Por otra parte, encontramos mayor precisión y desarrollo en las normas relativas a la implementación de protecciones a las libertades civiles en el ámbito de las comunicaciones y la privacidad de datos, entre las cuales resaltan las siguientes:

- Ley N°29733, Ley de Protección de Datos personales, del 3 de julio de 2011.

- Ley N°28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), del 11 de abril de 2005.

- Ley N°27806, Ley de transparencia y acceso a la información pública, del 2 de agosto de 2002.

- Ley N°27291, Ley que modifica el Código Civil permitiendo la utilización de medios electrónicos para la manifestación de la voluntad y la utilización de la firma electrónica, del 24 de junio de 2000.

- Ley N°27269, Ley de Firmas y Certificados Digitales, del 25 de mayo de 2000.

- Decreto Legislativo N°681, relativo al uso de tecnologías avanzadas en materia de archivos, del 11 de noviembre de 1991.

- Decreto Supremo N°050-2018-PCM, que aprueba la definición de Seguridad Digital en el Ámbito Nacional, de fecha 14 de mayo de 2018.

- Decreto Supremo N°081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017, de fecha 09 de julio de 2013.

Entre la legislación relevante en materia de criminalización de la ciberdelincuencia, así como en cuanto a proveer un marco jurídico para su persecución se encuentran:

- Ley N°30096, Ley de delitos informáticos, del 21 de octubre de 2013, modificada por la Ley N°30171, de fecha 17 de febrero de 2014.

- Ley N°30077, Ley contra el crimen organizado, del 19 de agosto del 2013.

- Ley N°27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, de fecha 10 de abril de 2002, modificada por la Ley N°30096 del 2013, que agrega los delitos informáticos a la lista de delitos en que los jueces tendrán la facultad constitucional para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional

- Decreto Legislativo N°1410, que incorpora el delito de acoso, acoso sexual, chantaje sexual y difusión de imágenes, materiales audiovisuales o audios con contenido sexual al código penal, y modifica el procedimiento de sanción del hostigamiento sexual, del 11 de setiembre de 2018.

- Decreto Legislativo N°1244, que fortalece la lucha contra el crimen organizado y la tenencia ilegal de armas, del 27 de octubre de 2016.

- Decreto Legislativo N°1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, del 26 de julio de 2015.

Resoluciones de Fiscalía de la Nación

Por su parte, el Ministerio Público ha emitido disposiciones a través de resoluciones que crean condiciones para una afectiva lucha contra la ciberdelincuencia y regulan aspectos concernientes al uso de sistemas de información, así como de protección de datos, entre los que encontramos:

- Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN, de fecha 30 de diciembre de 2020, que crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima.

- Resolución de la Fiscalía de la Nación N°2189-2018-MP-FN, de fecha 27 de junio de 2018, que aprueba el Reglamento Interno para el Acceso y uso de Herramientas y Servicios Informáticos en el Ministerio Público.

- Resolución de Fiscalía de la Nación N°2432-2016-MP-FN, de fecha 23 de mayo de 2016, que aprueba las Cláusulas de Confidencialidad y de Protección de Datos Personales.

- Resolución de la Fiscalía de la Nación N°6644-2015-MP-FN, de fecha 31 de diciembre de 2015, que aprueba la Política de Protección de Datos Personales del Ministerio Público.

Específicamente, en materia de seguridad de la información, la Fiscalía de la Nación ha emitido la siguiente resolución:

- Resolución de Fiscalía de la Nación N°2895-2017-MP-FN, que aprueba la "Política y Objetivos de la Seguridad de la Información y el alcance del Sistema de Gestión de Seguridad de la Información".

Procedimientos de actuación

Cabe señalar que existen guías, manuales y protocolos que buscan estandarizar procedimientos relacionados con investigación y persecución de delitos informáticos, entre los que destacan:

- La Guía de Análisis Digital Forense del Ministerio Público, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG, del 11 de agosto de 2020.

- El "Manual para el Recojo de Evidencia Digital", aprobado por el Ministerio del Interior a través de Resolución Ministerial N° 848-2019-IN.

- La "Guía Práctica para solicitar la Prueba electrónica a través de las Fronteras" elaborada por la Organización de las Naciones Unidas sobre las Drogas y el Crimen (UNODC), Dirección Ejecutiva del Comité de lucha contra el Terrorismo (CTED) y la Asociación Internacional de Fiscales (IAP), del 2019.

- El "Manual de Evidencia Digital", elaborado por el Ministerio de Justicia y Derechos Humanos y la American Bar Association – ABA ROLI, del 2017.

Asimismo, para la labor de análisis digital forense se cuenta con las siguientes normas técnicas:

- Norma ISO/IEC 27037:2012 "Lineamientos para la identificación, recolección, adquisición y preservación de evidencia digital".

- Norma ISO/ IEC 27042/2015 "Lineamientos para la identificación, recolección, adquisición y preservación de evidencia digital".

- Norma ISO/IEC 27041/2015 “Orientación para asegurar la idoneidad y adecuación de los métodos de investigación de incidentes y las fases de examen (o análisis) e interpretación del proceso de análisis forense digital.”.

1.2. MARCO PENAL ACTUAL Y CONCEPTOS RELEVANTES

El concepto de Ciberdelincuencia

En el X Congreso de Naciones Unidas sobre Prevención del delito y Tratamiento del Delincuente, celebrado en Viena en abril del 2000 se realizó una importante distinción que contribuye a una mejor precisión del concepto.

- La Ciberdelincuencia puede entenderse en sentido estricto, comprendiendo cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y datos que se procesan.

- La Ciberdelincuencia también puede entenderse en sentido amplio, comprendiendo cualquier ilícito cometido por medio de un sistema informático o una red de computadores o relacionados con estos, incluyendo la posición o puesta a disposición de información mediante sistemas de información o redes de computadores.

En efecto, a nivel doctrinario se cuenta con diversas definiciones de lo que es ciberdelincuencia, delitos informáticos o cibercrimen; algunas de las cuales ponen el acento en ciertos aspectos de la ciberdelincuencia, más que en otros. Por ejemplo, frente a quienes trataron de identificar la ciberdelincuencia con aquellas actividades ilícitas realizadas a través de redes electrónicas mundiales o sistemas de información interconectados en el sentido que lo propugna la cibernética o el uso del internet, se propuso el concepto de delitos informáticos que permite precisar que la afectación puede darse a través y hacia sistemas informáticos autónomos que no están conectados a una red.

No obstante, a fin de reducir dichas disquisiciones teóricas, que surgen además sobre un campo más tecnológico que jurídico, desde una perspectiva aplicada a nuestros fines, distinguimos en efecto conceptualizaciones que tienden a otorgar a la ciberdelincuencia un contenido en el sentido estricto del término, y otras que tienden a otorgar un sentido amplio al mismo; finalmente otras que intentan unificar dichos sentidos.

Así, entre las primeras conceptualizaciones encontramos lo planteado por Felipe Villavicencio, quien desde una perspectiva tendiente a lo restrictivo señala: “Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasión a computadoras, correo o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente

pueden ser cometidas a través de la tecnología(…)De la concepción de los delitos informáticos se entiende que no todo delito puede ser clasificado como delito informático por el solo hecho de haber empleado la computadora u otro instrumento tecnológico." (Villavicencio, 2014, p.286).

Ahondando más bien en lo que buscan las definiciones más amplias, Miró Linares explica la ciberdelincuencia como categoría tipológica antes que normativa entendiendo que: "Si utilizamos el término de forma amplia, podremos definir como cibercrimen cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo, el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet(…)Desde una concepción amplia, debe entenderse por cibercrimen cualquier delito en el que las tecnologías de la información juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que se derivan de ello". (Miró, 2013, p.10).

Así, para efectos del análisis desarrollado en el presente informe, se adoptó una posición intermedia en referencia a lo esbozado por el Convenio de Budapest y a entender que los delitos informáticos o la cibercriminalidad hacen referencia a aquel fenómeno criminal que aborda los hechos y conductas dirigidas a la protección de la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, los que tienen ocasión a partir del desarrollo científico - tecnológico de la humanidad, y además que para su ejecución, emplean los sistemas informáticos, datos informáticos y tecnologías de la información y comunicación (TIC´s), siempre que éstos ostenten un marco convencional de protección o se encuentren regulados como tal (instrumentos), en los tipos penales de cada legislación nacional.

Por otra parte, cabe resaltar que un concepto conexo es el de Ciberseguridad, el mismo que hace referencia a la organización y recolección de recursos, procesos, tecnologías o estructuras utilizadas para proteger el ciberespacio y los sistemas potenciados por el ciberespacio (computadoras, servidores, individuos, organizaciones, redes, etc.) de ataques u ocurrencias que vulneren derechos.

El Convenio de Budapest y la legislación penal nacional

La relevancia del Convenio de Budapest o denominado "Convenio de Ciberdelincuencia", a la hora de analizar el presente tema, implica hacer referencia a la adecuación de nuestra legislación penal respecto a esta clase de delitos o de manera conexa. Debemos precisar que el Convenio de Budapest, es un tratado internacional generado por los países miembros del Consejo de Europa, con la finalidad de combatir el fenómeno de la ciberdelincuencia, que contiene un modelo de legislación-tipo, el cual trasunta en mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y cooperación jurídica internacional.

Asimismo, conviene anotar que el Perú, en el año 2014, solicitó suscribirse al precitado convenio; siendo que, en el año 2015, el Consejo Europeo aprobó nuestro pedido. Posteriormente, el Congreso de la República, el 12 de febrero de 2019, aprobó el Convenio de Budapest, a través de la Resolución Legislativa N° 30913 -con algunas reservas-, el cual fue ratificado, por el Poder Ejecutivo, mediante Decreto Supremo N° 010-2019-RE, del 09 de marzo de 2019, estableciéndose el día 01 de diciembre de 2019 como fecha de entrada en vigor.

En este sentido, debemos señalar la existencia de un primer grupo de delitos denominados contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos referidos en el Convenio de Budapest que encuentran su similitud en los artículos 2, 3, 4, 7 y 10 de la Ley N° 30096, Ley de Delitos Informáticos y modificatorias. Tal como se gráfica a continuación:

I. DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS	
CONVENIO DE BUDAPEST	**LEGISLACIÓN PERUANA**
Artículo 2. Acceso Ilícito	Artículo 2. Acceso Ilícito
Artículo 3. Interceptación Ilícita	Artículo 7. Interceptación de datos informáticos
Artículo 4. Ataques a la integridad de los datos	Artículo 3. Atentado a la integridad de datos informáticos
Artículo 5. Ataques a la integridad del sistema	Artículo 4. Atentado a la integridad de sistemas informáticos
Artículo 6. Abuso de los dispositivos	Artículo 10. Abuso de mecanismos y dispositivos informáticos

Asimismo, en el Convenio de Budapest se hace referencia a un segundo grupo de delitos denominados "delitos informáticos", los cuales comprenden las siguientes modalidades: falsificación informática (artículo 7) y fraude informático (artículo 8), los mismos que podríamos encontrar comparación con los artículos 8 y 9 de la Ley N° 30096, Ley de Delitos Informáticos y modificatorias. Como se muestra en el gráfico siguiente:

II. DELITOS INFORMÁTICOS	
CONVENIO DE BUDAPEST	**LEGISLACIÓN PERUANA LEY 30096, LEY DE DELITOS INFORMÁTICOS**
Artículo 7– Falsificación Informática	Art. 9. Suplantación de identidad.
Artículo 8 – Fraude Informático	Art. 8 Fraude Informático[1].

Debemos precisar que los dos grupos de delitos señalados precedentemente son los que se conocen como el "núcleo duro" de la ciberdelincuencia.

Si seguimos explorando el relevante Convenio de Budapest, encontramos un tercer grupo referidos a los delitos relacionados a la pornografía infantil, el mismo que podemos encontrar comparación con el artículo 183-A del Código Penal[2]. Tal como se observa a continuación:

III. DELITOS RELACIONADOS CON EL CONTENIDO	
CONVENIO DE BUDAPEST	**LEGISLACIÓN PERUANA CÓDIGO PENAL**
Artículo 9 – Delitos relacionados con la Pornografía Infantil.	Artículo 183-A. Pornografía Infantil.

Por otro lado, en el Convenio citado se encuentra un cuarto grupo referido a "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines", los mismos que podemos encontrar una comparación con los denominados delitos contra los derechos intelectuales previstos en el Código Penal peruano, en el Libro Segundo, Título VII- Delitos contra Derechos Intelectuales, que contiene el Capítulo I (Delitos contra los derechos de autor y conexos) y Capítulo II (Delitos contra la propiedad industrial). Tal como se muestra a continuación:

1. La CONAPOC (2020, p.31), citando a Gercke 2014, señala: "Cabe hacer una diferenciación entre el fraude informático y el fraude convencional, este último también conocido como estafa, su distinción principal consiste en el objetivo que persigue, es decir, si el estafador trata de manipular a una persona, mediante engaño suficiente, se considera por lo general que se trata de un delito de estafa. Mientras que en el fraude informático el objetivo apunta a los sistemas informáticos o de procesamiento de datos, es decir, la manipulación de sistemas informáticos con propósitos fraudulentos que generen perjuicio en el patrimonio de terceros".
2. Se precisa que si bien no constituye el núcleo de protección a datos y sistemas informáticos. El desarrollo alcanzado por los criminales para dificultar su identificación a través de la web requiere dadas las modalidades cada vez más sofisticadas empleadas, de una especialización en la investigación, así como protección reforzada, como se desprende de instrumentos internacionales como el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000) y el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual del 2007.

IV. DELITOS RELACIONADOS CON LA PROPIEDAD INTELECTUAL Y AFINES	
CONVENIO DE BUDAPEST	**LEGISLACIÓN PERUANA CÓDIGO PENAL**
Artículo 10 – Delitos relacionados con la propiedad intelectual y afines	Artículo 220-A. Elusión de medida tecnológica efectiva Artículo 220-B. Productos destinados a la elusión de medidas tecnológicas. Artículo 220-C. Servicios destinados a la elusión de medidas tecnológicas Artículo 222-A. Penalización de la clonación o adulteración de terminales de telecomunicaciones

Código Penal peruano en el marco de la ciberdelincuencia

Existen una diversidad de delitos conexos que no se consideran dentro del universo de delitos contenidos en el Convenio de Budapest, que protegen diferentes bienes jurídicos, sin embargo, consideramos que debemos enumerarlos dado que para su comisión o referencia típica se hace uso de tecnologías de la información y comunicación, lo cual podría resultar útil al momento de establecer indicadores en aquellos casos en los cuales la obtención de la denominada prueba digital o electrónica sea determinante para la investigación.

V. OTROS DELITOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUAL	
DELITOS	**NORMA LEGAL**
Art.5. de la Ley N°30096, Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.	Ley N° 30096, modificada por la Ley N°30171 del 2014
Artículo 183-B. Proposiciones a niños, niñas y adolescentes con fines sexuales.	Incorporado por Ley N° 30171 en 2014 y modificado por Ley N° 30838 del 2018 y la Ley N° 30963, del 2019.
Artículo 176-B. Acoso Sexual. -	Incorporado por DL N°1410 del 2018.
Artículo 176-C. Chantaje Sexual.	Incorporado por DL N°1410 del 2018.
Artículo 177. Formas por uso de TIC Agravadas.	Modificado por la Ley N°30838 de agosto del 2018.

VI. DELITOS CONTRA LA LIBERTAD PERSONAL	
DELITOS	**NORMA LEGAL**
Art. 151-A. Acoso (Tercer párrafo)	Incorporado por DL. N°1410 del 2018.

