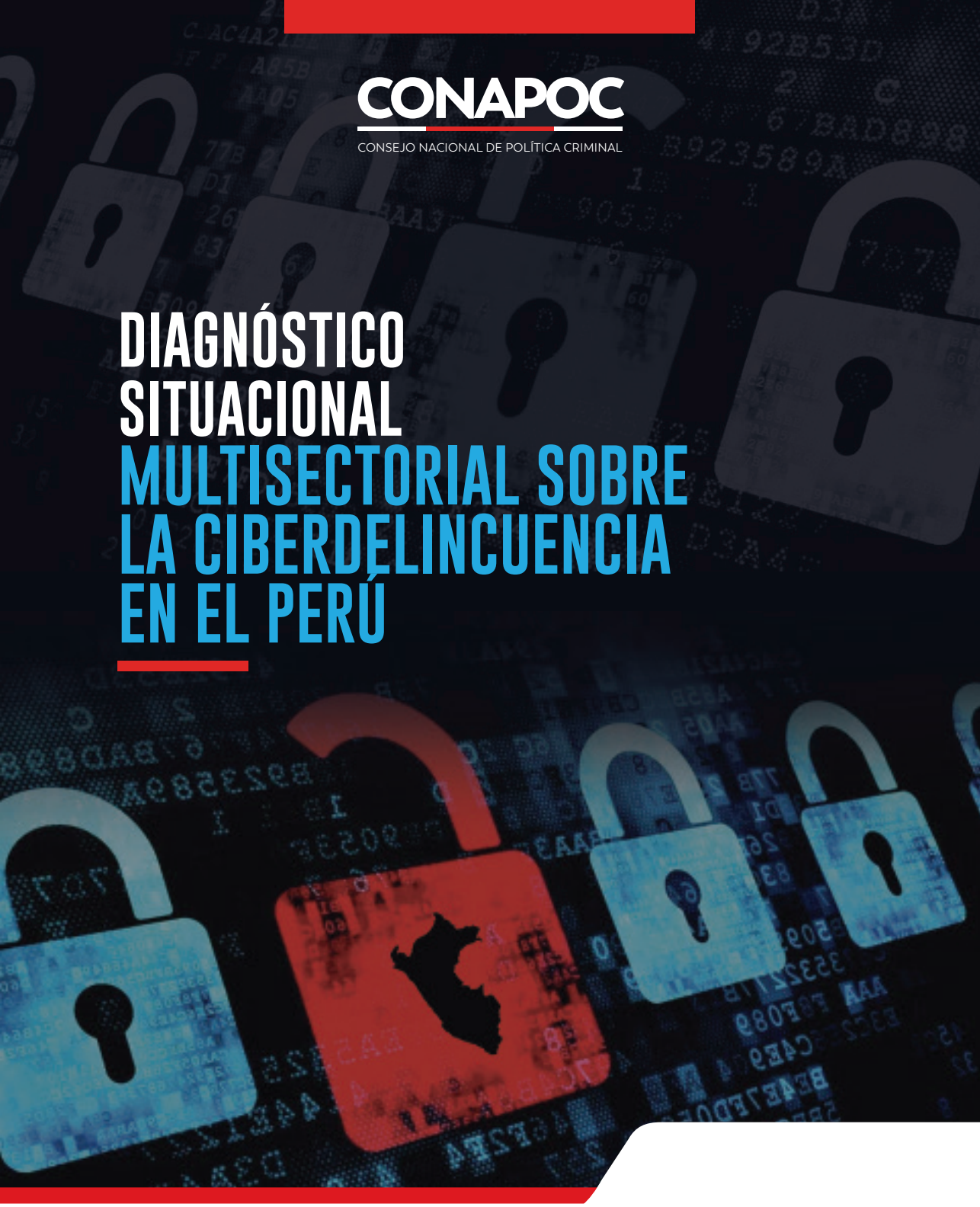
CONAPOC

CONSEJO NACIONAL DE POLÍTICA CRIMINAL

DIAGNÓSTICO SITUACIONAL MULTISECTORIAL SOBRE LA CIBERDELINCUENCIA EN EL PERÚ



PERÚ Ministerio de Justicia y Derechos Humanos

INDAGA
OBSERVATORIO NACIONAL DE POLÍTICA CRIMINAL

INDAGA
OBSERVATORIO NACIONAL
DE POLÍTICA CRIMINAL

DIAGNÓSTICO SITUACIONAL MULTISECTORIAL SOBRE LA CIBERDELINCUENCIA EN EL PERÚ

PERÚ
Ministerio
de Justicia
y Derechos Humanos

CONSEJO NACIONAL DE POLÍTICA CRIMINAL

PERÚ Ministerio de Justicia y Derechos Humanos

PERÚ CONGRESO de la REPÚBLICA

PODER JUDICIAL DEL PERÚ

MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN

PERÚ Ministerio del Interior

DEFENSORÍA DEL PUEBLO

INPE

ANGR

AMPE

MUNICIPALIDAD DE LIMA

EDUARDO VEGA LUNA
Ministro de Justicia y Derechos Humanos

FELIPE ANDRÉS PAREDES SAN ROMÁN
Viceministro de Justicia

MARIELLA LENKIZA VALCÁRCEL ANGULO
Directora General de Asuntos Criminológicos

ARTURO HUAYTALLA QUISPE
Coordinador del Observatorio Nacional de Política Criminal – INDAGA

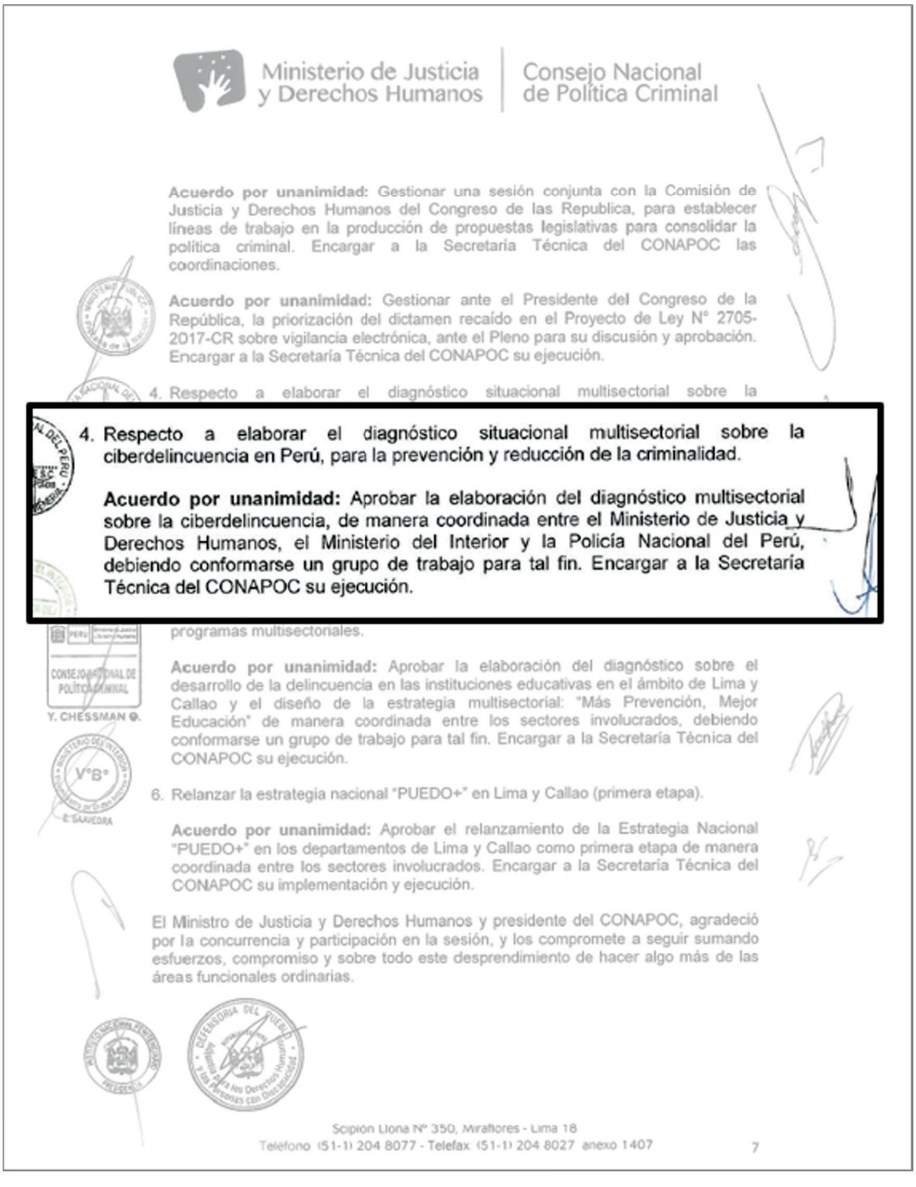
Responsables del documento:
Christian Flores Calderón
Grace Mosquera Huapaya
Tadeo Rodríguez Vargas
Mirian Cervantes Zapana
Luis Guerra Pallqui
Julissa Urbizagástegui Manrique