VII. DELITOS CONTRA LA INTIMIDAD Y VIOLACIÓN DEL SECRETO A LAS COMUNICACIONES	
DELITOS	**NORMA LEGAL**
Art. 154. Violación de la intimidad*	De Acción privada según DL N°1237 del 2015
Art. 154-A. Tráfico Ilegal de Datos Personales	Incorporado por Ley N°30171 en el 2014
Art. 154-B. Difusión de imágenes, materiales audiovisuales o audios con contenido sexual	Incorporado por DL N° 1410 del 2018. De Acción Privada según DL N°1237 del 2015
Art. 155. Agravante por razón de la función	Modificado por DL N°1237 del 2015
Art. 157. Organización y Uso indebido de archivos computarizados	
Art. 162. Interferencia Telefónica	
Art. 162-A. Posesión o comercialización de equipos destinados a la interceptación telefónica o similares	
Art. 162-B. Interferencia de comunicaciones electrónicas, de mensajería instantánea y similares	

*De acción privada

VIII. DELITOS CONTRA EL PATRIMONIO	
DELITOS	**NORMA LEGAL**
Artículo 196-196-A inciso 5 Estafa Agravada	Incorporado por Ley N°30076 Modificado por DL N°1351 del 2017

IX. DELITOS CONTRA LA TRANQUILIDAD PÚBLICA	
DELITOS	**NORMA LEGAL**
Artículo 316-A. (último párrafo) Apología del delito de terrorismo.	Incorporado por la Ley N° 30610 del 2017.
Artículo 323. (segundo párrafo Discriminación agravada	Modificado por Ley N° 30171 en el 2014

X. DELITOS INFORMÁTICOS COMETIDOS POR ORGANIZACIÓN CRIMINAL	
DELITOS	**NORMA LEGAL**
Artículo 3, inciso 9. Delitos Informáticos previstos en la ley penal.	Ley N°30077 del 2013 modificada por el Decreto Legislativo N°1244 del 27 de octubre del 2016.
Artículo 11 de la Ley de Delitos Informáticos.	Agravante de la Ley N° 30096, Ley de Delitos Informáticos

Con respecto a los diferentes tipos penales aquí citados solo es referencial, lo cual no excluiría otros que puedan ser cometidos mediante las tecnologías de la información o comunicación pese a que no se señalen expresamente en determinado tipo penal.

La necesidad de adecuación de la legislación penal peruana al Convenio de Budapest

Como se ha podido apreciar en la legislación penal peruana existe un marco normativo compatible con el Convenio de Budapest, así conceptualmente podemos agrupar los siguientes tipos penales:

I. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (relacionados con el Convenio de Budapest).

II. Delitos informáticos (relacionados con el Convenio de Budapest).

III. Delitos relacionados con el contenido (relacionados con el Convenio de Budapest).

IV. Delitos relacionados con la Propiedad Intelectual y afines (relacionados al Convenio de Budapest).

V. Delitos contra la indemnidad y la libertad sexual (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación)

VI. Delitos contra la Libertad (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación)

VII. Delitos contra la intimidad y violación al secreto de las comunicaciones (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación).

VIII. Delitos contra el patrimonio (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación).

IX. Delitos contra a tranquilidad pública (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación)

X. Delitos informáticos cometidos por organización criminal (relacionados a la utilización o instrumentalización de las tecnologías de la información o comunicación).

Sin embargo, debemos indicar que varios de los tipos penales referidos presentan deficiencias en su regulación, por lo cual resulta necesario ser perfeccionados en su redacción y en su marco punitivo, e incluso vacíos normativos como es el caso, por ejemplo, de la regulación de los delitos de propiedad intelectual, falsificación informática, la responsabilidad de las personas jurídicas enmarcados en la ciberdelincuencia, etc. De igual manera sucede con la adecuación de la legislación procesal penal para estos supuestos, con la finalidad de una persecución penal adecuada donde la prueba digital o electrónica es de gran importancia.

II. ESTADÍSTICAS OFICIALES

2.1 DENUNCIAS REGISTRADAS POR LA DIVISIÓN DE DELITOS DE ALTA TECNOLOGÍA

La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), en el periodo de octubre 2013 a diciembre de 2020, registró 12169 delitos vinculados a la Ley 30096. El 78% (9515) de los delitos registrados es por fraude informático, seguido por el delito de suplantación de identidad (13%) y delitos contra datos y sistemas informáticos (6%).

El delito con mayor cantidad de registros, dentro del fraude informático, corresponde a las operaciones y transferencia electrónicas y/o de fondos no autorizados, con el 86% (8142).

Asimismo, se observa que el registro de los delitos ha tenido un ritmo creciente año a año, donde los registros del 2020 representaron el 134% de crecimiento en comparación a los registros del 2017.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**0.1%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

Respecto a los requerimientos realizados por los despachos fiscales hacia la DIVINDAT; en la tabla 2 se observa que, el 70% (193) de los requerimientos se hicieron desde las fiscalías comunes y el 30% (82) desde cinco fiscalías especializadas: Fiscalías Especializadas en Criminalidad Organizada (FECCOR), Fiscalías Especializadas en delitos de Trata de Personas (FISTRAP), Fiscalías Especializadas en delitos de Tráfico Ilícito de Drogas (FETID), Fiscalías Especializadas en delitos de Corrupción de funcionarios (FECOF) y Fiscalías Especializadas en delitos de Lavado de Activos (FISLAA).

Tabla 2. Requerimientos realizados por los despachos fiscales a DIVINDAT

AÑO	FECCOR	FISTRAP	FETID	FECOF	FISLAA	FISCALÍAS COMUNES	TOTAL
2013 a 2018	4	6	5	12	12	56	95
2019	10	6	0	14	3	100	133
2020 (A julio)	5	2	1	1	1	37	47
TOTAL	**19**	**14**	**6**	**27**	**16**	**193**	**275**
%	7	5	2	10	6	70	

Tomado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020. La información corresponde al periodo de octubre de 2013 a julio de 2020

2.2. DENUNCIAS REGISTRADAS POR EL MINISTERIO PÚBLICO

El presente análisis se ha realizado a partir de la información proporcionada por la Oficina de Racionalización y Estadística del Ministerio Público respecto a las denuncias por delitos informáticos (Ley N°30096), registradas en el Sistema de Gestión Fiscal (SGF) y el Sistema Integrado de Apoyo al Trabajo Fiscal (SIATF), desde el 22 de octubre de 2013 al 31 de julio de 2020.

Como se muestra en la tabla 3; en dicho periodo ingresaron a las Fiscalías Penales Comunes Especializadas y a Fiscalías Mixtas 21,687 denuncias por delitos informáticos. El 48% (10340) de las denuncias policiales se registraron en el Distrito Fiscal de Lima y otro 35% (7668), fue registrado en siete Distritos Fiscales: Lima Norte (7%), Arequipa (6%), Lima Este (6%), La Libertad (5%) y Lambayeque (4%), Callao (3%) y Lima Sur (3%). Así, encontramos que el 83% de los delitos informáticos se concentró en ocho Distritos Fiscales.

Se observa que anualmente las denuncias muestran incrementos constantes. Es así que, en el 2014 se registraron 540 denuncias y en el 2015 éstas llegaron a 907. En el 2016 se elevaron a 1410 y un año después se duplicaron hasta alcanzar las 2,841 denuncias. En el 2018, las denuncias continuaron ascendiendo hasta llegar a 4648 y cerrar el 2019 con 8504 denuncias, representando este último año el 39% de todas las denuncias ingresadas, entre el 2014 y 2019 Los mapas 1 y 2, evidencian la magnitud de las denuncias, por distrito fiscal, en el 2019 y 2020.

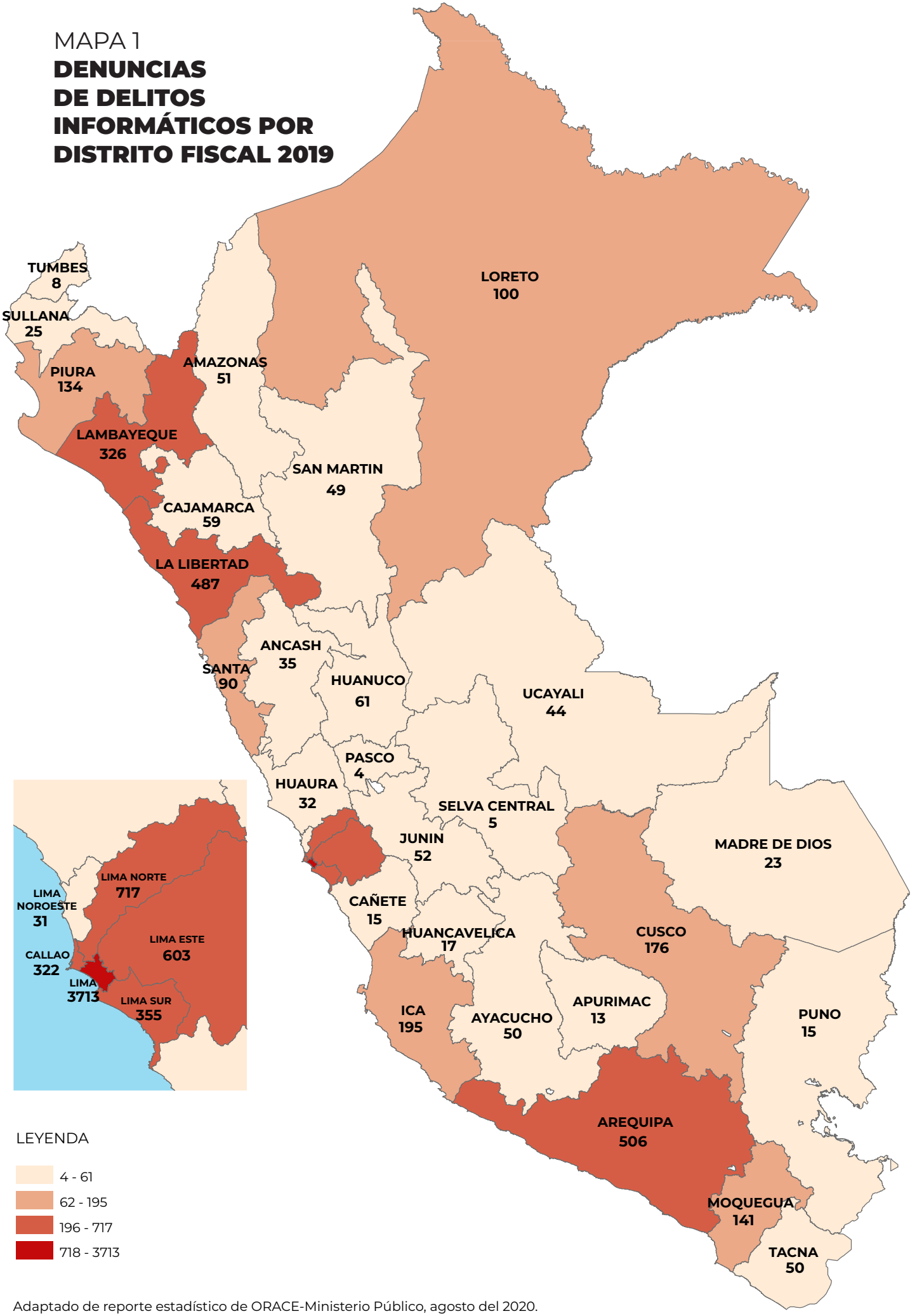
Tabla 3. Denuncias por delitos informáticos registradas en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
LIMA	67	325	550	708	1495	2366	3713	1116	10 340	47.68%
LIMA NORTE	3	24	24	99	174	357	717	220	1618	7.46%
AREQUIPA	1	18	47	155	255	291	506	115	1388	6.40%
LIMA ESTE	3	17	26	53	147	251	603	183	1283	5.92%
LA LIBERTAD	3	20	35	36	94	213	487	232	1120	5.16%
LAMBAYEQUE	1	11	31	82	119	182	326	124	876	4.04%
CALLAO	3	15	16	52	57	130	322	101	696	3.21%
LIMA SUR	1	4	9	27	52	120	355	119	687	3.17%
CUSCO	4	33	42	41	79	81	176	81	537	2.48%
ICA		3	10	22	24	91	195	57	402	1.85%
PIURA	3	10	33	15	34	68	134	40	337	1.55%
LORETO	1	7	15	24	48	93	100	32	320	1.48%
MOQUEGUA	1	2	1	5	19	46	141	47	262	1.21%
SANTA		3	3	6	36	20	90	27	185	0.85%
HUANUCO		3	2	3	30	25	61	36	160	0.74%
JUNIN		5	7	5	16	44	52	27	156	0.72%
UCAYALI		4	6	9	18	43	44	15	139	0.64%
SAN MARTIN		3	4	6	32	31	49	13	138	0.64%
AMAZONAS	2	1	2	6	30	18	51	20	130	0.60%
CAJAMARCA	1	3	2	4	5	21	59	31	126	0.58%
AYACUCHO	2	3	2	9	9	24	50	15	114	0.53%
TACNA		6		5	4	20	50	15	100	0.46%
SULLANA		3	12	9	12	15	25	15	91	0.42%
HUAURA		4	6	8	11	20	32	10	91	0.42%
ANCASH		2	4	5	12	20	35	8	86	0.40%
LIMA NOROESTE			2	6	3	15	31	15	72	0.33%
PUNO	1		3	3	12	8	15	6	48	0.22%
APURIMAC		3	1	1	2	18	13	4	42	0.19%
MADRE DE DIOS		2	3		3	1	23		32	0.15%
TUMBES		4	3	2	5	6	8	1	29	0.13%
HUANCAVELICA	1	1	2	3		4	17	1	29	0.13%
CAÑETE		1	1	1	1	1	15	3	23	0.11%
SELVA CENTRAL			3		1	1	5	8	18	0.08%
PASCO	1				2	4	4	1	12	0.06%
TOTAL	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21 687**	**100.00%**

Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

MAPA 1

DENUNCIAS DE DELITOS INFORMÁTICOS POR DISTRITO FISCAL 2019



Adaptado de reporte estadístico de ORACE-Ministerio Público, agosto del 2020.

MAPA 2

DENUNCIAS DE DELITOS INFORMÁTICOS POR DISTRITO FISCAL 2020(JUL)

LEYENDA

- 0- 57
- 58 - 124
- 125 - 232
- 233 - 1116

Adaptado de reporte estadístico de ORACE-Ministerio Público, agosto del 2020.

Característica de los delitos informáticos

Según ORACE, los delitos contra el patrimonio representan el 42% (9014) de los delitos informáticos. Con pocos registros aparecen los delitos contra la fe pública (4%), contra datos y sistemas informáticos (3%), contra la indemnidad y libertad sexuales (2%), contra la intimidad y el secreto de las comunicaciones (1%) y por disposiciones comunes (0.7%). Resalta que en el 48% (10 384) de las denuncias, no se ha especificado el tipo del delito, esta situación es particularmente relevante en el Distrito Fiscal de Lima que alcanza el 63% (6523) de los casos descritos.

Tabla 4. Delitos informáticos según tipo subgenérico

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Sin especificar			57	643	1513	2431	4415	1325	10384	48%
Contra el patrimonio	99	535	812	614	931	1657	3228	1138	9014	42%
Contra la fe pública		2	7	45	123	160	335	116	788	4%
Contra datos y sistemas informáticos		2	16	41	118	159	281	79	696	3%
Contra la indemnidad y libertad sexuales			4	35	68	137	115	25	384	2%
Contra la intimidad y el secreto de las comunicaciones			6	25	49	72	68	40	260	1%
Disposiciones comunes		1	5	7	39	32	62	15	161	0.7%
TOTAL	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21687**	**100.0%**

Adaptado de reporte de la Oficina de Racionalización y Estadística,
remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

Fiscalías Provinciales con mayor incidencia de delitos informáticos

Desde octubre de 2013 al 31 de julio de 2020, se identificaron a 542 Fiscalías en 34 Distritos Fiscales que registraron denuncias por delitos informáticos. El 21% (4493) de las denuncias se registró en once fiscalías de cuatro Distritos Fiscales: Lima, Arequipa, Lambayeque y La Libertad.