Diagramación:
Michael Bances Sandoval

Observatorio Nacional de Política Criminal
Calle Scipión Llona 350, Miraflores
https://indagaweb.minjus.gob.pe
ISBN: 978-612-4225-39-0

Primera edición digital, diciembre 2020

ÍNDICE



Ministerio de Justicia y Derechos Humanos | Consejo Nacional de Política Criminal

Acuerdo por unanimidad: Gestionar una sesión conjunta con la Comisión de Justicia y Derechos Humanos del Congreso de las Republica, para establecer líneas de trabajo en la producción de propuestas legislativas para consolidar la política criminal. Encargar a la Secretaría Técnica del CONAPOC las coordinaciones.

Acuerdo por unanimidad: Gestionar ante el Presidente del Congreso de la República, la priorización del dictamen recaído en el Proyecto de Ley N° 2705-2017-CR sobre vigilancia electrónica, ante el Pleno para su discusión y aprobación. Encargar a la Secretaría Técnica del CONAPOC su ejecución.

4. Respecto a elaborar el diagnóstico situacional multisectorial sobre la ciberdelincuencia en Perú, para la prevención y reducción de la criminalidad.

Acuerdo por unanimidad: Aprobar la elaboración del diagnóstico multisectorial sobre la ciberdelincuencia, de manera coordinada entre el Ministerio de Justicia y Derechos Humanos, el Ministerio del Interior y la Policía Nacional del Perú, debiendo conformarse un grupo de trabajo para tal fin. Encargar a la Secretaría Técnica del CONAPOC su ejecución.

programas multisectoriales.

Acuerdo por unanimidad: Aprobar la elaboración del diagnóstico sobre el desarrollo de la delincuencia en las instituciones educativas en el ámbito de Lima y Callao y el diseño de la estrategia multisectorial: "Más Prevención, Mejor Educación" de manera coordinada entre los sectores involucrados, debiendo conformarse un grupo de trabajo para tal fin. Encargar a la Secretaría Técnica del CONAPOC su ejecución.

6. Relanzar la estrategia nacional "PUEDO+" en Lima y Callao (primera etapa).

Acuerdo por unanimidad: Aprobar el relanzamiento de la Estrategia Nacional "PUEDO+" en los departamentos de Lima y Callao como primera etapa de manera coordinada entre los sectores involucrados. Encargar a la Secretaría Técnica del CONAPOC su implementación y ejecución.

El Ministro de Justicia y Derechos Humanos y presidente del CONAPOC, agradeció por la concurrencia y participación en la sesión, y los compromete a seguir sumando esfuerzos, compromiso y sobre todo este desprendimiento de hacer algo más de las áreas funcionales ordinarias.

CONSEJO NACIONAL DE POLÍTICA CRIMINAL
Y. CHESSMAN
V°B°
E. SAAVEDRA

Scipión Llona N° 350, Miraflores - Lima 18
Teléfono (51-1) 204 8077 - Telefax (51-1) 204 8027 anexo 1407

7

A través del Acuerdo N°4 de la XV Sesión del Consejo Nacional de Política Criminal, celebrada el 18 de julio de 2019, se acordó la elaboración de un documento técnico que brinde mayores aproximaciones al fenómeno de los ciberdelitos en nuestro país.

PRESENTACIÓN

Las acciones o actividades que las sociedades definen como ilegales, han variado y se han ajustado a lo largo del tiempo; adaptándose a las circunstancias en las que las personas, las instituciones, y, en general, las naciones han establecido sus flujos de movilización e intercambio de bienes y servicios, necesarios para la subsistencia.

Con la evolución de los sistemas de producción, así como de los procesos de intercambio de información, facilitados o impulsados por el desarrollo tecnológico de la cibernética durante los últimos treinta años, los actos ilícitos también han conseguido reinventarse y ajustarse a las nuevas condiciones, especialmente, a aquellas que tienen que ver con el espacio virtual en el que transitan importantes elementos de información, propiedad y riqueza de los ciudadanos y las ciudadanas, sin importar las barreras físicas o las fronteras entre las países y continentes.

Tomando en consideración las diferentes formas en las que las organizaciones delictivas infringen daños a los sistemas de información de las personas, así como de las instituciones públicas y privadas, los gobiernos de todo el mundo –en los márgenes que sus recursos y disposiciones normativas se lo permiten– han venido desarrollando importantes esfuerzos por controlar y reducir los actos delictivos que ocurren en el ámbito virtual y, ya sea considerándolos como medios o como fines en sí mismos, estos ciberdelitos imponen a los tomadores de decisiones, importantes retos en

materia de adecuación normativa, formación de capacidades e implementación de nuevas políticas para el resguardo del bienestar. Sin embargo, todas estas líneas de intervención no podrían ser posibles sin insumos de información que nos permitan acercarnos a la comprensión de los fenómenos, formas y dinámicas de la ciberdelincuencia.

Este trabajo, llevado a cabo por especial encargo del Consejo Nacional de Política Criminal, y hecho realidad gracias a la estrecha articulación entre las instituciones que lo componen, responde a la necesidad de ir avanzando en los compromisos que posee el Estado para generar alternativas de políticas públicas frente a los ciberdelitos, teniendo en cuenta a la evidencia y la información confiable.

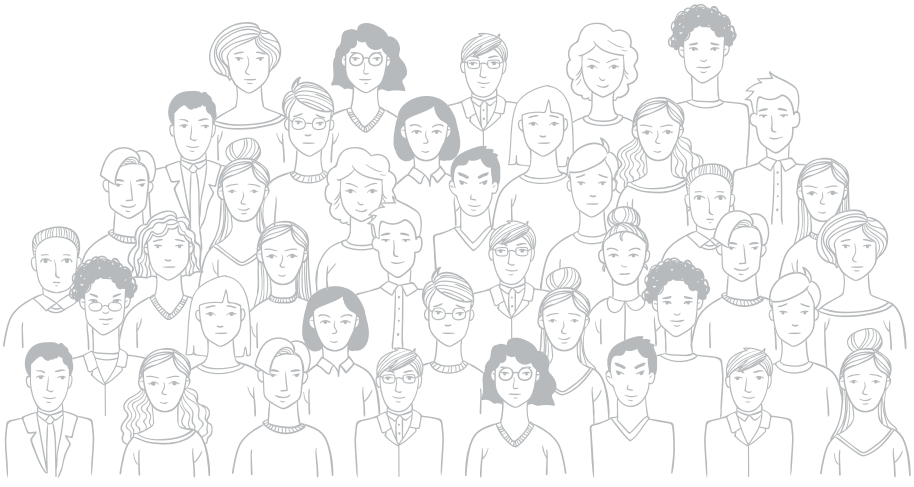
PRÓLOGO

La decisión de llevar a cabo la elaboración de un documento diagnóstico —que brinde mayor información—sobre la situación en la que se encuentran los ciberdelitos en nuestro país, así como las condiciones con las que cuenta el Estado para hacerles frente, constituye un parteaguas trascendente en el relato de la Política Criminal del Perú, pues se convierte en el primer gran esfuerzo de articulación interinstitucional que consolida la información de distintos sectores y entidades, teniendo en cuenta el rol que desempeñan frente a la criminalidad tras las pantallas, desde sus distintos ámbitos y funciones.

Desde que el CONAPOC encargara, luego de su XV Sesión, la elaboración del Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia;la Secretaría Técnica de este espacio —cuya responsabilidad recae sobre la Dirección General de Asuntos Criminológicos del MINJUSDH— ha desplegado importantes esfuerzos por tratar de conducir un proceso que permita elaborar un documento útil a la gestión de las políticas contra la criminalidad en el campo cibernético. En ese sentido, los compromisos establecidos y las comunicaciones entabladas son material indispensable que ahora ponemos a disposición de todas y todos aquellos quienes busquen herramientas de información sobre las cuales tomar sus decisiones o trazar intervenciones.

Además de incluir aquellas definiciones operativas y alcances elaborados con anterioridad por instituciones de la academia y/o centros de investigación; el trabajo realizado se robustece con información oficial que incluye bases de data estadística, registros administrativos y documentación descriptiva elaborada por las propias áreas a cargo del tratamiento de los casos de ciberdelitos, al interior de cada una de las instituciones que colaboraron en este proceso, a lo largo de los casi doce meses que ha tomado el análisis y la redacción.

Esperamos que el conocimiento organizado y presentado, a través de las siguientes páginas, sume considerablemente a las incansables labores del servicio público que buscan soportar sus actividades en evidencia.



AGRADECIMIENTOS

La elaboración de documentos como el que se traza en estas páginas, posee especial valor pues se realizó a consecuencia de la sinergia de múltiples esfuerzos de las diferentes instituciones que integran el Consejo Nacional de Política Criminal, quienes desde hace buen tiempo vienen impulsando importantes iniciativas para el resguardo de la seguridad y del bienestar de las y los ciudadanos de nuestro país.

Partiendo de ese impulso conjunto, la Dirección General de Asuntos Criminológicos del MINJUSDH —a través del equipo profesional de su Observatorio Nacional de Política Criminal— ha podido llevar a cabo la redacción de este texto que traslada las voces, perspectivas, preocupaciones y recursos de información que poseen las entidades que confrontan, día tras día, a las organizaciones criminales que se encuentran detrás de la comisión de los delitos que ocurren en el ciberespacio. Somos conscientes de que, sin la colaboración y disposición brindadas, las páginas que siguen no habrían podido convertirse en esa herramienta de evidencia que requiere el Estado con urgencia para hacer frente a la criminalidad detrás de los ordenadores. Por esa razón, extendemos un agradecimiento

especial a las áreas técnicas involucradas, participantes de este proceso de organización del conocimiento.

Subgerencia de Estadística
Poder Judicial del Perú

Unidad de Cooperación Judicial Internacional y Extradiciones
Ministerio Público – Fiscalía de la Nación

Dirección General de Información para la Seguridad
Ministerio del Interior

División de Investigación de Delitos de Alta Tecnología
Policía Nacional del Perú

Oficina Técnica de Informática
Instituto Nacional de Estadística e Informática

Gerencia de Seguridad Ciudadana
Municipalidad de Lima Metropolitana

Subdirección de Inteligencia Penitenciaria
Instituto Nacional Penitenciario

GLOSARIO DE SIGLAS Y ACRÓNIMOS

AMPE	:	Asociación de Municipalidades del Perú
ANGR	:	Asamblea Nacional de Gobiernos Regionales
BID	:	Banco Interamericano de Desarrollo
CONAPOC	:	Consejo Nacional de Política Criminal
CONASEC	:	Consejo Nacional de Seguridad Ciudadana
DIVINDAT	:	División de Investigación de Alta Tecnología de la PNP
DIRINCRI	:	Dirección de Investigación Criminal de la PNP
DGAC	:	Dirección General de Asuntos Criminológicos del MINJUSDH
GT	:	Grupo de Trabajo sobre Ciberdelincuencia
INDAGA	:	Observatorio Nacional de Política Criminal
INEI	:	Instituto Nacional de Estadística e Informática
INPE	:	Instituto Nacional Penitenciario
MININTER	:	Ministerio del Interior
MINJUSDH	:	Ministerio de Justicia y Derechos Humanos
MP-FN	:	Ministerio Público – Fiscalía de la Nación
ONU	:	Organización de las Naciones Unidas
PJ	:	Poder Judicial
PNP	:	Policía Nacional del Perú
ST	:	Secretaría Técnica del CONAPOC
TIC	:	Tecnologías de la Información y del Conocimiento
UNODC	:	Oficina de las Naciones Unidas contra las Drogas y el Delito

INTRODUCCIÓN

La velocidad con la que se demanda información suele superar a las capacidades con las que se procesan, generan y ofrecen dichos recursos, no obstante, existen importantes alternativas que nos ayudan a reducir el margen de distancia frente a aquellos bordes de la realidad que pretendemos comprender. En ese camino, los intentos por construir información útil y válida a la gestión de las políticas públicas, siempre resultan más pertinentes cuando van acompañados por la articulación, el consenso y el diálogo de perspectivas. Por esta razón, la elaboración de este documento posee un perfil particular, debido a la conjugación de perspectivas provenientes de diferentes instituciones públicas inmersas en la lucha contra los delitos que tienen lugar en (o que se producen mediante) el ciberespacio.

Para iniciar con el abordaje, el documento propone alcances sobre el método y las formas de organizar el proceso de acopio, análisis y redacción de este trabajo multisectorial; reconociendo el valor que le aporta la articulación entre las instituciones participantes, así como también destacan las formas y variaciones que poseen los insumos de datos y de información que se recibieron de parte de cada una de ellas. Este segmento cierra con una mirada por encima al esquema que se propone con el texto, dando relevancia a los objetivos que persigue el diagnóstico en términos de utilidad a la política pública frente a los ciberdelitos.

En un segundo momento, encontramos necesario detenernos a delinear los límites conceptuales que poseen los ciberdelitos y sus principales expresiones. Para ello, repasamos algunos aspectos esenciales elaborados por la academia, pero dando especial énfasis a la delimitación que brinda la legislación peruana.

Luego de este segmento, el siguiente acápite se dedica a reconocer las dimensiones de los ciberdelitos, entendiéndolos como un aspecto de problema público que requiere de una mirada urgente. Para ello desagregamos los elementos más resaltantes, atendiendo a los rasgos que más caracterizan a las víctimas, usuarios y consumidores de tecnologías de comunicación en el espacio virtual. Del mismo modo, complementamos esa perspectiva, ofreciendo información sobre los perpetradores de estos hechos delictivos, ahondando en sus aristas más características; con el objetivo de hacer un posterior balance que facilite la comprensión de los riesgos y amenazas que generan a la seguridad de las sociedades.

Siendo la ciberdelincuencia un problema que demanda de la intervención estatal, es inevitable no mirar hacia la situación en la que se encuentran los servicios e instituciones públicos que se avocan a investigar, prevenir, perseguir y castigar estos actos que contravienen la norma y afectan al bienestar de las y los ciudadanos. En ese sentido, planteamos observar las condiciones de respuesta que posee el Estado frente a los ciberdelitos, empezando por

ver lo avanzado en cuanto a normatividad, para pasar luego a ver el panorama en el que están las instituciones y las acciones emprendidas.

Con esa misma intención, en el siguiente y penúltimo espacio, pretendemos contribuir a la identificación de brechas en la oferta y capacidades que posee el Estado frente a los ciberdelitos, destacando aquellos elementos pendientes de mejora que son necesarios para lograr la articulación entre los esfuerzos de las entidades públicas, así como para asegurar que los recursos a emplearse resulten suficientes y acorde a los requerimientos de intervención de la política pública.

Finalmente, el texto trata de dar por sentadas algunas conclusiones elementales en materia de los ciberdelitos en nuestro país, así como también sugiere un conjunto de recomendaciones sobre acciones que pudieran tomarse en el corto, mediano y largo plazo, en el ámbito de la política criminal, con el propósito de mejorar el combate a este tipo de delitos.

Esperamos, como ya se había señalado, que las páginas que siguen a continuación, constituyan un aporte significativo y de utilidad a las labores que llevan a cabo las diferentes instituciones a cargo de la seguridad en el ciberespacio; tanto como también pueda ser de relevancia para la comunidad en general, en tanto ayudará a contar con más herramientas para la comprensión de estos delitos cada vez más presentes en nuestra cotidianidad.

Capítulo

1 METODOLOGÍA

Con el objetivo de brindar mayores alcances sobre el camino recorrido para dar con el presente diagnóstico, en este segmento nos avocamos a presentar la metodología de trabajo empleada en el proceso; partiendo por los factores que contribuyeron a la decisión de elaborar este documento, hasta la recopilación de la información y el trabajo de análisis de las diversas fuentes ubicadas.