Tabla 5. Fiscalías con mayor cantidad de registros por delitos informáticos

Distrito Fiscal	FISCALIA ASIGNADA	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL
LIMA	01° FPP DE SAN ISIDRO				1	72	136	218	54	481
LIMA	02° FPP DE MIRAFLORES			1	8	106	136	161	57	469
LIMA	02° FPP DE SAN ISIDRO				1	61	135	212	55	464
LIMA	01° FPP DE MIRAFLORES				8	98	132	162	43	443
AREQUIPA	01° FPP CORPORATIVA DE AREQUIPA		6	19	49	84	92	149	33	432
AREQUIPA	03° FPP CORPORATIVA DE AREQUIPA	1	2	3	36	76	98	158	42	416
AREQUIPA	02° FPP CORPORATIVA DE AREQUIPA		3	17	60	85	72	117	29	383
LAMBAYEQUE	03° FPP CORPORATIVA DE CHICLAYO		4	11	41	65	77	120	54	372
LA LIBERTAD	01° FPP CORPORATIVA DE TRUJILLO	1	9	12	15	31	75	182	27	352
LA LIBERTAD	03° FPP CORPORATIVA DE TRUJILLO	1	1	12	4	16	41	140	133	348
LA LIBERTAD	02° FPP CORPORATIVA DE TRUJILLO	1	5	9	6	32	86	139	55	333
TOTAL		**4**	**30**	**84**	**229**	**726**	**1080**	**1758**	**582**	**4493**

Adaptado de reporte de la Oficina de Racionalización y Estadística,
remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

A la fecha, el 58% (12608) de las denuncias han sido archivadas y el 41% (8842) está en proceso de investigación y juzgamiento, 125 fueron sobreseídas y cuatro se acogieron a la terminación anticipada. De acuerdo a la información estadística registrada, en 108 casos se llegó a sentencia (la data no precisa el tipo de sentencia). Asimismo, se observa que las once Fiscalías Provinciales Penales identificadas como las que más denuncias reciben, solo seis Fiscalías tienen registradas sentencias, estas son: 03° FPP Corporativa de Chiclayo (8 sentencias), 01° FPP Corporativa de Arequipa (6 sentencias), 02° FPP Corporativa de Arequipa (6 sentencias), 01° FPP Corporativa de Trujillo (4 sentencias), 03° FPP Corporativa de Trujillo (4 sentencias) y 02° FPP Corporativa de Trujillo (2 sentencias).

Tabla 6 . Denuncias por delitos informáticos 2013-2020, según estado procesal

ESTADO	CANTIDAD	%
Archivadas	12608	58%
En proceso	8842	41%
Sobreseimiento	125	1%
Sentencia	108	0%
Terminación anticipada	4	0%
TOTAL	**21 687**	

Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

Delitos informáticos, según artículos de la Ley N°30096

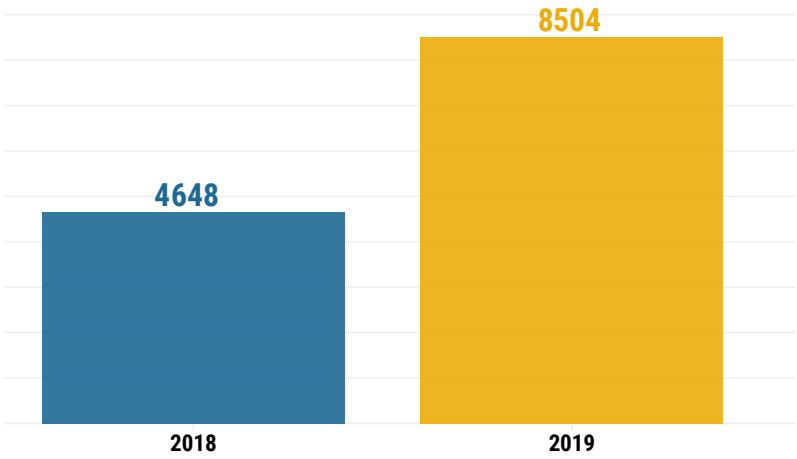
Tomando como referencia el periodo 2018 a julio 2020, se observa que el 37.8% (6001) de los delitos informáticos registran como delito específico el artículo 8 (Fraude informático) de la Ley N°30096. Con 3.8% (611), aparecen los delitos del artículo 9 (Suplantación de identidad); con 1.7% (277), los delitos del artículo 5 (Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos) y, con 1.4% (216) los delitos del artículo 2 (Acceso ilícito). Sin embargo, en el 53.4% (8490) no se ha especificado el tipo específico de delito.

Tabla 7. Denuncias de delitos informáticos, según artículos específicos de la Ley N°30096

LEY 300096	2018	2019	2020	TOTAL	%
Sin especificar	2542	4572	1376	8490	53.4%
Artículo 8. Fraude informático	1652	3215	1134	6001	37.8%
Artículo 9. Suplantación de identidad	160	335	116	611	3.8%
Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	137	115	25	277	1.7%
Artículo 2. Acceso ilícito	62	120	34	216	1.4%
Artículo 7. Interceptación de datos informáticos	28	37	24	89	0.6%
Artículo 3. Atentado a la integridad de datos informáticos	25	33	10	68	0.4%
Artículo 10. Abuso de mecanismos y dispositivos informáticos	16	39	3	58	0.4%
Artículo 11. Agravantes	9	18	10	37	0.2%
Artículo 4. Atentado a la integridad de sistemas informáticos	11	11	1	23	0.1%
Artículo 6. Tráfico ilegal de datos	6	9	5	20	0.1%
TOTAL	**4648**	**8504**	**2738**	**15890**	**100.0%**

Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

Figura 1. Evolución de denuncias de Delitos informáticos. Ley N°30096



Adaptado de reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020.

2.3. FISCALÍAS ESPECIALIZADAS CONTRA LA CRIMINALIDAD ORGANIZADA

Las Fiscalías Especializadas contra la Criminalidad Organizada, entre el 2018 y julio de 2020, registraron 23 delitos informáticos: el 65% (15) se registró en la Fiscalía Provincial Especializada contra la Criminalidad Organizada de Arequipa; el 30% (07), en la Fiscalía Supraprovincial Especializada contra la Criminalidad Organizada y el 4% (01), en la Fiscalía Provincial Especializada contra la Criminalidad Organizada de Piura.

Tabla 8. Delitos informáticos registrados en FECCOR, según tipo de fiscalía

FISCALÍA ESPECIALIZADA	CANTIDAD	%
Fiscalía Provincial Especializada contra la Criminalidad Organizada de Arequipa	15	65%
Fiscalía Provincial Especializada contra la Criminalidad Organizada de Piura	1	4%
Fiscalía Supraprovincial Especializada contra la Criminalidad Organizada	7	30%
TOTAL	**23**	**100%**

Adaptado de la información proporcionada por la Fiscalía Superior Nacional Coordinadora de Fiscalías Especializadas contra la Criminalidad Organizada. Remitido a la OFAEC, con Oficio N° 1571-2020-MP-FN-FSCN-FECCO, de fecha 02 de noviembre de 2020.

El registro no permite precisar el delito especifico recurrente; en el 57% (13) de los casos no ha sido consignado o no ha sido correctamente precisado.

Tabla 9. Delitos informáticos registrados en las Fiscalías Especializadas contra la Criminalidad Organizada

DELITO	DELITO ESPECÍFICO	TOTAL
Delito informático	Accede a BD, sistema, red, usando información privilegiada obtenida en función a su cargo.	3
	Delitos contra datos y sistemas informáticos.	1
	Delitos informáticos contra el patrimonio.	1
	Fraude informático.	2
	Ley N° 30096, Ley de delitos informáticos.	**13 (57%)**
	Comete o facilita la comisión de delitos acopia o entrega información, realiza vigilancia.	2
	Uso indebido de información privilegiada.	1
	TOTAL	**23**

Adaptado de la información proporcionada por la Fiscalía Superior Nacional Coordinadora de Fiscalías Especializadas contra la Criminalidad Organizada. Remitido a la OFAEC, con Oficio N° 1571-2020-MP-FN-FSCN-FECCO, de fecha 02 de noviembre de 2020.

2.4. OFICINA DE PERITAJES DEL MINISTERIO PÚBLICO: ÁREA DE ANÁLISIS DIGITAL FORENSE

La Oficina de Peritajes del Ministerio Público, fue creada en el 2018 como dependencia del Instituto de Medicina Legal. Al año siguiente, a través de la Resolución de la Fiscalía de la Nación N° 1974-2019-MP-FN, de julio del 2019, se convierte en órgano de apoyo de la Gerencia General.

Cuenta con cinco áreas; correspondiendo al Área de Análisis Digital Forense la atención de las siguientes pericias: a) autentificación de archivos digitales en audio, imagen y video; b) procesamiento de imágenes digitales con fines de identificación; c) recuperación y búsqueda de archivos electrónicos en dispositivos tecnológicos (equipos celulares, computadoras, USB, etc.); d) análisis de sistemas informáticos con fines de identificar manipulaciones indebidas; e) recuperación de imágenes de cámaras (circuito cerrado de televisión); f) desbloqueo de celulares Android, iOS y otros sistemas operativos; y, g) recuperación de mensajes de textos, WhatsApp y otros.

Durante el 2019 y julio del 2020, el Área de Análisis Digital Forense recibió 534 solicitudes de pericias, el 21% (110) fue en el 2019 y el 79% (424) en el 2020. De esta cantidad, el 27% (120) de solicitudes se generaron en los Distritos Fiscales de Lima y Callao. Otro 22% de solicitudes (118) en los Distritos Fiscales de Huánuco (5%), Ancash (5%), Lima Norte (4%), Santa (4%) y Arequipa (4%). El 37% (200) restante provino de 26 Distritos Fiscales. El 18% (96) de los casos, correspondió a otros Distritos Fiscales.

Asimismo, se observa que los Distritos Fiscales de Huánuco, Santa y Ancash, con baja cantidad de denuncias por delitos informáticos en el 2019 y 2020, han solicitado mayor cantidad de peritajes en comparación a los Distritos Fiscales de Arequipa, Lima Este y La Libertad, que han registrado mayores denuncias.

Tabla 10. Solicitudes de peritajes recibidas por el Área de Análisis Digital Forense

Distrito Fiscal	2019	2020	TOTAL	%
OTROS	11	85	96	18%
LIMA	13	66	79	15%
CALLAO	12	29	41	8%
HUÁNUCO	10	17	27	5%
ANCASH	6	21	27	5%
LIMA NORTE	7	17	24	4%
SANTA	7	14	21	4%
AREQUIPA	3	16	19	4%
PUNO	2	15	17	3%
LIMA NOROESTE	2	13	15	3%
SAN MARTÍN	1	14	15	3%
LIMA SUR	0	14	14	3%
LAMBAYEQUE	2	11	13	2%
LIMA ESTE	1	11	12	2%
CUSCO	7	4	11	2%
ICA	2	9	11	2%
APURÍMAC	2	8	10	2%
LA LIBERTAD	5	5	10	2%
CAJAMARCA	0	8	8	1%
UCAYALI	2	6	8	1%
HUAURA	1	6	7	1%
AMAZONAS	2	4	6	1%
PASCO	5	1	6	1%
TACNA	0	6	6	1%
CAÑETE	2	3	5	1%
JUNIN	0	5	5	1%
LORETO	2	3	5	1%
HUANCAVELICA	1	3	4	1%
AYACUCHO	2	1	3	1%
PIURA	0	3	3	1%
MADRE DE DIOS	0	2	2	0.4%
TUMBES	0	2	2	0.4%
MOQUEGUA	0	1	1	0.2%
SULLANA	0	1	1	0.2%
TOTAL	**110**	**424**	**534**	**100%**

Adaptado de la información proporcionada por la Oficina Peritajes, remitido a la OFAEC a través del Oficio 7898-2020-MP-FN-GG-OPERIT, de fecha 06 de noviembre de 2020.

Considerando a la entidad solicitante; mostradas en la tabla 11; el 43% (229) de las solicitudes fueron generadas por Fiscalías Provinciales Penales y el 42% (224) por Fiscalías Especializadas. En menor porcentaje, las solicitudes fueron realizadas por la PNP (8%), Fiscalías Supremas

(4%), Poder Judicial (0.9%), Fiscalías Superiores (0.7%), Control Interno (0.2%) y UCJIE (0.2%). Respecto a las 224 solicitudes presentadas por las Fiscalías Especializadas; el 69% correspondió a la Fiscalías Especializadas en delitos de Corrupción de Funcionarios (FECOF) y, el 19% a la Fiscalías Especializadas contra el Crimen Organizado (FECCOR).

Tabla 11. Peritajes Digitales Forenses solicitados a la Oficina de Peritajes del Ministerio Público, según entidad solicitante

INSTITUCIÓN	ENTIDAD SOLICITANTE	CANTIDAD	%
MINISTERIO PÚBLICO	FISCALÍAS PROVINCIALES PENALES	229	42.9
	FECOF	155	29
	FECCOR	43	8.1
	FISCALIAS SUPREMAS	23	4.3
	FEDAPI	6	1.1
	FETID	5	0.9
	FEMA	4	0.7
	FISCALÍAS SUPERIORES	4	0.7
	FISTRAP	4	0.7
	VIOLENCIA CONTRA LA MUJER	4	0.7
	FISLAAPD	3	0.6
	CONTROL INTERNO	1	0.2
	UCJIE - MP	1	0.2
PNP	DIRINCRI	44	8.2
PODER JUDICIAL	PODER JUDICIAL	5	0.9
	NO IDENTIFICADO	3	0.6
	TOTAL	**534**	**100**

Adaptado de la información proporcionada por la Oficina de Peritajes, remitido a la OFAEC a través del Oficio 7898-2020-MP-FN-GG-OPERIT, de fecha 06 de noviembre de 2020.

2.5. UNIDAD DE COOPERACIÓN JUDICIAL INTERNACIONAL Y EXTRADICIONES

La Unidad de Cooperación Judicial Internacional y Extradiciones se crea mediante la Resolución de Fiscalía de la Nación N° 124-2006-MP-FN, del 3 de febrero de 2006, con el objetivo de centralizar la coordinación y ejecución de todas las acciones reguladas por el Libro Séptimo del Nuevo Código Procesal Penal.

Esta Unidad, durante el periodo de enero 2017 a octubre de 2020, ha registrado 99 asistencias judiciales activas y 28 asistencias judiciales pasivas, relacionadas a delitos informáticos y delitos en los que se utilizó la tecnología como medio determinante para su ejecución.

Se observa que los requerimientos realizados a las entidades extranjeras (asistencias judiciales activas), ha tenido un crecimiento constante; es así que de los 16 requerimientos que se realizaron en el 2017, ascendió a 30 en el 2018 y llego a 47 requerimientos en el 2019. Por otra parte, los requerimientos realizados por entidades extranjeras también alcanzaron un pico en el 2019, con 12 requerimientos. Sin embargo; en el 2020 los requerimientos se reducen considerablemente, probablemente condicionado por la declaración del estado de emergencia y el establecimiento de la emergencia sanitaria.

Tabla 12. Asistencias Judiciales Activas y Pasivas. 2017-2020(octubre)

AÑO	Asistencias Judiciales Activas	Asistencias Judiciales Pasivas
2017	16	5
2018	30	5
2019	47	12
2020	6	6
TOTAL	**99**	**28**

Adaptado de la información proporcionada por la UCJIE, remitido a la OFAEC a través de correo electrónico de fecha 17 de noviembre de 2020.