La importancia de generar información articulada sobre la ciberdelincuencia

En el difícil reto que supone llevar adelante las políticas públicas para transformarlas en acciones y/o servicios que generen bienestar en la población de un determinado territorio, existen un conjunto de procesos o momentos intermedios que impactan directamente sobre la calidad de la intervención que se busca realizar, así como de los efectos que puede ocasionar en la vida de las personas. En esa línea, importantes trabajos han señalado en más de una oportunidad, que el manejo adecuado de la evidencia en las políticas públicas constituye un elemento potenciador que contribuye no solo a que se empleen de mejor forma los recursos, sino que también ofrece mayores posibilidades de satisfacer las necesidades de los ciudadanos y ciudadanas (Jaime & Vaca, 2017).

Aplicando ello al campo de la investigación sobre los fenómenos criminales, las necesidades se hacen mucho más urgentes, en tanto la disponibilidad de la información también suma a la evaluación de las acciones implementadas, permitiendo ver si es que, tras la ejecución de las acciones, programas o proyectos, determinados indicadores se vieron trastocados.

En la vista dirigida hacia el contexto que propicia la elaboración de este documento diagnóstico sobre la ciberdelincuencia en nuestro país, encontramos los siguientes tres factores que nos condujeron hacia su formulación:

1. Desde la década de los cincuenta existe una innegable tendencia que impacta de sobremanera a las economías y a las sociedades, con llegada a diversos campos de la investigación y el desarrollo (I+D), tales como la neurotecnología, la conectividad 5G, la analítica avanzada de datos, la inteligencia artificial (IA) y el machine learning, los vehículos autónomos y las Smart cities, entre otros (OECD, 2016). A pesar de ello, sabemos que existe una relación directa entre innovación tecnológica y nuevos delitos cibernéticos que resulta innegable. Esta relación aumenta, aunque no quisiéramos, la vulnerabilidad de los sistemas informáticos sobre los que se soportan buena parte de las actividades que ahora

realizan las personas y las organizaciones, con el objetivo de intercambiar información, almacenar datos, además de adquirir bienes y servicios.

2. El volumen de actividades que se llevan a cabo a través de los medios cibernéticos no se detiene, y muestra cifras gigantescas. A nivel de las transacciones económicas, sabemos que en todo el mundo se pueden llegar a producir hasta 30 billones de tratos económicos, diariamente; sin contar que solo durante el año 2018, en nuestro país se alcanzó a invertir hasta 60 millones de dólares en "tecnologías cloud". Instituciones especializadas en informática señalan que las pérdidas por ciberdelitos, para el año 2022, podrían bordear los 8 trillones de dólares(«Los ciberdelitos más frecuentes en Perú», 2019).

3. Luego de que el Congreso de la República aprobó, en el año 2019, la propuesta del Ejecutivo que buscaba garantizar la adhesión de nuestro país al Convenio contra la Ciberdelincuencia, también conocido como Convenio de Budapest, ingresamos en un nuevo momento que demanda la generación de instrumentos y herramientas que faciliten la labor de las instituciones vinculadas a la prevención, control y castigo de los ciberdelitos; más si tenemos presente que sobre ello existen espacios de información todavía no cubiertos.

Conscientes de estos aspectos, en el marco de las funciones y atribuciones que poseen las instituciones del CONAPOC, se le encargó a la DGAC —a través del Observatorio Nacional de Política Criminal INDAGA— la elaboración de un documento diagnóstico que permitiera aproximarnos hacia la naturaleza y formas que toman los ciberdelitos en nuestro país, así como a una mirada por sobre las capacidades instaladas que posee el Estado para hacerles frente .

Desde esa perspectiva, la Secretaría Técnica del CONAPOC (a cargo de la DGAC) ha impulsado un conjunto de eventos y actividades que faciliten la elaboración de este documento, teniendo en cuenta la necesidad de articular y dialogar con base en la información que cada una de las instituciones involucradas posee en torno a estos delitos específicos. Por esta razón, se da inicio a un Grupo de Trabajo (GT) cuyas reuniones y encuentros han servido de vital importancia, ya que sumaron a la construcción del diagnóstico desde el momento mismo del diseño metodológico, ajustando objetivos y procurando que el mismo posea fines prácticos en favor de la política criminal.

En el camino recorrido, la primera reunión del GT se llevó a cabo el 18 de setiembre de 2019, y contó con la participación de las y los diferentes representantes del CONAPOC, quienes recibieron importantes insumos de orientación por parte de la Dra. Nayelly Loya, de la Oficina de las Naciones

Unidas contra las Drogas y el Delito (UNODC). En esta primera reunión se abordaron conceptos fundamentales sobre el ciberdelito desde una perspectiva comparada a nivel de Latinoamérica.

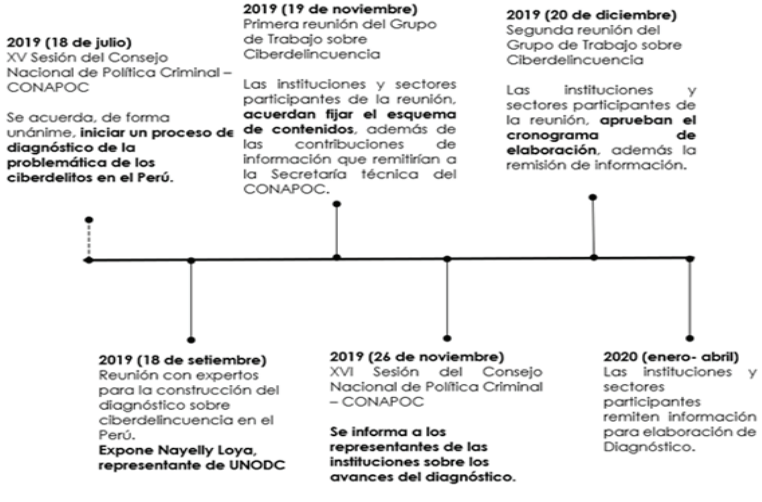
Posteriormente, el 19 de noviembre del mismo año, las instituciones del GT consensuaron importantes aspectos relacionados a la importancia de intercambiar información precisa sobre cómo han venido trabajando de cara a los casos y lassituaciones más recurrentes en cuanto a delitos informáticos o cibernéticos. Del mismo modo, acordaron también un esquema base de contenidos que abordaría el documento diagnóstico, así como los compromisos de remisión de datos y documentación que sume al análisis.

Casi un mes después de dicha reunión, y en el contexto de la XVI Sesión del CONAPOC, convocada por la Presidencia de dicho espacio multisectorial, las y los representantes del GT pudieron conocer sobre los avances obtenidos en cuanto al acopio de los insumos de información fundamentales para el trabajo de análisis y redacción del documento.

Finalmente, el día 20 de diciembre de 2019, convocados formalmente por la ST del CONAPOC, se produjo la última reunión presencial con participación de las y los integrantes del GT. En este encuentro se pudieron plasmar importantes aportes sobre la relevancia de incorporar componentes de metodología y del proceso llevado a cabo para la realización del documento diagnóstico, así como de los compromisos sujetos a la remisión de los insumos de información.

El siguiente gráfico permite visualizar la línea de tiempo trazada a lo largo de este proceso:

Tabla 1: Tipología general de la violencia



Proceso de articulación institucional y de acopio de información para la elaboración del documento diagnóstico

La calidad de la información sobre la ciberdelincuencia

Elaborar un documento diagnóstico sobre un fenómeno tan complejo como el de los delitos cibernéticos o informáticos, requiere de un esfuerzo que incluya diversas perspectivas, tomando en consideración aquellos actores y/o instituciones que se ven afectadas por estos problemas, o de las que intervienen en el desarrollo de acciones que buscan reducir sus efectos en la población que resulte o pueda resultar afectada.

En ese sentido, la elaboración de este trabajo ha involucrado un conjunto de compromisos articulados entre las diversas instituciones que conforman el CONAPOC, entre las que cabe mencionar al Poder Judicial, el Ministerio Público – Fiscalía de la Nación, el Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, la Municipalidad Metropolitana de Lima, el Instituto Nacional de Estadística e Informática , el Consejo Nacional de Seguridad Ciudadana y la Defensoría del Pueblo. Desde la sinergia y el trabajo multisectorial de todos estos actores institucionales es que obtenemos las principales herramientas e insumos que empleó el equipo del Observatorio INDAGA en los diversos momentos que componen el proceso, y entre estas cabe mencionar a las siguientes:

a. De tipo cuantitativa

- Base de datos estadísticas (que brindaban alcances sobre la situación y características de las víctimas, las modalidades y formas más empleadas, etc.)
- Registros de tipo administrativo con información de casos (número de atenciones realizadas, número de intervenciones efectuadas, etc.)

b. De tipo cualitativa

- Mapeo de actores involucrados (instituciones, organizaciones, etc.)
- Balance de normativa vinculada (nacional e internacional)
- Información descriptiva de estado situacional de las instituciones
- Documentación oficial administrativa

Con base en estos elementos recopilados, el trabajo se trasladó hacia el gabinete, empleando una metodología que parte por identificar factores que influyen, directa o indirectamente, en la situación de los ciberdelitos en el Perú (descripción y explicación), para luego abordar los aspectos pendientes y de brechas que necesitan ser reducidas (sintetización). Finalmente, se formulan conclusiones generales, siguiendo la pauta de los datos obtenidos (interpretación), hasta llegar a plantear un conjunto de alternativas (proyección) que permitan mejorar el perfil de las intervenciones que destina el Estado para afrontar los ciberdelitos (Buisan & Marín, 2001).