El 45% de la asistencia judicial activa se ha orientado a la solicitud de información de cuentas de Facebook y, el 18% a las solicitudes de información de cuentas de correos electrónicos. Asimismo, se observa que en asistencias judiciales donde se ha solicitado más de un acto de cooperación, en el 9% de los casos ha implicado a las redes sociales. Por lo que se constata que el 54% de la asistencia judicial activa está relacionada a las redes sociales como Facebook, Messenger, Google, WhatsApp, etc.

Desde el 01 de diciembre de 2019, los pedidos se tramitan en el marco del Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, por ser el instrumento multilateral específico en dicha materia. Sin embargo, algunos fiscales continúan invocando en sus pedidos de asistencia judicial activos, la Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Tabla 13. Solicitudes de Asistencia Judicial Activa. 2017-2020(octubre)

REQUERIMIENTOS	NÚMERO
Información de cuenta Facebook	45
Información de cuenta de correo electrónico	18
Solicita información a Facebook, Messenger, WhatsApp	3
Solicita información a Google	2
Solicita información de una página web	2
Identidad de usuario detenido, información de intervención en la cuenta de red social rusa	**1**
Solicita información a diversas empresas proveedoras de redes sociales	**1**
Solicita a empresa Cloudflarenet INC. Informe quien es titular de una cuenta.	**1**
Solicita información a Google y Microsoft	**1**
Solicita información sobre un blog	**1**
Solicita levantamiento de las comunicaciones e información de tráfico y contenido de una cuenta Facebook	**1**
Ubicación desde donde se remitieron mensajes vía correo electrónico	1
TOTAL	**99**

Adaptado de la información proporcionada por la UCJIE, remitido a la OFAEC a través de correo electrónico de fecha 17 de noviembre de 2020.

Como se observa en la tabla 14, de las 99 asistencias judiciales activas, en 31 casos los delitos están relacionados a la Ley N°30096, Ley de Delitos Informáticos. En otros 68 casos, se utilizó la tecnología como medio determinante para su ejecución.

Tabla 14. Asistencia Judicial Activa por delitos informáticos. 2017-2020(octubre)

N°	DELITOS	CANT.
1	Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	8
2	Delitos informáticos y otros	1
3	Fraude Informático	7
4	Suplantación de identidad	6
5	Actos contra el Pudor/Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	2
6	Exhibición y publicaciones obscenas/proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	1
7	Fraude Informático, abuso de mecanismos y mecanismos informáticos	1
8	Fraude Informático/Suplantación de identidad	1
9	Interceptación de datos informáticos/Fraude Procesal/ Falsedad Genérica	2
10	Atentado contra la integridad de datos y sistemas informáticos	1
11	Clonación o alteración de Terminales de Comunicaciones	1

Adaptado de la información proporcionada por la UCJIE, remitido a la OFAEC a través de correo electrónico de fecha 17 de noviembre de 2020.

2.6 ESCUELA DEL MINISTERIO PÚBLICO

Entre el 2018 y 2020, la Escuela del Ministerio Público registró 05 actividades académicas, en temas relacionados a ciberdelincuencia y delitos informáticos: tres actividades fueron virtuales y dos presenciales (ambas en la ciudad de Lima). En dos casos el coorganizador fue la Escuela del Ministerio Público, en otros dos casos la ONG American Bar Association Rule of Law Initiative (ABA ROLI PERÚ) y en un caso la Unión Europea.

Tabla 15. Actividades académicas desarrolladas por el Ministerio Público. 2018–2020

AÑO	ACTIVIDAD ACADÉMICA	MODALIDAD	DURACIÓN	CO-ORGANIZADOR
2018	Taller: Delitos informáticos	Presencial (Lima)	10 horas académicas	Escuela MP
2018	Curso: Delitos Informáticos	Virtual	120 horas académicas	Escuela MP
2020	Taller de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos - Cybercrimen	Presencial (Lima)	50 horas académicas	American Bar Association Rule of Law Initiative ABA ROLI PERÚ
2020	Curso de Investigación Criminal y Litigación Oral Especializado en Delitos Informáticos - Cybercrime	Virtual	Del 30.03 al 27.05 de 2020	American Bar Association Rule of Law Initiative ABA ROLI PERÚ
2020	Ciberdelincuencia, Delitos Tecnológicos	Virtual	36 horas académicas	Unión Europea

Adaptado de la lista de actividades académicas, remitido por la Escuela del Ministerio Público al Gabinete de Asesores, a través de correo electrónico institucional de fecha 02 de diciembre de 2020.

Según este registro, los cursos presenciales beneficiaron a 86 (18%) personas y los cursos virtuales a 389 (82%) personas: 214 fiscales, 93 asistentes en función fiscal, 5 especialistas del Instituto de Medicina Legal, 151 administrativos y 8 peritos. No se cuenta con información de los beneficiarios del curso virtual coorganizado por la Unión Europea, en el 2020.

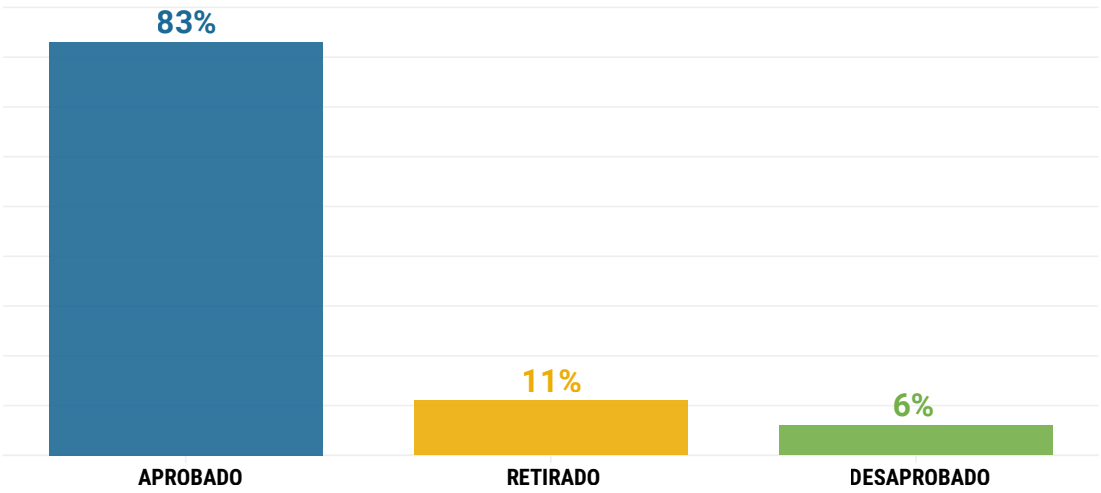
Tabla 16. Actividades académicas, según modalidad y características de los participantes. 2018-2020

AÑO	MODALIDAD	PARTICIPANTES					VACÍOS	TOTAL
		FISCAL	ASIST. EN FUNCIÓN FISCAL	FORENSES	ADM.	PERITOS		
2018	Presencial (Lima)	17	7		34	5		63
2018	Virtual	95	84	5	116		2	302
2020	Presencial (Lima)	19			1	3		23
2020	Virtual	83	2				2	87
2020	Virtual	-		-	-			
		214	**93**	**5**	**151**	**8**	**4**	**475**

Adaptado de la lista de actividades académicas, remitido por la Escuela del Ministerio Público al Gabinete de Asesores, a través de correo electrónico institucional de fecha 02 de diciembre de 2020.

Respecto al desempeño académico de los participantes o a los resultados de los participantes en los cursos de capacitación, se observa que el 83% (392) de los participantes aprobó los cursos. El 11% (54) se retiró y el 6% (29) desaprobó. En ningún caso, se encontró registro de participantes inscritos en más de un curso.

Figura 2. Actividades académicas, según resultados de su participación



Adaptado de la lista de actividades académicas, remitido por la Escuela del Ministerio Público al Gabinete de Asesores, a través de correo electrónico institucional de fecha 02 de diciembre de 2020.

III. ENTREVISTAS A ACTORES DEL SISTEMA

3.1. REPRESENTANTES DE FISCALÍAS CON MAYOR INCIDENCIA DE DELITOS INFORMÁTICOS

Con el objetivo de conocer la experiencia, percepción y opinión de los fiscales en la investigación de los delitos informáticos, se diseñó un cuestionario de 21 preguntas, el mismo que fue aplicado por vía correo electrónico y la plataforma Google Forms a 8 Fiscales de las Fiscalías Provinciales Penales de mayor incidencia de denuncias por delitos informáticos en el periodo de octubre 2013 a julio 2020.

Tabla 17. Perfil de fiscales a quienes se dirigió el cuestionario

N°	DISTRITO FISCAL	NOMBRE	FISCALÍA	EXPERIENCIA	CASOS	SENTENCIAS CONDEN.	CAPACITACIÓN
1	LIMA	Fiscal 1	01 FPP de San Isidro	03 años	+20	No	Si
2	LIMA	Fiscal 2	02 FPP de Miraflores	04 años	+20	No	Si
3	LIMA	Fiscal 3	02 FPP de San Isidro	04 años	+20	01	Si
4	LIMA	Fiscal 4	01 FPP de Miraflores	03 años	+20	No	Si
5	LAMBAYEQUE	Fiscal 5	03 FPP Corporativa de Chiclayo	07 años	10	01	No
6	AREQUIPA	Fical 6	01 FPP Corporativa de Arequipa	08 años	10	02	No
7	AREQUIPA	Fiscal 7	03 FPP Corporativa de Arequipa	16 años	12	No	No
8	LA LIBERTAD	Fiscal 8	03 FPP Corporativa de Trujillo	01 años	04	No	No

La mayoría de fiscales entrevistados tienen más de 3 años de experiencia en la investigación de este tipo de delitos, siendo la fiscal entrevistada de la Tercera Fiscalía Provincial Corporativa de Arequipa, quien refiere la mayor experiencia, con 16 años investigando, entre otros casos, delitos informáticos.

Durante dichos años de experiencia, los fiscales del Distrito Fiscal de Lima (Fiscalías Provinciales Penales de San Isidro y Miraflores), afirman haber investigado más de 20 casos relacionados a delitos informáticos. Siguen, los fiscales de los Distritos Fiscales de Arequipa y Lambayeque, refiriendo haber investigado 10 y 12 casos.

Tres fiscales de los Distritos Fiscales de Lima, Lambayeque y Arequipa, afirman que han logrado que sus investigaciones culminen en sentencias condenatorias. Asimismo, los cuatro fiscales de los distritos fiscales mencionados, aseveran no haber recibido capacitación en materia de ciberdelincuencia.

Todos los entrevistados coinciden en sostener que el fraude informático es el delito específico con mayor cantidad de denuncias. Esta opinión es consistente con los registros facilitados por ORACE, en donde se aprecia que los delitos contra el patrimonio representan el 42% de los delitos informáticos. Les siguen la suplantación de identidad y las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. También son mencionados, otros tipos penales relacionados con nuevas formas de delincuencia sexual a través de medios informáticos: pornografía infantil, difusión de imágenes, materiales audiovisuales o audios con contenido sexual, chantaje sexual, acoso sexual. Finalmente, en menor proporción en Lima se da cuenta de frecuencia de atentados contra la integridad de datos informáticos, y en Arequipa de clonación o adulteración de terminales de telecomunicaciones.

Tabla 18. Delitos Informáticos frecuentes referidos por fiscales entrevistados

Distrito Fiscal	DELITOS FRECUENTES
LIMA	• Fraude informático
	• Fraude informático, Suplantación de identidad • Difusión de imágenes, materiales audiovisuales o audios con contenido sexual
	• Fraude informático (85%), Suplantación de identidad (3%) • Atentado contra la integridad de datos informáticos (5.5%)
	• Fraude informático (30%), Suplantación de identidad (10%) • Chantaje sexual (1%), Pornografía infantil (1%)
LAMBAYEQUE	• Fraude informático
AREQUIPA	• Fraude informático. • Clonación o adulteración de terminales de telecomunicaciones • Pornografía infantil, Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. • Fraude informático (75%) • Acoso sexual (19%) Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. (7%)
LA LIBERTAD	• Fraude informático (60%), Suplantación de identidad (30%) • Proposiciones a niños, niñas y adolescentes con fines sexuales (10%)

Los fiscales han tenido dificultades para la investigación del delito en la etapa preliminar. Los fiscales de Chiclayo y Arequipa mencionan que la mayor dificultad se encuentra en la obtención de información de algún elemento electrónico, dirección de IP o apertura de teléfonos bloqueados con clave. Para la fiscal de Chiclayo, el no contar con la Unidad de Alta Tecnología de la Policía Nacional ni con peritos informáticos del Ministerio Público, genera demoras en la investigación ya que tiene que remitir las pruebas a la ciudad de Lima.

Tabla 19. Dificultades de investigación y enjuiciamiento de la ciberdelincuencia

DILIGENCIAS PRELIMINARES	
Dificultades propias de la materia	Poca información y dificultades para identificar al autor (2 veces)
	Los Jueces en base al art.230 del NCPP (pena mínima, no identificación autor) niegan el levantamiento de secreto de las comunicaciones.
	Necesidad de equipos de alta tecnología para identificar a los autores.
Insuficientes o deficientes órganos de apoyo	Falta de capacitación de los policías en uso técnicas de investigación especiales.
	Falta de peritos en la materia. Necesidad de pericias sobre dispositivos telefónicos electrónico y/o equipos de informática, o para determinar dirección IP, apertura de teléfonos bloqueados. (3 veces).
El denunciante no colabora en esclarecer los hechos	
FORMALIZACIÓN Y CONTINUACIÓN DE LA INVESTIGACIÓN PREPARATORIA	
Insuficientes o deficientes órganos de apoyo	Falta de capacidades tecnológicas de la PNP.
	Falta de peritos y de capacidad de la PNP de técnicas especiales.
Cooperación con otras Fiscalías	Investigar a imputados que se encuentran fuera del Distrito Fiscal.
JUICIO ORAL	
Insuficientes o deficientes órganos de apoyo	Asistencia de los peritos al juicio oral (2 veces). No contar con peritos informáticos.
	Ubicación de los órganos de prueba, agraviado y efectivos policiales para participación en el proceso.

Las dificultades en primer lugar se relacionan con lo complicado que es lograr identificar a los autores de estos delitos.

En particular, para los fiscales del Distrito Fiscal de Lima, al amparo del Código de Procedimientos Penales de 1940, los problemas se concentran en la etapa denominada preliminar, donde son más importantes sus actuaciones.

Otros fiscales refieren la dificultad de los cortos plazos de investigación y la de investigar a imputados que se encuentran fuera del Distrito Fiscal. Además, precisan que no participan en juicio oral al no contarse con juzgados homólogos. Varios otros refieren la dificultad en etapa preliminar y preparatoria de contar con investigación especializada de la PNP y de peritos informáticos, así como posteriormente, en juicio oral, la necesidad de garantizar la presencia del perito. Es entonces, una problemática del enjuiciamiento de estos delitos ubicar a los órganos de prueba: agraviados, testigos y efectivos policiales intervinientes.

Tabla 20. Formas de afectación de las víctimas de delitos informáticos

FORMAS DE AFECTACIÓN A LAS VÍCTIMAS
De manera económica/ de forma patrimonial.
Existe afectación psicológica y moral en el tema de acoso sexual y suplantación de identidad informática.
Afectación a la intimidad, a la libertad personal. Necesidad de establecer otros medios de protección; las víctimas por el uso de sus teléfonos o cuentas de redes sociales pierden el uso de estas, y tienen que crear otros perfiles.
Frustración, sentimiento de injusticia al no identificarse a los autores.
A la libertad e indemnidad sexual

La afectación de la víctima depende de la modalidad del delito informático; es así que la afectación puede ser económica o patrimonial, pero también puede ser moral o psicológica. En este último caso, la afectación también podría estar generada por la pérdida de sus cuentas en redes sociales y por la frustración al no poder identificar a los autores de los delitos.