La redacción de este documento, tomando de referencia esta metodología planteada por Carmen Buisan, se ajusta a un trabajo que "implica una labor de síntesis de toda la información recogida. Supone una destreza. Tiene una función preventiva o correctiva. A menudo esta última es la que queda más subrayada y es la más conocida. El diagnóstico no constituye una finalidad en sí mismo. Sin la proyección de pronóstico pierde su carácter dinámico que le confiere valor" (Ibíd.).

De forma mucho más práctica, podríamos señalar que el proceso metodológico toma la pauta siguiente:

Tabla 2: Tipología general de la violencia

Elaborar un Diagnóstico situacional es un proceso	- Describe - Explica - Sintetiza - Interpreta - Proyecta	Un aspecto determinado de la realidad

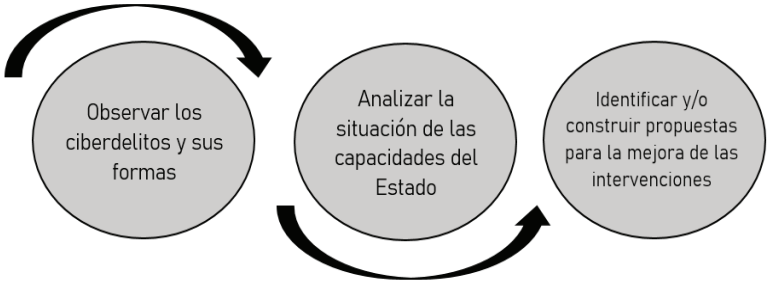
Estructura y componentes para el análisis de la ciberdelincuencia

Elaborar un documento con rigurosidad técnica en cuanto al manejo de la evidencia, no debe de reñirse con su orientación hacia los fines prácticos y/o de pertinencia instrumental; siendo ello un propósito que el presente documento ha buscado realizar desde que fue requerido o planteado como una necesidad por parte de las instituciones que conforman el CONAPOC.

Conservando ese objetivo, nos concentramos en la redacción de un diagnóstico situacional que no implique un esfuerzo redundante en lo reflexivo, teniendo en cuenta además que la academia y otros importantes organismos internacionales también vienen realizando y publicando notables trabajos de divulgación de información constante sobre delitos en el ciberespacio. Empero, con la mira puesta en la necesidad de fortalecer nuestras políticas públicas frente a estos fenómenos criminales, hacemos hincapié en ofrecer alcances sobre la situación en la que se encuentra el Estado de cara a los ciberdelitos. Solo llevando a cabo ese ejercicio, encontramos

mayores oportunidades para formular posteriores herramientas que sumen al robustecimiento de las intervenciones estatales en torno a los ciberdelitos.

Tabla 3: Tipología general de la violencia



Así, los contenidos de este documento se dividen en siete grandes acápites que cumplen con el flujo dinámico de procesamiento de la información señalado líneas arriba. Luego de proponer un abordaje metodológico específico para la elaboración de un diagnóstico situacional, nos trasladamos hacia el repaso sintético del marco normativo y teórico que nos facilita una comprensión esencial de los fenómenos delictivos en el ámbito del ciberespacio, teniendo presente la tipificación y los aspectos que sanciona la legislación en nuestro país.

Posteriormente, damos forma al problema público, apostando por una entrada que dirija la mirada hacia las características que poseen las víctimas de estos ciberdelitos, así como de los actores que se ven involucrados. Tras ello, del balance de la literatura y de los datos recopilados de determinadas fuentes oficiales, intentamos dar rostro a los agentes perpetradores, para pasar posteriormente hacia el reconocimiento de aquellos riesgos y amenazas más significativas.

Superado ese tercer segmento, analizamos la evolución de la normativa nacional y de las oportunidades que le brinda al actuar estatal para perseguir estos delitos; concentrándonos luego en aquellas intervenciones (servicios y acciones) que emplean las instituciones para atender a la problemática.

Una vez reunida esa información, pasamos a buscar y visualizar brechas a nivel de la articulación entre las instituciones encargadas de investigar, perseguir y sancionar estos delitos; así como también analizamos los recursos de los que disponen para llevar adelante esas acciones.

Finalmente, con el panorama casi completo, nos dirigimos hacia la formulación de los aspectos concluyentes más resaltantes, y proponemos un conjunto de acciones que pueden realizarse en el corto, mediano y largo plazo, en cuanto a las capacidades del Estado para hacer frente a los ciberdelitos. Es así que —mediante este trabajo— buscamos enlazar la gestión de la información que supone organizar, evaluar, presentar y comparar grupos de datos; con la gestión del conocimiento que implica un posterior proceso de uso y acciones que potencie el cumplimiento de los objetivos (Ledo & Pérez, 2012).

Capítulo

2 Marco teórico

Aproximaciones al concepto de ciberdelincuencia

La Organización de las Naciones Unidas, define en su "13° Congreso sobre la Prevención del Delito y la Justicia Penal", del mes de abril de 2015, a la ciberdelincuencia como "un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos" . En ese sentido, "los actos comprendidos habitualmente en la categoría de "ciberdelincuencia" son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito"

La ciberdelincuencia, también denominada por algunos autores como "ciberdelito" o "cibercrimen", normalmente se caracteriza por utilizar sistemas informáticos, así como sistemas de comunicación masivos, tales como teléfonos, computadoras, celulares, entre otros, mediante los cuales se cometen diversos delitos o hechos punibles, que dan lugar a la afectación de distintos bienes jurídicos o también denominados derechos fundamentales, tales como el honor, la intimidad, la indemnidad y libertad sexuales, entre otros.

En ese sentido, la criminalidad informática es entendida como el conjunto de "aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es: invasiones a computadoras, correos o sistemas de data mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas mediante tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TIC (Tecnologías de la Información y la Comunicación) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos" (Villavicencio, 2014, p. 286).

Es así que, en diversos países del mundo se han creado legislaciones en base a diversos convenios e instrumentos internacionales para combatir la ciberdelincuencia. Uno de ellos es el denominado "Convenio sobre la Ciberdelincuencia", también conocido como el "Convenio de Budapest", documento que emerge al interior de la Unión Europea, y que incorpora medidas que deberán adaptarse a las legislaciones nacionales de los diversos países miembro, siendo el Perú uno de ellos.

Tabla 4: Tipología general de la violencia

Ciberseguridad y ciberdefensa

Ciberseguridad

Entendida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los datos activos de una organización y de los usuarios de un ciberentorno(UIT, 2010).

Ciberdefensa

Posee una connotación estratégico-militar de defensa nacional, y está asociado al ámbito de las redes y sistemas de información de un Estado o de un conjunto de instituciones estatales; para lo cual se emplean acciones, medios y procedimientos que buscan el uso seguro del ciberespacio (CIBER, 2016).

Ciberdelitos desde la norma en el Perú

Para comenzar a hablar sobre los denominados ciberdelitos o también llamados delitos informáticos, comenzaremos indicando que para que un acto realizado se considere delito, este debe cumplir con el requisito de encontrarse tipificado en la ley penal, estableciéndose una sanción y/o pena correspondiente. Es así que, un ciberdelito o delito informático es "el acto en el cual interviene un sistema de cómputo como utensilio en la producción de un hecho criminológico, en donde se atenta contra los derechos y libertades de los ciudadanos" . De esta definición se puede determinar que un delito informático, además de reunir las características mencionadas en el concepto de "delito", este debe ser cometido utilizando o vulnerando medios informáticos en perjuicio de terceros.