Tabla 21. Motivo de archivamiento o sobreseimiento

MOTIVO DEL ARCHIVAMIENTO Y SOBRESEIMIENTO	FRECUENCIA
No se logra identificar a los autores de los hechos	3
Competencias: 1. Falta capacitación 2. Investigación deficiente, desconocimiento de la obtención y tratamiento de la prueba digital 3. Falta de capacidad de investigación de la fiscalía y la policía	3
Falta de cooperación de la víctima	2
Por falta de información	1
Falta de pericias, porque se desvanece la posibilidad de vincular a alguna persona con los hechos investigados	1

Tres fiscales consideran que la imposibilidad de identificar a los autores de los hechos, es el principal motivo de archivamientos y sobreseimientos de los procesos relacionados a los delitos informáticos. A decir de un fiscal; “uno de los requisitos para formalizar denuncia o investigación preparatoria contra un imputado o investigado es haberlo identificado con sus patronímicos completos”. Con la misma frecuencia, y también relacionada con las dificultades de desarrollar conocimientos sobre técnicas y actuaciones que lleven a la identificación de los responsables, es mencionada la falta de competencias profesionales, expresado en falta de capacitación, desconocimiento y falta de capacidad para la investigación. Con dos menciones se ubica la falta de cooperación de la víctima, La carencia de pericias y la limitada información es mencionada una sola vez.

Tabla 22. Requerimientos a DIVINDAT, Criminalística de la PNP y Oficina de Peritajes, para investigaciones de delitos informáticos

DIVINDAT	OFICINA DE PERITAJES MP	CRIMINALÍSTICA PNP	NINGUNO	NO ESPECIFICA	TIPO DE SOLICITUD	FRECUENCIA
✓					Identificación del IP	3
✓	✓	✓			Visualización de mensajes de redes sociales y correos electrónicos	3
✓					Recuperar archivos eliminados o borrados	2
✓					Descubrir archivos ocultos	1
				✓	Apertura de discos duros	1
✓					Peritajes sobre equipos celulares u otros equipos tecnológicos (tablets, laptop, pc):	1
			✓		Pericia Informática Forense	1
				✓	-	

Respecto a los requerimientos fiscales a la DIVINDAT, Dirección de Criminalística de la PNP y Oficina de Peritajes del Ministerio Público, para el desarrollo de las investigaciones de los delitos informáticos; cinco fiscales mencionaron que acuden a la DIVINDAT y dos fiscales, afirman que realizan requerimientos pero no especifican a cuál de las entidades.

Por otra parte, un fiscal suele realizar requerimientos a las tres entidades; y, otro fiscal respondió que no realiza requerimientos a ninguna de ellas, argumentando que éstas no cuentan con equipos que les permitan realizar peritajes.

Los peritajes solicitados con mayor frecuencia, fueron: identificación de la dirección IP (internet Protocol) de dispositivos informáticos y la visualización de los mensajes de redes sociales y correos electrónicos. Seguido, por las solicitudes de recuperación de archivos eliminados o borrados y, solicitudes de peritaje sobre equipos celulares u otros equipos tecnológicos.

Con tres menciones, la identificación de la dirección IP (internet Protocol) de dispositivos informáticos es el tipo de peritaje mayormente solicitado por los fiscales. Con la misma cantidad, se ubica la visualización de los mensajes de redes sociales y correos electrónicos. La recuperación de archivos eliminados o borrados es mencionada por dos fiscales. Con una sola mención aparecen solicitudes algo generales como: peritajes sobre equipos celulares u otros equipos tecnológicos y pericia informática forense.

Tabla 23. Requerimiento a proveedores de servicios extranjeros

REQUERIMIENTOS A PROVEEDORES DE SERVICIO EXTRANJERO	FRECUENCIA
No	7
Sí, a Facebook y compañías telefónicas	1

De los entrevistados, solo un fiscal de la Fiscalía Provincial Penal de Miraflores, fue el único en haber realizado requerimientos a proveedores de servicios extranjeros (Facebook y compañías telefónicas). El resto de los fiscales no ha realizado ningún requerimiento.

Tabla 24. Capacitaciones que se requieren para la investigación de los delitos informáticos

REQUERIMIENTO DE CAPACITACIONES
Seguridad informática con relación a la gestión de casos a nivel fiscal y judicial
Técnicas de análisis, softwares y tecnologías aplicadas a la investigación de delitos informáticos.
Diligencias de investigación en materia de delitos informáticos (identificación de IP y otros).
Curso especializado en delitos informáticos: abordaje sobre cada uno de los tipos penales: análisis de tipicidad objetiva, subjetiva, diferenciación con otros tipos penales previstos en el código penal.
Lineamientos para la solicitud directa y/o requerimientos a proveedores de servicios informáticos extranjeros, proveedores de redes sociales, etc.
Lineamientos para la solicitud y requerimientos ante la Unidad de Cooperación Judicial Internacional y Extradiciones del Ministerio Público.
Lineamientos para solicitud de información de cuentas de correos electrónicos: identidad real del titular, verificación de autenticidad de la información obtenida, vínculos con otras redes sociales (WhatsApp, Facebook, Instagram Twitter y otros).
Nuevas tecnologías, herramientas informáticas para la investigación de delitos informáticos (celulares, internet), manejo de evidencia digital y tratamiento de la prueba electrónica.

Los fiscales entrevistados sugieren ser capacitados en lineamientos para requerimientos a proveedores de servicios informáticos extranjeros, a proveedores de redes sociales y correos electrónicos y, en requerimientos ante la Unidad de Cooperación Judicial Internacional y Extradiciones del Ministerio Público.

Tres de los fiscales entrevistados sugieren cursos que permitan conocer las diligencias a seguir en casos de investigaciones por delitos informáticos (identificación de IP y otros), manejo de evidencia digital en la investigación y tratamiento de la prueba electrónica. Asimismo, dos fiscales sugieren capacitaciones sobre Técnicas de análisis, softwares y tecnologías aplicadas a la investigación de delitos informáticos.

Tabla 25. Coordinador con conocimientos en delitos informáticos-ciberdelitos que les brinde asesoría en estos casos

PERTINENCIA DE UN COORDINADOR EN DELITOS INFORMÁTICOS	
Sí	8

Ante la pregunta si debería existir un coordinador con altos conocimientos en delitos informáticos o ciberdelitos que brinde asesoría en estos casos; la respuesta afirmativa de los fiscales es unánime. El sustento puede encontrarse en la respuesta de dos fiscales: "es un delito complejo" y "podría orientar y dirigir mejor una investigación penal".

Tabla 26. Recomendaciones para mejorar la persecución del delito

RECOMENDACIONES
La existencia de una fiscalía especializada.
En cuanto al MP, gente especializada técnica como jurídicamente en la materia: peritos en el MP y la PNP que tengan estudios o capacitaciones en estos delitos para que coadyuven a la investigación fiscal. (En la pregunta 20 sugiere la creación de fiscalías especializadas).
Capacitación más constante y dinámica (no solo charlas sino también talleres) tanto al personal fiscal como administrativo, con disertaciones impartidas por personas especializadas en la materia, básicamente respecto a las diligencias a seguir en cada tipo penal relacionado con la Ley 30096 y convenciones internacionales que permitan obtener resultados positivos.
Sugiere establecer mecanismos de cooperación directa con entidades financieras y de telecomunicación, básicamente, a fin de conseguir datos relevantes de forma directa (identificación de las partes intervinientes) sin poner en peligro el secreto bancario, bursátil y tributario y tampoco los detalles de las comunicaciones.)
Creación de fiscalías especializadas en delitos informáticos.
Capacitación de personal en dicha materia.
Creación de una unidad de peritaje informático a cargo del Ministerio Público de Lambayeque.
Establecer mesas de trabajo, con representantes del MP, PNP, peritos, a fin de establecer unidades de criterio para la investigación de estos delitos.
Creación de fiscalías especializadas en ciberdelitos, para que exista una mejor forma de combatir del ciberdelito.
Establecer a nivel de fiscalías y PNP una red de coordinación a nivel nacional, para procurar intervenciones rápidas y lograr capturas en flagrante delito.
Talleres de capacitación para mejorar las prácticas de investigación del ciberdelito, en cada modalidad.
Protocolos de investigación para cada modalidad delictual)
Capacitación en el despacho fiscal y policía.
Pero el principal problema es que los peritajes se llevan a cabo solo en la capital de la República y en pocos casos han se han traído estos equipos a la ciudad para casos emblemáticos.
Implementar un laboratorio con tecnología moderna.

Finalmente, recogiendo las recomendaciones de los fiscales a quienes se aplicó el cuestionario, encontramos que el 50% (4) de estos sugieren la creación de Fiscalías Especializadas. En ese mismo porcentaje, los fiscales solicitan capacitación. En ese sentido, es relevante (por el interés mostrado y las respuestas dadas) lo expresado por fiscales que solicitan capacitación constante y dinámica (no solo charlas sino también talleres) dirigido por especialistas en la materia.

Para dos fiscales, la capacitación en diligencias por cada tipo penal o modalidad de la Ley N°30096 y convenciones internacionales, son importantes. Dos fiscales, también sugieren establecer redes de coordinación local y nacional; las primeras, con el objetivo de establecer

unidades de criterio para la investigación de estos delitos, mientras que las redes de coordinación nacional, permiten intervenciones rápidas y lograr capturas en flagrante delito.

Adicionalmente, sugieren:

1. El establecimiento de mecanismos de cooperación con entidades financieras y de telecomunicación, para obtener información relevante sin poner en peligro el secreto bancario, bursátil y tributario y tampoco los detalles de las comunicaciones.

2. La creación de una unidad de peritaje informático a cargo del Ministerio Público de Lambayeque.

3. La Implementación de un laboratorio con tecnología moderna.

4. El contar con especialistas en el Ministerio Público y la Policía Nacional del Perú para que colaboren a la investigación fiscal.

3.2. PERITOS DEL ÁREA DIGITAL FORENSE DE LA OFICINA DE PERITAJES DEL MINISTERIO PÚBLICO

Para contar con información de la labor que cumplen los peritos del Ministerio Público y su opinión respecto al análisis que desarrollan, se decidió remitir un cuestionario con 23 preguntas a tres peritos, de los siete con que cuenta el Área de Análisis Digital Forense de la Oficina de Peritajes. Posteriormente, la información proporcionada fue ampliada a través de conversaciones telefónicas.

Tabla 27. Perfil y experiencia de peritos a quienes se dirigió el cuestionario

PERITO	AÑOS DE EXPERIENCIA	CAPACITACIONES	PERICIAS INFORMÁTICAS 2019-2020	PERICIAS EN CIBERDELINCUENCIA POR MES
Perito 1	05	180 horas	110	3
Perito 2	05	360 horas	90	0
Perito 3	05	60 horas	50	5

De sus respuestas observamos que los tres peritos tienen cinco años de experiencia en ese tipo de labores y que han recibido capacitaciones variadas que van de 60 a 360 horas. En el periodo de 2019 y 2020, han realizado entre 50 y 110 pericias.

Las pericias vinculadas a los ciber delitos han sido realizadas por dos peritos, en un promedio de 3 a 5 pericias por mes. Uno de los peritos, no realiza pericias en ciberdelincuencia.

Los lineamientos y procedimientos de las actividades periciales, están establecidas en la Guía de Análisis Digital Forense, aprobada con Resolución de la Gerencia General 365-2020-MP-FN-GG del 11 de agosto de 2020.

Tabla 28. Dificultades en pericias informáticas

PERITO	DIFICULTADES
Perito 1	Desconocimiento de la parte fiscal al formular el objeto de estudio. Alta demanda
Perito 2	Celulares dañados físicos. Compatibilidad del software con los equipos celulares en celulares modernos por eso es necesario tener varios softwares forenses para lograr vulneras los bloqueos y extracción de información de los equipos celulares
Perito 3	Falta de objeto de estudio

Dos de los peritos señalan como dificultad el desconocimiento de los fiscales para formular el requerimiento de estudio. Otro de los peritos, observa como dificultad los celulares dañados que son entregados para el análisis, así como la carencia de softwares forenses que permita desbloquear y extraer información de teléfonos móviles. La alta demanda de los requerimientos es, también, una dificultad para uno de los peritos.

La falta de logística, se traduce principalmente en la limitada cantidad de equipos informáticos y en la carencia de "llaves" para los distintos softwares que utilizan, esto último ocasiona largas y tediosas esperas hasta que la "llave" se desocupe y pueda ser utilizada por otro perito. Como ejemplo; se menciona que cuentan con cinco "llaves" de software forense para que sea utilizado por 26 personas (entre peritos, analistas y personal de apoyo). El perito 3, está convencido que solucionando la carencia de "llaves", el 80% de la carga de peritos se reduciría.

Tabla 29. Tipo de peritaje

PERITO	TIPO DE PERITAJE
Perito 1	En dispositivos móviles como celulares, se realiza la extracción y búsqueda de información de acuerdo a lo solicitado por el fiscal
Perito 2	Desbloqueo y extracción de información de equipos celulares, mejoramiento de videos para identificación de placa de vehículos, extracción de información de computadoras, USB, laptop, escaneo de escena con software FARO para escena de crimen.
Perito 3	Celulares, equipos de computo

Los tres peritos han desarrollado trabajos de desbloqueo, búsqueda y extracción de información de celulares. Dos peritos han realizado la extracción de información de computadoras. Y uno de los peritos, además de lo anterior, se ha dedicado a la extracción de información de USB, el mejoramiento de videos para identificación de placa de vehículos y el escaneo de escena con software FARO para escena de crimen, que crea un modelo en tercera dimensión a escala real.

Tabla 30. Capacitación requerida para peritos en investigaciones de delitos informáticos-ciberdelitos

PERITO	CAPACITACIÓN REQUERIDA
Perito 1	La parte legal para tener conocimiento hasta donde está permitido realizar una investigación en dispositivo tecnológico sin vulnerar los derechos del investigado
Perito 2	Es necesario adquirir más herramientas en la actualidad solo se cuenta con una sola llave de XRY y UFED4PC para la extracción de celulares cuando la herramienta está en uso los demás tienen que esperar a que alguna de las llaves este libre para poder realizar trabajos, lo mismo en computo forense lo que implica capacitación y actualización para la extracción en los nuevos modelos, la tecnología avanza y los parámetros a desbloquear también hay que actualizarse.
Perito 3	Ciberseguridad

Los requerimientos de capacitación se centran en tres pedidos concretos: capacitación en cómputo forense[3] para la extracción de información en nuevos modelos de celulares; capacitación en temas legales relacionados a la investigación en dispositivo tecnológico sin vulnerar los derechos del investigado y, capacitación en ciberseguridad.