Para construir una definición de cada uno de los delitos informáticos, tomaremos como referencia el "Convenio de Budapest" y la Ley N° 30096 "Ley de delitos informáticos", creada en nuestro país en el año 2013 y modificada por la Ley N° 30171 en el año 2014.

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

- Acceso ilícito

El "Convenio de Budapest" lo define como "el acceso deliberado e ilegítimo a todo o parte de un sistema informático(...) infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva" . Nuestra legislación ha optado por tipificar este delito de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 2.- "El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado"

Este tipo de delito está referido al hecho de ingresar a un sistema informático, infringiendo las medidas de seguridad adoptadas para este, con la intención de conseguir datos informáticos en desmedro del titular del sistema o de terceros. Sin embargo, se puede apreciar que el hecho punible va dirigido al simple hecho de acceder sin autorización al sistema informático, no exigiendo en el tipo el perjuicio del titular de dicho sistema o de terceros.

- **Ataques a la integridad de los datos informáticos**

En el "Convenio de Budapest" estos ataques están referidos a "todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima los datos informáticos" .En nuestra legislación se ha tipificado este delito de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 3.- El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

En el referido tipo penal, se exige una serie de conductas (dañar, introducir, borrar, deteriorar, suprimir, hacer inaccesibles), no exigiendo nuevamente el perjuicio a terceros, sino que simplemente se castiga la realización de dichas conductas para el atentado a la integridad de los datos informáticos.

- **Ataques a la integridad del sistema informático**

El "Convenio de Budapest" lo define como "la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informáticos mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos" . Nuestra legislación tipifica el tipo penal de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 4.- El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

"Para la configuración de este ilícito no basta con cumplir el tipo que es (inutilizar o perturbar), sino además es necesario que la acción vaya seguida de un resultado (impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios). Por tanto, el delito se consuma cuando se impide el acceso, se imposibilita el funcionamiento, etcétera; del sistema informático, caso contrario el hecho solo dará lugar a la tentativa" (Villavicencio, 2014, p. 293).

- **Interceptación de datos informáticos**

El "Convenio de Budapest" lo define como "la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos" . En nuestra legislación encontramos el tipo penal de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 7.- El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

En este tipo penal, lo que se pretende sancionar es el hecho de interceptar los datos, es decir, lo sancionable es la conducta y el solo hecho de realizarla es suficiente para determinar la pena mencionada en el tipo.

- Abuso de mecanismos y dispositivos informáticos

El "Convenio de Budapest" establece que será tipificado como delito:"a. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición decualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de

cualquiera de los delitos [previstos anteriormente]:una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos [previstos anteriormente]; yb. la posesión de alguno de los elementos contemplados en los incisos i) y ii) del apartado a) (...) con intención de que sean utilizados para cometer cualquiera de los delitos previstos [anteriormente]" . Nuestra legislación, ha tipificado el delito de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 10.- El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos. Programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la [Ley N° 30096 Ley de Delitos Informáticos], o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

En el caso peruano, el legislador se adelanta a la comisión de cualquier delito que se encuentre tipificado en la Ley N° 30096 Ley de Delitos Informáticos, puesto que sanciona el solo hecho de fabricar, vender, distribuir, entre otros, programas y/o dispositivos que faciliten la comisión del hecho delictivo. Sin embargo, "hay una interpretación muy amplia(...) por cuanto se extiende a toda gama de delitos previstos en la [ley mencionada anteriormente], y que podría generar problemas en la interpretación judicial, debido a la extensión de ilícitos" (Villavicencio, 2014, p. 299).

Delitos informáticos contra el patrimonio

- **Fraude informático**

El "Convenio de Budapest" establece al fraude informático como "actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona" . En nuestra legislación se ha tipificado del siguiente modo:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 8.- El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático. Será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social".

Al respecto, cabe hacer una diferenciación entre el fraude informático y el fraude convencional, este último también conocido como estafa. Es así que "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" (Gercke, 2014). 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" (Gercke, 2014) que generen perjuicio en el patrimonio de terceros.

Asimismo, este tipo de ciberdelito, tiene la exigencia de generar un perjuicio a terceros, más específicamente, en el patrimonio de terceros.

Delitos informáticos contra la fe pública

- Suplantación de identidad

En nuestra legislación, este delito ha sido tipificado de la siguiente manera:

Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171

Art. 9.- El que, mediante la tecnología de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Al respecto, el ilícito sanciona el resultado, es decir, el prejuicio causado a la víctima, siendo insuficiente la realización de la conducta. Si solo se realiza la conducta (suplantar), no llegándose a ocasionar el perjuicio, este delito quedará como tentativa.

- Delitos contra la indemnidad y libertad sexuales

Respecto a la protección de los bienes jurídicos indemnidad y libertad sexuales, el "Convenio de Budapest" solo se pronuncia ante la posibilidad de tipificar delitos que difundan pornografía infantil a través de medios informáticos. Es así que, el artículo 9° del presente convenio se encuentra redactado de la siguiente forma:

"Será tipificado como delito:la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;la difusión o la transmisión de pornografía infantil a través de un sistema informático;la adquisición, para uno o para otros, de pornografía infantil a través de un sistema informático;la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos" . Sin embargo, lo que debemos tomar en cuenta del artículo mencionado anteriormente es lo que se califica como "pornografía infantil", considerando lo siguiente:Segundo y tercer párrafo del artículo 9° del "Convenio de Budapest":"Se entenderá por 'pornografía infantil' todo material pornográfico que contenga la representación visual de:un menor adoptando un comportamiento sexualmente explícito;una persona que parezca un menor adoptando un comportamiento sexualmente explícito;imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.(...) se entenderá por 'menor' toda persona menor de 18 años".

En nuestra legislación, la Ley N° 30096 "Ley de delitos informáticos" modificada por la Ley N° 30171, sanciona las "proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos". En ese sentido, el artículo 5° de la presente ley sanciona lo siguiente:

Art. 5.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación (...)Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación...

Como se menciona en el título de este apartado, con este ilícito penal lo que se busca proteger es la indemnidad y la libertad sexuales de menores de edad.

El tipo penal sanciona la conducta de contactar con un menor de edad con la intención de obtener de él material pornográfico y/o de conseguir algún otro fin de connotación sexual (violación sexual, tocamientos indebidos, actos contra el pudor, entre otros), es decir, la intención de llevar a cabo actividades sexuales con el menor.

Es importante mencionar que, la intención del perpetrador del delito es clave para la sanción, puesto que el sujeto debe querer perpetrar tales conductas. Sin embargo, a pesar de ello, el tipo sanciona la conducta per se, sin que exista la necesidad de que se llegue a difundir el material pornográfico o que la víctima llegue a encontrarse con el delincuente.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

El artículo 10° del "Convenio de Budapest" exhorta a los Estados miembro a adoptar las medidas necesarias para la protección de este tipo de bienes jurídicos. Es así que, el artículo se encuentra redactado de la siguiente manera:

"1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación (...)".En ese sentido, el Código Penal peruano ha tipificado los delitos contra los derechos de propiedad intelectual en los artículos 216° al 225°, dividiéndolos en dos grupos: delitos contra derechos de autor y conexos, y delitos contra la propiedad industrial.

Al respecto, si bien en dichos artículos no se menciona explícitamente la comisión de tales delitos mediante las TIC, se entiende de manera tácita que ciertos delitos tales como reproducción no autorizada, copia, plagio, entre otros, se pueden realizar utilizando las Tecnologías de la Información y de la Comunicación.

Así también, destacamos la relevancia de incorporar —en el esfuerzo de comprender los ciberdelitos— la propuesta del Grupo de Trabajo de la Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC), en tanto ofrece importantes componentes de análisis de los ciberdelitos.

Desde esta perspectiva, existe la necesidad de entender los ciberdelitos como resultado de una tensión entre conceptos jurídicos y conceptos criminológicos, teniendo en cuenta que existe, además, una importante cifra negra u oculta que impacta también en la posibilidad de establecer elementos probatorios. Desde este espacio, los ciberdelitos generan necesidades de prevención tanto como de reacción.

Capítulo

3 Problema público

La tarea de diseñar y poner en marcha medidas para atender a demandas de una población en un territorio determinado, no es posible de realizar si es que antes no se trascurre por un ejercicio que ayude a esclarecer cuáles son los aspectos que resultan preocupantes, y que a su vez ameriten la intervención de las instituciones del Estado. Esta premisa —como punto de partida— es vital para comprender que cuando hablamos de delitos que ocurren en el ciberespacio, se trata defenómenos que propician la intervención de una autoridad pública para su solución, pues se trata de enfrentar un problema social con una política estatal (Pedroza Estrada, 2018). Así también, y de forma casi inherente a lo mencionado, este ejercicio de problematización implica la minuciosa labor de descomponeren diversas partes inteligibles, las múltiples variables de análisis que guardan relación con el ciberdelito como un "problema público", entendiendo que entre ellas existe una conexión de complejidad que no puede ser pasada por alto, más si se busca tener una visión integral que facilite encontrar soluciones reales (Mballa & López, 2017).

Por esta razón, optamos por formular un diagnóstico sobre la ciberdelincuencia, no sin antes entender que tras el fenómeno persiste un tramado de relaciones que involucra a poblaciones capaces de ser víctimas, tanto como a perpetradores con características o rasgos particulares envueltos todos en un contexto o escenario altamente dinámico, que conlleva riesgos y amenazas a la seguridad; razón por la cual se hace necesaria la participación del Estado.

Entendiendo ello, nos ubicamos entonces ante un contexto histórico y global en el que los ciberdelitos han establecido una clara tensión entre el libre uso/consumo de tecnologías y productos de información, por un lado, y el resguardo de la propiedad y del bienestar de las personas, por el otro. En ese juego de disyuntivas complejas, un sinnúmero de actores (institucionales y no institucionales) vienen emprendiendo importantes estrategias que buscan asegurar un clima propicio para el continuo mejoramiento e innovación de la tecnología, sin que ello implique renunciar a principios elementales como el de la privacidad, el respeto y la libertad de los ciudadanos(Daigle, 2015).

Entonces, nuestra preocupación se enmarca en dos grandes niveles de comprensión del problema público, que suponen en un primer lugar a los actores involucrados (víctimas y perpetradores), y en un segundo lugar a los riesgos y amenazas que pueden ir conjugándose y agravándose si es que no se promueven acciones efectivas; teniendo en cuenta que ellas debieran producirse desde un modelo de intervención respaldado en la evidencia.

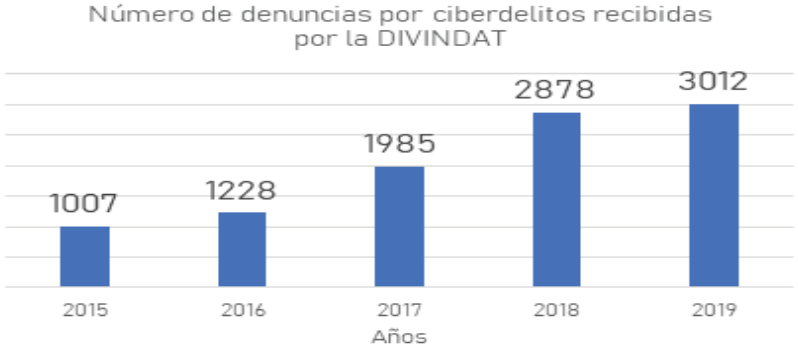
Para el año 2016, el BID señaló que los ciberdelitos generaban costos que llegaban casi a los 575 millones de dólares al año, lo que a su vez representaba cuatro veces el monto total de las donaciones internacionales destinadas a las

políticas de desarrollo en todo el mundo(Observatorio de la Ciberseguridad en América Latina y El Caribe, 2016).

Y como si aquello no fuera suficiente para preocuparnos, la misma institución indicó en el año 2020, que a nivel de la región latinoamericana, solo 7 de los 32 países llegaron a implementar medidas y/o planes de protección de su infraestructura más sensible, aumentando así la vulnerabilidad frente a ataques cibernéticos(Observatorio de la Ciberseguridad en América Latina y El Caribe, 2020).

En el escenario peruano, de acuerdo a las cifras oficiales que maneja la DIVINDAT,las cifras de denuncias por delitos cibernéticos vienen aumentando cada año. De hecho, en cinco años se han atendido 10 110 denuncias correspondientes a delitos informáticos; en un notorio ascenso que alcanza a triplicarse de forma sostenida en el tiempo.

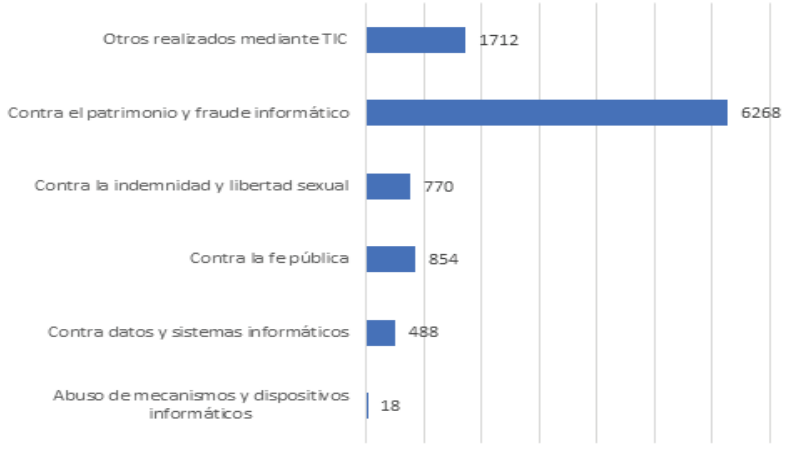
Tabla 5: Tipología general de la violencia



Fuente: Estadística DIVINDAT – DIRINCRI PNP / Elaboración: Observatorio INDAGA

De forma desagregada, tratando de ver el detalle de los tipos de ciberdelitos sobre los que se han formulado denuncias, encontramos que existen algunos de ellos que suelen mantener mayor notoriedad durante los últimos años, siendo ese el caso de los que afectan el patrimonio y/o que inciden en fraude a través de la informática, los cuales ascienden al 62% del total de los ciberdelitos en el Perú.

Tabla 6: Número de denuncias recibidas por la DIVINDAT según tipo de ciberdelito



Fuente: Estadística DIVINDAT – DIRINCRI PNP / Elaboración: Observatorio INDAGA

Complementando con la información con la que también cuenta elMinisterio Público, encontramos durante el último año, que solo los treinta y cuatro distritos fiscales que componen esta institución, han atendido un total de 4636 casos de ciberdelitos; y que, en concordancia con lo señalado por la PNP, también refiere que los casos de daño al patrimonio y fraude informático, tienden a ser los más significativos, con un total de 1788 incidentes, que a su vez representan el 38.6% del total de los delitos. Por otro lado, desde una mirada comparativa a nivel de las regiones de nuestro país, encontramos que existe una mayor regularidad o frecuencia en determinados territorios, entre los que destaca Lima a la cabeza (405 casos), seguido por Lima Este (326 casos) y Lima Norte (272 casos). En todos estos casos, la incidencia supera a regiones como Arequipa (177 casos) o Ica (88 casos) .

Tabla 7: Casos de ciberdelitos atendidos por el Ministerio Público

Delito Subgenérico	Casos	%
Ley N°30096, Ley de Delitos Informáticos	2,420	52.2%
Delitos informáticos contra el patrimonio	1,788	38.6%
Delitos informáticos contra la fe pública	160	3.5%
Delitos contra datos y sistemas informáticos	151	3.3%
Delitos informáticos contra la indemnidad y libertad sexual	67	1.4%
Delitos informáticos contra la intimidad y el secreto de las comunicaciones	31	0.7%
Disposiciones comunes	19	0.4%
Total	4,636	100%

Fuente: SIATF-SGF, Ministerio Público

Casos de ciberdelitos contra el patrimonio atendidos por el Ministerio Público, según distrito fiscal con mayores casos registrados.

Tabla 8: Casos de ciberdelitos contra el patrimonio atendidos por el Ministerio Público, según distrito fiscal con mayores casos registrados

Distrito fiscal	Casos	%
Lima	405	22.7%
Lima Este	326	18.2%
Lima Norte	272	15.2%
Arequipa	177	9.9%
Callao	102	5.7%
Ica	88	4.9%
Lima Sur	64	3.6%
Otros	354	19.8%
Total	1,788	100%

Fuente: SIATF-SGF, Ministerio Público

Cabe mencionar que, aunque cuente con cifras bastante menores, llama la atención la situación de los delitos contra los datos y sistemas informáticos, cuya presencia en la ciudad capital resultó significativa, pues supuso un total de 151 casos atendidos por los distritos fiscales de la ciudad de Lima.