3. "La computación forense es un macro procedimiento que permite identificar, preservar, analizar y presentar evidencias digitales de forma que puedan aceptarse legalmente" (Torrealba y Devenish, 2017,p.84)

Tabla 31. Qué ha observado de los requerimientos fiscales que merezca ser mejorado

PERITO	OBSERVACIONES A LOS REQUERIMIENTOS FISCALES
Perito 1	Procedimiento en Informática Forense para que sepan que podemos recuperar y que no se puede realizar en una pericia informática
Perito 2	Ser más claro con el objeto de la pericia, incluir un número de teléfono para coordinar hay que entender el caso para tener claro qué tipo de información se está buscando e incidir en recopilar información valiosa para el caso del fiscal
Perito 3	Falta de objeto de estudio, falta de visualización previa, desconocimiento del caso

Dos de los tres peritos mencionan que los fiscales no son claros con el objeto del estudio solicitado. A decir, del perito 2, muchas veces los fiscales colocan como requerimiento la "entrega de toda información de interés", lo cual no permite centrar su análisis ya que lo que puede ser de interés para el perito quizá no lo sea para el fiscal. Por tal razón, sugiere que es necesario que los fiscales incluyan un número telefónico de referencia en el oficio, para que facilite la comunicación y se precise el tipo de información que pretende obtener. El perito 3, además ha observado que los fiscales no visualizan el contenido de la muestra antes de realizar el requerimiento a la Oficina de Peritajes. El hacerlo ayudaría a precisar el objeto de estudio y precisar el rango de tiempo. Visualización que muchas veces es realizado por el fiscal en las instalaciones de la Oficina de Peritajes, ocupando el poco espacio que tienen y una de las pocas PC con las que cuentan.

En esa misma línea, el perito 1, solicita que los fiscales sean capacitados en procedimientos de informática forense para que orienten mejor sus solicitudes y sepan qué se puede recuperar y qué no se puede realizar en una pericia informática. Asimismo, se recomienda:

Tabla 32. Aspectos a mejorar de la relación fiscal–perito

PERITO	ASPECTOS POR MEJORAR
Perito 1	Sería bueno que el fiscal trabaje conjuntamente con el perito ya ellos conocen el caso y nos pueden indicar que información podemos buscar, pero muchas veces eso no se da por la imposibilidad que el fiscal pueda quedarse trabajando con el perito ya sea por la lejanía o la alta demanda que se tiene
Perito 2	Mejorar la comunicación entre fiscales y peritos
Perito 3	Una mejor coordinación previa a la solicitud de la pericia

Los tres peritos coinciden en que un aspecto a mejorar de la relación con los fiscales, es la comunicación y coordinación. El perito 1, considera importante que el fiscal trabaje conjuntamente con el perito para precisar la información que se pretende analizar. Para el perito 3, la coordinación debería ser previa a la solicitud de la pericia, de ese modo se evitaría solicitudes sin especificar el objeto de estudio.

Tabla 33. Recomendaciones para mejorar la labor de los peritos y la calidad de las pericias

PERITO	RECOMENDACIONES
Perito 1	Descentralizar el área de análisis digital forense para descongestionar el cuello de botella generado en Lima por la alta demanda de requerimientos a nivel nacional
Perito 2	Capacitaciones con fines de actualización y adquisición de herramientas forenses
Perito 3	Instrucción en Criminalística

El perito 1, sugiere descentralizar el Área de Análisis Digital Forense lo que permitiría reducir la alta demanda de requerimientos. El perito 2, sugiere desarrollar capacitaciones y adquirir herramientas forenses.

El perito 3, recomienda que se instruya en criminalística a los peritos y que se cree el Área de Gestión de Requerimientos dentro de la Oficina de Peritajes, que se encargue de registrar, seleccionar y evaluar los requerimientos fiscales, antes de que sea derivado. El Área de Gestión serviría como filtro y evitaría distraer a los peritos con solicitudes poco claras y confusas. Asimismo, recomienda establecer un software de control de la productividad que permita medir el tiempo de trabajo de cada perito y de cada pericia, así como permita conocer el avance y ubicación del requerimiento.

IV. ANÁLISIS COMPARADO DE UNIDADES ESPECIALIZADAS

4. EXPERIENCIAS COMPARADAS DE UNIDADES QUE INVESTIGAN LA CIBERDELINCUENCIA

El desarrollo de este capítulo, se basó en el Informe de las Naciones Unidas denominado "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos"; así como, en las conclusiones arribadas en la Conferencia Internacional y Segunda Reunión de CiberRed de la Asociación Iberoamericana de Ministerios Públicos-AIAMP, realizados en Santiago de Chile el 25 y 26 de junio de 2019, en donde se identificaron modelos adoptados por las fiscalías de los diferentes países de Iberoamérica para hacer frente a la ciberdelincuencia:

1. Unidades de investigación centralizadas nacionales especializadas;
2. Unidades de coordinación nacional, con descentralización de la investigación en puntos focales;
3. Unidades nacionales de coordinación (centradas específicamente en la capacitación y el apoyo a distancia) y dispersión de la investigación;
4. Unidades nacionales de investigación (no específicamente especializadas);
5. Unidades nacionales de apoyo técnico, con dispersión de la investigación y
6. La inexistencia de especialización.

Así, se estableció una ficha que recogió las características esenciales de los modelos adoptados en España, Portugal, Chile, Paraguay, Colombia, Costa Rica y Argentina, con el apoyo de analistas de la OFAEC y del Gabinete de Asesores de la Fiscalía de la Nación, contándose además con las reuniones de trabajo convocadas por la Comisión encargada de evaluar técnicamente la creación de un piloto de Fiscalía o Unidad Especializada en Ciberdelincuencia. Adicionalmente, la OFAEC se reunió los días 18 y 23 de noviembre por videoconferencia con el responsable de la Unidad Fiscal Especializada en Ciberdelincuencia de la Procuraduría General de Argentina, así como, con fiscales de la Asesoría Técnica y Relaciones Internacionales y de la Fiscalía de Fraudes y Cibercrimen de Costa Rica.

El tipo de unidad que predominó, fue el de Unidad de Coordinación Nacional con descentralización en la investigación, que es el modelo seguido por España, Portugal y Argentina, con facultades de investigación en casos complejos, emblemáticos o de crimen organizado y capacidad de coordinar con fiscalías o puntos de enlace en demarcaciones territoriales así como de brindar formaciones, generar y difundir buenas prácticas a cualquier fiscalía que enfrente delitos de ciberdelincuencia en el sentido amplio del término.

4.1. ESPAÑA

PAÍS	ESPAÑA
Nombre de dependencia	MINISTERIO FISCAL
Tipo de unidad	Unidad de Coordinación Nacional con Descentralización de la Investigación
Norma de creación	Ley Orgánica 5/2010 del 22 de agosto de 2006. Ley Orgánica 1/2015 Y Ley Orgánica 2/2015 DEL del 30 de marzo de 2015.
Competencia • **Material** • **Territorial**	**Delitos competencia propia del Área de especialización:** · Delitos relacionados con ataques a los sistemas de información · Delitos de pornografía infantil · Delitos de Child grooming · Delitos de estafa cometidos a través de manipulaciones informáticas · Delitos contra la propiedad intelectual cometidos a través de las TIC **Delitos en los que el Área de Especialización asume la coordinación y/o intervención en supuestos complejos:** · Delitos de estafa tradicional planificados y ejecutados online · Ciberodio-Discurso del odio online · Delitos contra bienes personalísimos en entorno tecnológico
Funciones	· Potenciar e impulsar la unificación de criterios en la interpretación y aplicación de las normas jurídicas. · Garantizar la actuación coordinada en la investigación y enjuiciamiento de acciones ilícitas con proyección en más de una Fiscalía provincial. · Realizar el control y seguimiento de expedientes objeto de intervención o de coordinación del Área de Especialización. · Formación de los Fiscales en las materias propias de la Especialidad. · Promover/facilitar comunicaciones con otros colectivos e instituciones.
Objetivos	**Intervención directa en asuntos competencia del Área de Especialización:** · Competencia ordinaria: secciones territoriales · Competencia excepcional: Unidad Central Especializada

PAÍS	ESPAÑA
Marco regulatorio • **Legislación especial** • **Procedimiento especial investigación** • **Cooperación internacional** • **Procedimiento evidencia digital**	· Art.124 CE y Estatuto Orgánico Ministerio Fiscal · Aspectos procesales: Reforma LECrim por L0 13/2015 5/OCT sobre investigación tecnológica · Unidad Central Especializada: Fiscal de Sala, Fiscales Adscritos, Unidades de enlace con Policía Nacional y Guardia Civil · Red de fiscales especialistas-dimensión nacional
Organización/ Estructura	**Red compuesta por 145 fiscales:** · 3 Fiscales integrados en la Unidad Especializada contra la Criminalidad Informática de la Fiscalía General del Estado. · 1 Fiscal de enlace en la Fiscalía de la Audiencia Nacional. · 50 Fiscales delegados al frente de cada una de las secciones territoriales especializadas en las que a su vez desempeñan sus funciones. · 60 Fiscales colaboradores. · 31 fiscales de enlace distribuidos en las Fiscalías de Área constituidas en 17 demarcaciones provinciales.

4.2. PORTUGAL

PAÍS	PORTUGAL
Nombre de dependencia	Gabinete de Cibercrimen (OFICINA DE CIBERDELITO)
Tipo de dependencia	Unidades de Coordinación Nacional, con descentralización de la investigación en puntos focales
Norma de creación	Se creó en febrero del año 2011 (no se tuvo acceso a la norma)
Competencia • **Material** • **Territorial**	**La Oficina de cibercrimen es una oficina de coordinación centralizada que rige a nivel nacional.** **Los Procuradores especializados en ciberdelitos rigen en cada distrito y son competentes para investigar:** · Casos puros (comprendidos en la Ley). · Casos de cualquier naturaleza, pero donde la prueba digital será determinante. · Casos de crímenes clásicos como estafas o pornografía si el medio informático es determinante para la comisión del delito lo investigan los procuradores.
Funciones	**Oficina de cibercrimen** · Coordinar con la estructura del Ministerio Público (en temas de ciberdelitos y obtención de prueba y/o evidencia digital). Enfocado, sobre todo en los métodos que deben ser aplicados en todo el territorio. · Capacitar a magistrados del Ministerio Público en tema de ciberdelito y evidencia digital. Las básicas, en cada comarca y avanzada, en sede central- Lisboa. · Interactuar con los distintos cuerpos de policía (difusión de buenas prácticas, establecer rutinas procesales, normas de obtención digital, etc). · Interactuar con el sector privado. · Acompañar las investigaciones. **Procuradores especializados en cibercrimen** · Son puntos de contacto encargados de coordinar con la Oficina Central para ver los métodos que deben aplicar
Marco regulatorio	· Con Ley del Ciberdelito, Ley N°109/2009, mediante el cual se regulan los delitos informáticos a luz del Convenio de Budapest. · Ley de Protección de Datos, Lei n° 58/2019, de fecha 8 de agosto de 2019. · Cuentan también con otras fuentes legislativas como el Código Penal. Se regulan tipo penales como la pornográfica infantil, estafa informática. · Incorporar en legislación internacional normas procesales y de cooperación específicas de entorno digital.

PAÍS	PORTUGAL
Organización/ Estructura	• La Oficina de Cibercrimen depende de la Procuraduría General de la República (Fiscal General). Cuentan con una Coordinación Nacional y un grupo técnico de apoyo (fiscales que brindan apoyo en términos de coordinación desde sus comarcas). • Procuradores especializados en ciberdelitos en cada uno de las comarcas (48 distribuidos en las 23 comarcas- se asigna de acuerdo a la dimensión del mismo)

4.3. CHILE

PAÍS	CHILE
Nombre de dependencia	Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (ULDDECO).
Tipo de dependencia	Unidades nacionales de coordinación (centradas específicamente en la formación y el apoyo a distancia) y dispersión de la investigación
Norma de creación	Resolución de la Fiscalía de la Nación N° 1506 del 2 de agosto de 2017
Competencia • **Material** • **Territorial**	La Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (ULDDECO, es una unidad centralizada que rige a nivel nacional. En todo el país, hay 769 fiscales para todo tipo de delitos, continúan 18 Fiscales Regionales (máxima autoridades), uno por cada región, más 4, que pertenecen a la región Metropolitana de Santiago de Chile. Cada Fiscalía Regional tiene sus abogados asesores y tiene algunos profesionales de análisis criminal en estas unidades, conocidas como Fiscalías de Foco.
Funciones	**En asesoría y asistencia internacional:** · servir de guía para la obtención de evidencia digital de proveedores de servicios en el extranjero y Proveedores nacionales. Les brinda asistencia penal formal. **En apoyo a la investigación** · Brindar asesoría legal de investigaciones por delitos de leyes 20.009 (uso fraudulento tarjetas de pago y transacciones electrónicas) y 19.223 (delitos informáticos). Propuestas de diligencias. Coordinaciones interinstitucionales (policías, especializadas, empresas, etc.). Asesor en gestiones internacionales. Propuestas de minutas de formalización, entre otras. A la Unidad Especializada en Derechos Humanos, Violencia de Género y Delitos Sexuales (UDDHH): la Preparación de los Fiscales en las investigaciones desarrolladas por delitos de elaboración y distribución de pornografía infantil. · Brindar jornadas de tecnologías de apoyo a la investigación y de manejo de evidencia digital. · Para el procesamiento de evidencia digital, se utilizan equipos computacionales estacionarios y móviles potenciados para el procesamiento y análisis de evidencia digital, los cuales trabajan en conjunto con software específicos para cada una de las tareas que se desprenden en cada una de las pericias realizadas. · El manejo de estas tecnologías otorga a la Fiscalía cierto grado de autonomía en materias informáticas forenses y genera productos que están disponibles para todos los fiscales, en investigaciones por delitos de distinta naturaleza, consideradas de alta connotación pública y/o especialmente sensibles y complejas.

PAÍS	CHILE
Objetivos	Los objetivos lo toman como ventajas, siendo: i) Conocer las tecnologías y sus desafíos (técnicos y jurídicos). ii) Tener mínima capacidad autónoma de apoyo con herramientas propias. iii) Contribuir al sistema con estándares técnicos.
Marco regulatorio	**1. Legislación Especial** · Leyes vigentes en la materia en Chile en la materia, se tiene las siguientes leyes: · Ley 19.223 (1993) tipifica los delitos informáticos de ataque a los sistemas, taque a los datos, acceso e interceptación ilícita y revelación de datos informáticos · Ley 20.009 (modificada en mayo de 2020 por ley 21.234) que tipifica el uso fraudulento de tarjetas de pagos y transacciones electrónicas, y el nuevo delito que sanciona la defraudación informática en Chile. **2. Procedimiento especial** • **En cuanto a leyes procesales:** No se tiene una regulación procesal adecuada (proyecto de ley). La única consideración especial respecto de la evidencia digital prescrita en el artículo 222 del CPP que establece que las empresas telefónicas y de comunicaciones deberán mantener un registro actualizado de sus direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. Lo anterior bajo reserva y para su entrega ante requerimiento del Ministerio Público. • **Reformas legales relacionadas a la especialidad:** Ley 21.234 publicada el 29 de mayo de 2020 (modifica ley 20.009), aborda: La ampliación del objeto material del delito: tarjetas de pago y transacciones electrónicas. Tipificación del "fraude informático" (inc. final art. 7). Técnicas especiales de investigación para investigar agrupaciones de dos o más personas o asociaciones ilícitas; y otros. Se incorporó que El delito de tarjetas es la base del delito de lavado de dinero. **3. Cooperación Internacional** · Unidad de Cooperación Internacional y Extradiciones (UCIEX), es una unidad de apoyo que funciona a nivel central, teniendo un enlace a nivel regional y de cooperación con las regiones del país, con una competencia amplia, siendo una autoridad central solo para asistencia mutua y no para extradiciones, en ese caso, la autoridad central para las extradiciones vendría a ser la Cancillería. Asimismo, el rol principal es el de apoyo y asesoría a todos los fiscales, abogados asistentes y abogados asesores, en todos sus requerimientos de cooperaciones, por ejemplo, se le otorgan formatos, asistencias, capacitaciones, solicitudes de extradiciones activas y pasivas; incluso, se brinda asesoría de cómo llevar a cabo los requerimientos solicitados por otros estados o países, a fin de como ejecutar de la mejor manera la labor solicitada. · Para el procesamiento de evidencia digital, se utilizan equipos computacionales estacionarios y móviles potenciados para el procesamiento y análisis de evidencia digital, los cuales trabajan en conjunto con software específicos para cada una de las tareas que se desprenden en cada una de las pericias realizadas.
Organización/Estructura	· La ULDDECO, tiene un área legal y una no legal, en donde hay un Subdirector de Análisis y Tecnologías de apoyo a la Investigación, del cual depende los informáticos que a lo largo de los años han sido capacitados como peritos, cumpliendo obligaciones en la asesoría técnica y netamente en las pericias.

4.4. PARAGUAY

PAÍS	PARAGUAY
Nombre de dependencia	Unidad Especializada de Delitos Informáticos.
Tipo de dependencia	Unidad de investigación centralizada nacional especializada
Norma de creación	Creada por Resolución de la Fiscalía General del Estado No. 4408/2011 del año 2011
Competencia • **Material** • **Territorial**	En cuanto a su competencia material, según las Resoluciones No. 3459/10 y 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes: · Acceso indebido a datos · Interceptación · Preparación al acceso indebido a datos · Alteración de datos · Acceso indebido a sistemas informáticos · Sabotaje a sistemas informáticos · Alteración de datos relevantes · Falsificación de tarjetas de crédito y débito · Estafa mediante sistemas informáticos. Tiene competencia territorial en todo el país
Funciones	· Llevar a cabo de la investigación en los delitos de su competencia. · Brindar apoyo técnico-jurídico a los agentes fiscales en la realización de diligencias. · Brindar asesoramiento a los agentes fiscales que lo soliciten, en cuanto a la realización de diligencias de investigación vinculadas al uso de sistemas informáticos. · Realizar el registro o decomiso de datos informáticos almacenados
Objetivos	Combatir los hechos punibles cometidos a través del uso de la tecnología que requieran de un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital

PAÍS	PARAGUAY
Marco regulatorio	**1. Legislación especial:** Las Resoluciones de la Fiscalía General del Estado No. 3459/10 y 4408/11 delimitaron los tipos penales de competencia exclusiva de dicha unidad. Y, mediante esta última se creó la Unidad Especializada de Delitos Informáticos. Además, se debe tener en cuenta las siguientes normas: · La Ley No. 3.440 publicada el 20 de agosto de 2008, que modificó diversos artículos del Código Penal (Ley No. 1160/97), entre otros, aquellos vinculados a los delitos contra la propiedad intelectual. · La Ley No. 4439 publicada el 05 de octubre de 2011, que modificó y amplió diversos artículos del Código Penal (Ley No. 1160/97). Mediante dicha norma se modificaron los siguientes delitos: artículo 140, Pornografía Infantil; artículo 175, Sabotaje de Sistemas Informáticos; y, artículo 188, Estafa mediante sistemas informáticos. · La Ley No. 5994 de fecha 20 de diciembre de 2017, que suscribió el Convenio de Ciberdelincuencia de Budapest **2. Procedimiento especial**: No se ha encontrado un procedimiento especial de investigación para los delitos informáticos. Se siguen las reglas del Código Procesal Penal, Ley No. 1286-98. Así, el artículo 52 de dicha norma dispone que son los agentes fiscales lo encargados de dirigir la investigación de los hechos punibles y promover la acción penal pública. **3. Cooperación Internacional:** Suscripción al Convenio de Ciberdelincuencia de Budapest, que se encuentra vigente en Paraguay a través de la Ley No. 5994 de fecha 20 de diciembre de 2017. · La Fiscalía General del Estado firmó un convenio en el año 2014, con el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC, siglas en inglés), a fin de agilizar el intercambio de información en los casos de sospecha de pornografía infantil. **4. Procedimiento evidencia digital:** No hay un protocolo específico, sino que se emplea el utilizado para el manejo de todas las evidencias de cualquier (Sequera y Samaniego, 2018, p. 48). · A nivel policial se rigen por el “Manual Policial de Criminalística, Tomo 27, Guía de Procedimientos de Campo y Laboratorio”, que contiene lineamientos desde la protección del lugar, la observación, la fijación de indicios, el levantamiento de evidencias, hasta la remisión a las áreas respectivas para su procesamiento. · A nivel Fiscal, se rigen por la Resolución F.G.E. No. 2443 de fecha 06 de junio de 2013, que aprobó la nueva estructura orgánica y el manual de funciones de la Dirección de Evidencias, que tiene como objetivo coordinar la recepción, guarda, custodia y entrega de las evidencias que sean presentadas ante la Dirección en el marco de un proceso penal.
Organización/Estructura	· La Unidad Especializada de Delitos Informáticos depende directamente de la Fiscalía General del Estado. · La Fiscalía General del Estado está a cargo de un total de 13 fiscalías especializadas. · Su competencia es nacional, por lo que investigan los delitos realizados en cada una de las XII áreas en las que se encuentra dividido el territorio a efectos fiscales. Además, coordina con la División Especializada contra delitos informáticos de la Policía Nacional, cuya actividad se encuentra reglamentada entre los artículos 38 al 40 de la Resolución No. 539 de fecha 31 de mayo de 2012.

4.5. COLOMBIA

PAÍS	COLOMBIA
Nombre de dependencia	Dirección de Apoyo a la Investigación y análisis contra la criminalidad organizada.
Tipo de dependencia	Unidades Nacionales de Investigación (no específicamente especializadas). Los temas de ciberdelito son abordados por unidades nacionales especializadas, pero no específicamente en cibercrimen, sino en temas más amplios, como el crimen organizado. Asimismo, existen investigaciones por ciberdelitos en otras fiscalías locales (comunes) no especializadas.
Norma de creación	Decreto Ley N° 016, del 2014 -modificado por el Decreto Ley N° 898, del 2017-.
Competencia • **Material** • **Territorial**	• A nivel de **competencia material,** se Investigan todos los delitos informáticos contenidos en el Título VII BIS del Código Penal colombiano. • En lo referente a la **competencia territorial,** algunos casos de delitos cibernéticos son destacados a una unidad nacional especializada en la investigación del **crimen organizado (con competencia nacional)**. • Sin embargo, la competencia de esta unidad nacional no es exclusiva, y hay investigaciones de casos de delitos cibernéticos dispersos por las **distintas unidades territoriales del país** (fiscalías locales -Bogotá, Manizales, Cali, Medellín, etc.-.
Funciones	**Dirección de Apoyo a la Investigación y Análisis contra La Criminalidad Organizada** Conforme el artículo 17 del Decreto Ley N° 016, del 2014 -modificado por el Decreto Ley N° 898, del 2017-, posee las siguientes funciones: 1. Asesorar, acompañar y apoyar casos o situaciones de competencia de la Delegada, con el fin de consolidar una estrategia jurídica e investigativa integral. 2. Realizar barras académicas con el fin de discutir problemas jurídicos doctrinales, jurisprudenciales y de casos, relevantes para el adecuado cumplimiento de las funciones de la Delegada. 3. Realizar investigaciones analíticas y en contexto y excepcionalmente ejercer la acción penal sobre casos o situaciones priorizados por el Comité Nacional de Priorización de Situaciones y Casos o asignados por el Fiscal General de la Nación. 4. Elaborar e implementar los planes de acción en el ámbito de su competencia, de acuerdo con la metodología diseñada para el efecto. 5. Aplicar las directrices y lineamientos del Sistema de Gestión Integral de la Fiscalía General de la Nación. 6. Las demás que le sean asignadas por la ley, por la Delegada contra la Criminalidad Organizada o por el Fiscal General de la Nación o el Vicefiscal General de la Nación.

PAÍS	COLOMBIA
Marco regulatorio • **Legislación especial** • **Procedimiento especial investigación** • **Cooperación internacional** • **Procedimiento evidencia digital**	· No existe una legislación especial. Los delitos informáticos se encuentran regulados en el Código Penal colombiano del año 2000, a partir de la modificación efectuada por la Ley N° 1273, del 05 de enero 2009, en el Título VII BIS. · El Código de Procedimiento Penal de 2004, en su artículo 37, inc. 6, establece que los delitos informáticos serán evaluados por los Jueces Penales Municipales (no exigen alguna especialización - delitos comunes no tan graves, excepto cuando recae sobre bienes del Estado o cometidos por grupos criminales). · En lo concerniente a cooperación internacional, ésta se rige por las normas del Código de Procedimiento Penal de 2004. · No se cuenta con un instrumento legal especializado de recojo de evidencia digital.
Organización/Estructura	1. La Fiscalía General de la Nación, la que cuenta con un Cuerpo Técnico de Investigaciones (CTI), que coadyuvan a la labor de identificación de los ciberdelitos. 2. Vicefiscal General de la Nación. 2.1 Delegada Contra la Criminalidad Organizada 2.1.1. Dirección de Apoyo a la Investigación y Análisis Contra la Criminalidad Organizada. 3. Fiscalías locales (conforme a cada ciudad).

4.6. COSTA RICA

PAÍS	COSTA RICA
Nombre de dependencia	Ministerio Público
Tipo de dependencia	Unidad Especializada Centralizada
Norma de creación	2017 a través de Budapest
Competencia • **Material** • **Territorial**	En todo el país conectan con una Rectoría
Funciones	Dirigir y controlar la investigación tenemos una dirección más fuerte, más de autoridad como fiscales a la hora de tomar decisiones que la investigación, y no la dejamos simplemente al arbitrio de una unidad policial.
Objetivos	Lucha contra el crimen organizado que afecten a los recursos de las personas y estas se queden sin sustento (Cibercrimen)
Marco regulatorio • **Legislación especial** • **Procedimiento especial investigación** • **Cooperación internacional** • **Procedimiento evidencia digital**	· Convenio de Budapest. · Consejo Europeo 247 · LEY No. 8148 Ley de Delitos Informáticos · Manual para Fiscales · Solicitudes siguiendo el procedimiento del Consejo Europeo
Organización/Estructura	1 Fiscal Coordinador, 1 Fiscal adjunto ,4 Fiscales auxiliares, 1 técnico por fiscal auxiliar

4.7. ARGENTINA

PAÍS	ARGENTINA
Nombre de dependencia	Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)
Tipo de dependencia	Unidad de Investigación Centralizada Nacional Especializada
Norma de creación	Creada con Resolución PGN N° 3743/15, de la Procuraduría General de la Nación, el 18 de noviembre de 2015. Argentina.
Competencia • **Material** • **Territorial**	Casos de ilícitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y crímenes en los que sea necesario realizar investigaciones en entornos digitales –aun cuando no hayan sido cometidos contra o mediante un sistema informático-.
Funciones	· Intervenir en los casos de su competencia y asistir a los/as fiscales. · Recibir denuncias y realizar investigaciones preliminares y genéricas. · Actuar como nexo con los diferentes actores e instituciones nacionales e internacionales con incidencia en cuestiones vinculadas a la temática. · Articular con las procuradurías, unidades fiscales y demás áreas de la Procuración General, a los efectos de la implementación de estrategias eficaces para el abordaje de la ciberdelincuencia. · Asesorar a los/as fiscales sobre los recursos tecnológicos y herramientas de apoyo técnico, laboratorios, métodos de investigación, obtención, análisis y preservación de la prueba, disponibles en el país. · Desarrollar estudios acerca de las reformas reglamentarias y legislativas necesarias. · Elaborar informes y diagnósticos sobre esta clase especial de criminalidad. · Desarrollar actividades de cooperación, divulgación y capacitación sobre cibercrimen
Objetivos	"Trabaja en el ámbito de la prevención general al usuario y de información al investigador para saber cuáles son los elementos que debe tener en cuenta en la investigación y que, a su vez, pueda recopilar las pruebas que necesita para el caso".
Marco regulatorio • **Legislación especial** • **Procedimiento especial investigación** • **Cooperación internacional** • **Procedimiento evidencia digital**	· Resolución 43/2019:Reglamento para la Administración de Dominios de Internet en Argentina · Disposición 153 - E/2016: Reglamento para la administración de dominios de internet en Argentina · Resolución 42/2019: Reglamento para la administración de dominios de internet en Argentina
Organización/Estructura	Áreas de Investigación y Litigio estratégico, Cooperación local e internacional, Análisis tecnológico, Formación, capacitación y comunicación y Gestión.

V. UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DEL MINISTERIO PÚBLICO

5.1. UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DEL MINISTERIO PÚBLICO

La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, fue creada el 30 de diciembre de 2020, a través de la Resolución de la Fiscalía de la Nación N°1503-2020-MP-FN. Dicha creación se realiza en el marco de los compromisos asumidos por el Estado Peruano al suscribir el Convenio de Budapest en el año 2019 y para garantizar el debido cumplimiento de Ley N°30096, Ley de delitos informáticos vigente desde el 2013, como respuesta institucional ante el incremento de la ciberdelincuencia en el país. En dicha Resolución se dispone además la creación de la "Red de fiscales en ciberdelincuencia a nivel nacional" que serán los puntos de contacto de cada distrito fiscal con la Unidad Fiscal Especializada.

Su creación se sustenta en las recomendaciones y sugerencias alcanzadas por la "Comisión encargada de evaluar técnicamente la creación de un Piloto de Fiscalía Especializada o Unidad Especializada en Ciberdelincuencia del Ministerio Público" conformada mediante Resolución de Fiscalía de la Nación N°1025-2020-MP-FN, de fecha 18 de setiembre de 2020 y cuyos plazos fueron ampliados con Resolución de Fiscalía de la Nación N°1194-2020-MPFN, de fecha 30 de octubre de 2020. Dicha comisión contó con la asistencia técnica del Programa de Asistencia contra el Crimen Transnacional Organizado de la Unión Europea (PACCTO) y de la Embajada de Estados Unidos en Perú. Estableció jornadas de trabajo, con reuniones virtuales semanales, que implicó el intercambio de ideas y el análisis de información relevante como las iniciativas de las fiscalías de otros países en la lucha contra la ciberdelincuencia; los tipos penales con mayor incidencia delictiva en el Ministerio Público; así como los distritos fiscales con mayores registros de denuncias en delitos informáticos.

La Unidad Fiscal Especializada, tendrá entre sus funciones el acompañamiento técnico a los fiscales en la realización de la investigación en los delitos de la Ley N°30096, Ley de delitos informáticos, de estafa agravada prevista en el inciso 5 del artículo 196-A del Código Penal, además de aquellos casos en los cuales la obtención de la prueba digital sea determinante para el desarrollo de la investigación. Asimismo, establecerá lineamientos que oriente las investigaciones y la unificación de criterios en procedimientos y métodos de investigación en materia de ciberdelincuencia. Se encargará también de promover la capacitación permanente con la Escuela del Ministerio Público para todos los fiscales y peritos de la especialidad. Desarrollará herramientas de gestión que permitan orientar a los fiscales en su labor. Tendrá a su vez la potestad de articular con las áreas encargadas para proponer reformas reglamentarias y legislativas. Hará lo mismo con organismos estatales y privados de Perú y a nivel internacional de manera que pueda acceder a información y a colaboración para el desarrollo de las investigaciones.

De esta manera se marca el inicio de la especialización en la materia en el Ministerio Público con el único fin de dar una respuesta eficaz y oportuna a este tipo de delitos que suponen un desafío para el Sistema de Justicia por su uso intensivo de tecnologías de la información y las comunicaciones, y porque existe aún en la actualidad una escasa cultura de la prevención y el cuidado de los datos personales. Esperándose a corto plazo, implementarse fiscalías especializadas en ciberdelincuencia en los diferentes distritos fiscales a nivel nacional donde exista alta incidencia delictiva de estos delitos, además de fortalecer la unidad de peritos en esta materia.

UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DEL MINISTERIO PÚBLICO CON COMPETENCIA NACIONAL	
OBJETIVOS	1. Brindar un tratamiento especializado de los denominados ciberdelitos. 2. Efectuar la orientación técnico-jurídica en las investigaciones de los ciberdelitos y de los delitos que son cometidos por los medios tecnológicos, así como recolección, manejo de evidencia y prueba digital, cuando los fiscales lo soliciten. 3. Realizar las gestiones necesarias con instituciones públicas y privadas para la eficiencia en el servicio fiscal en estas clases de delitos. 4. Procesar la información de la evolución de los sistemas informáticos, redes y datos informáticos, y tecnologías de la información y comunicación; en particular la forma de cómo son usadas para la comisión de delitos con el fin de crear mecanismos eficaces para su persecución y prevención.
ORGANIZACIÓN	· Depende administrativa y funcionalmente de la Fiscalía de la Nación y está conformada por: · Un Fiscal Superior · Dos Fiscales Adjuntos Superiores · Un abogado · Un ingeniero informático · Un especialista en tecnología de la información y comunicación · Un perito · Un asistente en función fiscal · Un personal administrativo · Se conformará la “Red de Fiscales en Ciberdelincuencia” que serán lo puntos de contacto de cada distrito fiscal con la Unidad Fiscal Especializada.
COMPETENCIA MATERIAL	La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, tendrá competencia para conocer los siguientes delitos: 1. Ley 30096, Ley de delitos informáticos 2. Estafa agravada 3. Otros casos en los cuales la obtención de prueba digital sea determinante para la investigación
COMPETENCIA TERRITORIAL	La Unidad Fiscal Especializada tiene competencia territorial a nivel nacional y su sede se encuentra en la ciudad de Lima.
MARCO REGULATORIO	A nivel internacional: 1. Convenio de Budapest: Instrumento jurídico multilateral en materia de ciberdelincuencia del cual el Perú es Estado Parte. A nivel nacional: 1. Legislación especial: tipos penales de la Ley 30096, Ley de Delitos Informáticos, modificada por la Ley 30171. 2. Código Penal: artículo 196, concordado con el artículo 196-A numeral 5.

FUNCIONES	1. Brindar acompañamiento técnico a los fiscales en la realización de la investigación en los delitos de la Ley N°30096, Ley de delitos informáticos, estafa agravada prevista en el inciso 5 del artículo 196-A del Código Penal, y aquellos casos en los cuales la obtención de prueba digital sea determinante para la investigación. 2. Celebrar reuniones periódicas de trabajo con los fiscales integrantes de la "Red de fiscales en ciberdelincuencia a nivel nacional". 3. Unificación de criterios en procedimientos y métodos de investigación en materia de ciberdelincuencia. 4. Elaborar directivas, lineamientos, instructivos, guías u otros, en el ámbito de su competencia, que orienten las investigaciones de las Fiscalías Especializadas en Ciberdelincuencia o los fiscales que se nombren para esta finalidad de los distritos fiscales a nivel nacional. 5. Coordinar con la Oficina de Peritajes el adecuado y eficiente trabajo para el debido cumplimiento de las funciones asignadas a la Unidad Fiscal Especializada en Ciberdelincuencia. 6. Promover la articulación entre el Ministerio Público y la Policía Nacional, con el fin de hacer más eficiente el modelo de coordinación funcional y la dirección efectiva de la investigación fiscal en la materia. 7. Coordinar con las áreas afines para analizar y valorar datos estadísticos de los delitos de la Ley 30096, Ley de Delitos Informáticos, estafa agravada prevista en el inciso 5 del artículo 196-A del Código Penal, y aquellos casos en los cuales la obtención de prueba digital sea determinante para la investigación con el fin de establecer políticas institucionales que mejoren el trabajo fiscal en la materia. 8. Coordinar con las Presidencias de las Juntas de Fiscales Superiores a nivel nacional sobre el apoyo necesario para el debido cumplimiento de las funciones asignadas a la Unidad Fiscal Especializada en Ciberdelincuencia. 9. Coordinar con los organismos estatales y privados afines a la materia de ciberdelincuencia. 10. Coordinar con la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación, para el cumplimiento de sus funciones, así como para la atención de los requerimientos en el marco de la Red 24/7 del Convenio de Budapest. 11. Coordinar con las diversas redes internacionales (tales como CiberRed, REDCOOP de la AIAMP, Iberred y otros), a fin de poder brindar respuesta inmediata a los casos relacionados en materia de ciberdelincuencia. 12. Proponer a la Fiscal de la Nación, los proyectos de lineamientos, reglamentos y/o directivas orientados a optimizar la actuación funcional de la Unidad Fiscal Especializada en Ciberdelincuencia. 13. Absolver consultas y emitir informes sobre la materia. 14. Implementar y supervisar la ejecución de las políticas institucionales dictadas por la Fiscalía de la Nación en la materia. 15. Implementar y supervisar una plataforma virtual del Ministerio Público en la materia. 16. Coordinar y promover permanentemente la capacitación transversal especializada y por niveles (básico y avanzado) con la Escuela del Ministerio Público para fiscales y peritos de la especialidad y para los que investigan casos en los que la tecnología es un medio para cometer otro delito. 17. Presentar trimestralmente el informe de gestión al despacho de la Fiscalía de la Nación. 18. Las demás afines que resulten necesarias para el óptimo desempeño de la Unidad Fiscal Especializada en Ciberdelincuencia y la "Red de fiscales en ciberdelincuencia a nivel nacional", debiendo dar cuenta al despacho de la Fiscalía de la Nación.

Adaptado de Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN y del Informe de la Comisión encargada de evaluar técnicamente la creación de un Piloto de Fiscalía Especializada o Unidad Especializada en Ciberdelincuencia del Ministerio Público.

CONCLUSIONES

- El Perú al suscribir el Convenio de Budapest, instrumento jurídico específico sobre la materia de ciberdelincuencia, el mismo que luego del proceso de aprobación y ratificación, entró en vigencia desde el 01 de diciembre de 2019. En este sentido, nuestro país asumió el compromiso de la lucha frontal y efectiva contra la ciberdelincuencia y la necesidad de cooperación internacional rápida y eficaz en materia penal

- En el periodo correspondiente del 22 de octubre de 2013 al 31 de julio de 2020, ingresaron a las fiscalías penales comunes y fiscalías mixtas 21,687 denuncias por delitos informáticos. El 48% (10340) de las denuncias se registraron en el Distrito Fiscal de Lima y otro 35% (7668), fue registrado en siete distritos fiscales: Lima Norte (7%), Arequipa (6%), Lima Este (6%), La Libertad (5%) y Lambayeque (4%), Callao (3%) y Lima Sur (3%). El 83% de los delitos informáticos se concentró en ocho Distritos Fiscales.

- Los delitos contra el patrimonio representan el 42% (9014) de los delitos informáticos. Con pocos registros aparecen los delitos contra la fe pública (4%), contra datos y sistemas informáticos (3%), contra la indemnidad y libertad sexuales (2%), contra la intimidad y el secreto de las comunicaciones (1%) y por disposiciones comunes (0.7%). • El 21% (4493) de las denuncias se registró en once fiscalías, de cuatro distritos fiscales: Lima, Arequipa, Lambayeque y La Libertad.

- Durante el 2019 y julio del 2020, el Área de Análisis Digital Forense atendió 534 solicitudes de pericias. El 29% (156) de solicitudes se generó en el Distrito Fiscal de Lima. Otro 27% de solicitudes (141), se generó en los Distritos Fiscales de Callao, (8%) Huánuco (5%), Ancash (5%), Lima Norte (5%) y Santa (4%).

- El 43% (229) de las solicitudes al Área de Análisis Digital Forense fueron realizadas por Fiscalías Provinciales Penales y el 42% (224) por Fiscalías Especializadas. En menor porcentaje, las solicitudes fueron realizadas por la PNP (8%), Fiscalías Supremas (4%), Poder Judicial (0.9%), Fiscalías Superiores (0.7%), Control Interno (0.2%) y UCJIE (0.2%).

- Entre el 2018 y 2020, la Escuela del Ministerio Público registró 05 actividades académicas, en temas relacionados a ciberdelincuencia y delitos informáticos: tres actividades fueron virtuales y dos presenciales (ambas en la ciudad de Lima).

- Los cursos presenciales beneficiaron a 86 (18%) personas y los cursos virtuales a 389 (82%) personas: 214 fiscales, 93 asistentes en función fiscal, 5 especialistas del Instituto de Medicina Legal, 151 administrativos y 8 peritos.

- Durante el periodo de enero 2017 a octubre de 2020, la UCJIE ha registrado 99 asistencias judiciales activas y 28 asistencias judiciales pasivas, relacionadas a delitos informáticos y delitos en los que se utilizó la tecnología como medio determinante para su ejecución.

- El 45% de la asistencia judicial activa se ha orientado a la solicitud de información de cuentas de Facebook y, el 18% a las solicitudes de información de cuentas de correos electrónicos. Asimismo, se observa que en asistencias judiciales donde se ha solicitado más de un acto de cooperación, en diez ocasiones ha implicado a las redes sociales. Por tanto, el 54% de la asistencia judicial activa está relacionada a las redes sociales como Facebook, Messenger, Google, WhatsApp, etc.

- En la actualidad y, debido al incremento del uso de las redes informáticas y la información electrónica para cometer delitos, diversos países de la región tales como: Chile, Argentina, Brasil, Costa Rica, así como del continente europeo: Portugal, España, entre otros, cuentan con una Unidad Especializada en Ciberdelincuencia, entidad que se encarga no sólo de brindar lineamientos en el marco de las investigaciones por este tipo de ilícitos, unificación de los criterios de interpretación y aplicación de las normas, labor que la realizan en ciertos países con los puntos focales que fueron designados a lo largo de su territorio nacional, y en otros países con los despachos de fiscalías especializadas en dicha materia, siendo que dichos funcionarios son constantemente capacitados, así como se establecen reuniones de coordinación a fin de unificar criterios de investigación y difundir las buenas prácticas, medidas que han permitido establecer en dichos países.

- Del estudio efectuado, se evidencia la necesidad de la implementación de la especialización en ciberdelincuencia en el Ministerio Público, motivo por el cual, se ha creado la Unidad Fiscal Especializada en Ciberdelincuencia, con competencia nacional.

- La especialización, prevé la creación de redes de fiscales en ciberdelincuencia a nivel nacional, quienes serán los puntos de contacto con la Unidad Fiscal Especializada. A corto y mediano plazo, dependiendo de la disponibilidad presupuestaria se considera necesaria la implementación de fiscalías especializadas a nivel nacional. Resultando necesario el fortalecimiento del Área de Análisis Digital Forense de la Gerencia de Peritajes, tanto en recursos humanos como de implementos logísticos.

RECOMENDACIONES

Del análisis de la información solicitada para la elaboración del presente informe, así como de la participación en la Comisión encargada de evaluar técnicamente la creación de un Piloto o Unidad Especializada en Ciberdelincuencia en el Ministerio Público, de acuerdo a la Resolución de Fiscalía de la Nación N°1025-2020-MP-FN del 18 de setiembre de 2020, se arribó a las siguientes recomendaciones:

PARA LA UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DEL MINISTERIO PÚBLICO

- Asumir competencias técnicas y de capacidad resolutiva de alto nivel para investigar casos complejos por el grado de sofisticación del modus operandi, en materia de delitos informáticos.

- Generar lineamientos y buenas prácticas a través de la coordinación y capacitación de enlaces o dependencias descentralizadas.

- Implementar órganos de apoyo técnicos descentralizados, debidamente organizados e integrados por profesionales con alto perfil especializado, así como con equipamiento (hardware) para labores de análisis forense informático con adecuados niveles de seguridad de la información, y los adecuados programas informáticos (software) para dicha labor.

- Definir un estándar de productividad asociada a un Sistema de Gestión de Calidad, así como a funciones, productos y resultados.

PARA LA OFICINA CENTRAL DE TECNOLOGÍAS DE LA INFORMACIÓN

- Generar filtros para el obligatorio registro, en el Sistema de Gestión Fiscal, por parte de los fiscales provinciales penales, mixtos y especializados, del tipo de sentencia alcanzada, así como de los tipos sub genéricos y específicos de los delitos contemplados en la Ley 30096, Ley de delitos informáticos.

PARA LA OFICINA DE PERITAJES

- Diseñar e implementar una base de datos con información detallada de las pericias de análisis digital forense solicitadas y desarrolladas, así como de los requerimientos realizados por entidades del sistema de justicia.

- Solicitar la adquisición de equipos informáticos y "llaves" para los distintos softwares que utilizan.

- Establecer un sistema de seguimiento en web para el control de la productividad que permita medir el tiempo de trabajo de cada perito y de cada tipo de pericia, así como el avance del análisis forense.

- Descentralizar el Área de Análisis Digital Forense, con la creación de unidades en distritos fiscales con alta demanda de casos, lo que permitiría reducir la carga de requerimientos en Lima y agilizar los análisis forenses.

PARA LA ESCUELA DEL MINISTERIO PÚBLICO

- Diseñar y desarrollar programas de capacitación dirigido al personal administrativo, así como a peritos forenses y fiscales penales, especializados y mixtos, con competencias para atender casos de delitos informáticos; en el marco de la quinta disposición complementaria final de la Ley 30096: "las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal…"

- Establecer oferta educativa desde la Escuela del Ministerio Público que sea compartida a nivel de plan de estudios con instituciones del Sistema de Administración de Justicia para que servidores públicos y funcionarios de la Policía Nacional y el Poder Judicial sean capacitados en los mismos contenidos.

PARA LA UNIDAD DE COOPERACIÓN INTERNACIONAL Y EXTRADICCIONES

- Elaborar un Manual de Cooperación Internacional en Ciberdelincuencia, dirigido a fiscales penales, especializados y mixtos.

- Implementar mecanismos de coordinación con instituciones de alcance internacional que coadyuven en las labores de prevención e investigación fiscal que realiza el Ministerio Público

- Diseñar guías informativas, dirigido a fiscales penales, especializados y mixtos, para requerimientos a proveedores de servicios informáticos extranjeros, a proveedores de redes sociales y correos electrónicos y, en requerimientos ante la Unidad de Cooperación Judicial Internacional y Extradiciones del Ministerio Público.

BIBLIOGRAFÍA

- CiberRed (2019). Conferencia Internacional y Segunda Reunión. Conclusiones de la Coordinación. Santiago de Chile: Asociación Iberoamericana de Ministerios Públicos.
- CONAPOC (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Primera edición digital. Lima: MINJUS.
- El Paccto (2020). Apoyo a la creación de una Fiscalía Especializada en Ciberdelito en Perú.
- Ministerio Público (2020). Guía de Análisis Digital Forense del Ministerio Público.
- Miró Linares, F. (2013). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- OEA (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?
- ONU (2019). Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.
- Sequera, Maricarmen y Samaniego, Marlene (2018). Cibercrimen: Desafíos de la armonización de la Convención de Budapest en el Sistema Penal Paraguayo. Paraguay.
- Torrealba, Miguel y Devenish, Nandy (2017). Computación forense: Una revisión general de sus fundamentos y aproximaciones. Revista Venezolana de Legislación y Jurisprudencia. No 9. 2017.
- Villavicencio, Felipe (2014). Delitos informáticos. Revista IUS ET VERITAS, N° 49, diciembre 2014 / ISSN 19

MINISTERIO PÚBLICO
FISCALÍA DE LA NACIÓN

MINISTERIO PÚBLICO-FISCALÍA DE LA NACIÓN
Abancay cuadra 5 s/n Sede Central en Lima- Perú
Central Telefónica 625-5555/ anexos 5786-5787-5788
ofaec@mpfn.gob.pe