Tabla 9: Casos de delitos contra datos y sistemas informáticos atendidos según distrito fiscal

Distrito fiscal	Casos	%
Lima	23	15.2%
Lima Este	19	12.6%
Callao	11	7.3%
Lima Norte	11	7.3%
Lima Sur	10	6.6%
Lambayeque	9	6.0%
Otros	68	45.0%
Total	151	100%

Fuente: SIATF-SGF, Ministerio Público

Ante este clima preocupante, resulta sumamente oportuno poder delimitar algunos aspectos más significativos y tratar de avanzar en la caracterización de aquellas poblaciones que pueden resultar más vulnerables frente a los ciberdelitos en nuestro país.

¿Quiénes son las víctimas y los perpetradores de la ciberdelincuencia?

Teniendo presente que todavía es escasa la información disponible sobre aquellas poblaciones que resultan ser afectadas por determinado tipo de ciberdelito en nuestro país, es importante generar algunas aproximaciones sobre quienes vienen siendo más vulnerables detrás de las pantallas, tomando en cuenta las fuentes oficiales y de centros de investigación sobre este fenómeno criminal.

Aunque la ONU ofreció una primera entrada formal a la identificación de las vulnerabilidades frente a los ciberdelitos, señalando que el blanco de los delitos se deposita en un sistema o una red informática (Naciones Unidas, 2000), es cierto que aquella resulta insuficiente frente a la actual situación global.

Para el caso de nuestro país, a partir de la información alcanzada por la DIVINDAT, sabemos que puede existir una correlación entre los ciberdelitos que poseen más incidencia y las posibles víctimas más afectadas por estos hechos ilícitos. Tomando en cuenta que para el año 2019, las denuncias sobre los delitos contra el patrimonio y, más específicamente, por fraude informático, llegaron a superar los 2 mil casos, siendo las principales víctimas a aquellas que adquieren bienes y/o servicios mediante canales virtuales. Este último aspecto dialoga también con las fuentes estadísticas oficiales, que señalan que las personas que se encuentran entre los 30 y 44 años de edad, resultan ser las más afectadas por los delitos de fraude bancario, llegando a alcanzar la mayor tasa con un 5.8% , frente a otros grupos de edad que registran porcentajes menores.

Así también, en un segundo plano, encontramos que los delitos de suplantación de identidad y la pornografía infantil, que fluye a través del ciberespacio, llegaron a contar con registros de hasta 247 y 237 casos para cada tipo de delito, respectivamente; razón por la cual podemos encontrar que los niños, niñas y adolescentes, además de las personas que desconocen del manejo y resguardo de sus datos, se encuentran también entre los sectores poblacionales de mayor peligro (Agencia Andina, 2019).

Por otro lado, desde una mirada que asegure involucrar también a quienes brindan y ofertan bienes y servicios, consideramos importante remitirnos a la afectación de las empresas. Según indica el informe de PWC, el 55% del empresariado peruano refiere haber sido víctima de delitos contra su patrimonio y por fraude, entre los cuales destaca el ciberdelito como medio, con un 16%y con pérdidas que van desde 25 mil hasta 1 millón de dólares americanos (PWC, 2018).

De igual forma, al ser consultados por las modalidades o las formas con las que fueron atacados, las empresas declaran el uso de malware como medio, en un 29% de casos, además del phishing, que alcanza hasta un 24%; sin dejar de mencionar el escaneo de red con un 7%. Posteriormente, al ser cuestionados por el perfil que podría tomar el ciberdelincuente detrás de la pantalla, los empresarios peruanos contestaron que en el 75% de las situaciones, se trataría de alguien ubicado al interior de la propia organización, y que en los casos en los que el perpetrador solía ser externo, el 50% de estos se relacionaba a la criminalidad organizada, mientras que solo el 30% podría relacionarse a casos con participación de hackers profesionales (Ibíd).

A modo de síntesis, y tratando de establecer un balance sobre las víctimas de los ciberdelitos y sus perpetradores, es posible trazar un esquema que permita identificar actores, en base a los casos investigados por la DIVINDAT.

Tabla 10:

Tipo de ciberdelito	Actoresidentificados	
	Perfiles del ciberdelincuente	Perfiles de las víctimas
Abuso de mecanismos y dispositivos informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Personas jurídicas.
Contra datos y sistemas informáticos	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Contra la fe pública	▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Empresas.
Contra la indemnidad y libertad sexual	▪ Profesionales de la educación. ▪ Personas con diagnóstico clínico de malestar psicológico. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Niños, niñas y adolescentes vulnerables.
Contra el patrimonio y fraude informático	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.
Otros cometidos mediante el uso de TIC	▪ Profesionales en ingeniería de sistemas e ingeniería electrónica. ▪ Personal técnico en computación. ▪ Personas con alto conocimiento sobre manejo de TIC.	▪ Personas naturales. ▪ Entidades financieras.

Fuente: DIVINDAT – DIRINCRI PNP / Elaboración: DIVINDAT – DIRINCRI PNP

Riesgos y amenazas a la seguridad

Si antes de la llegada del Covid-19, ya existía una gran dependencia de la economía internacional frente a las TIC; con la escalada de la pandemia, que consiguió reorientar gran parte de las actividades cotidianas al campo del ciberespacio, es posible hablar de nexos y puentes mucho más estrechos, a tal punto que, hoy por hoy, nos referimos a los medios virtuales como elementos estructurales de la sociedad contemporánea. Solo para ser mencionado, según el International Data Corporation, el ecosistema digital se estimaba a partir de un total de 20 mil millones de dispositivos conectados a la internet para el año 2025 en todo el mundo (IDC, 2019).

Un primer gran riesgo asociado a la criminalidad cibernética, guarda relación con el tratado y gestión de los grandes cúmulos de información y datos personales que se encuentran atravesando la red, y que ahora han cobrado mayor notoriedad, luego de que la pandemia haya impulsado enormemente el intercambio, los aprendizajes y el entretenimiento a través de las pantallas. Sin el debido protagonismo del Estado, este es un campo de latente riesgo frente a los ciberdelitos.

Por otro lado, si bien existen personas condenadas por delitos informáticos en nuestro país, los casos no alcanzan siquiera a corresponderse con la cantidad de denuncias que se realizan ante las autoridades competentes. De acuerdo al PJ, durante los últimos cinco años, se ha conseguido dar sentencia condenatoria por delitos informáticos a un total de 397 personas en el Perú. Esta cifra nos alerta sobre la débil cooperación y articulación entre las instituciones públicas y privadas, durante todos los momentos de lucha contra la cibercriminalidad, desde la prevención y la sanción a sus perpetradores, tanto como las acciones preventivas y de estímulos a la confianza, con el propósito de mejorar las cifras de denuncias ante estos hechos. De forma adicional, cabe encender las alertas por uno de los aspectos más destacados cuando se aborda la temática de los ciberdelitos y de su impacto: las brechas de cobertura y las asimetrías que ocasionan desigualdad en el uso de las TIC; entendiendo que alrededor de éstas existen dos grandes niveles de afectación, siendo el primero el de los ciudadanos usuarios, y el segundo el de las empresas que organizan sus procesos mediante estas tecnologías, las que a su vez pueden encontrar más dificultades debido a la reorientación de los gastos por la crisis.

En cuanto a las poblaciones que puedan resultar más vulnerables, aunque las detenciones e imputaciones por ciberdelitos que afectan a menores de edad, no supera el 7.1% del total de casos a nivel mundial (Montiel Juan, 2016), todavía sigue preocupando que buena parte de los esfuerzos institucionales de los Estados no se hayan dirigido a hacer más presencia preventiva y de sensibilización en espacios característicos, como los dedicados al entretenimiento por plataformas de videos y de videojuegos.

Capítulo

4 RESPUESTA DEL ESTADO

Los avances y las oportunidades para la normatividad: una aproximación comparada

A continuación, se presenta un análisis comparado del marco normativo en relación a la ciberdelincuencia de quince (15) países , los mismos que fueron analizados a partir de cuatro grandes variables, estas son: i) delito, ii) norma, iii) pena, y iv) agravantes.

Los resultados advierten grandes oportunidades de mejora en la dimensión normativa del Estado peruano, los mismos que serán detallados en la sección de recomendaciones.

Tabla 11:

PAÍS	Perú	Argentina	Alemania	Francia	Australia	Sudáfrica	Gran Bretaña
DELITO	Acceso Ilícito	Acceso Ilícito	Acceso Ilícito	Acceso Ilícito	Acceso no autorizado o modificación de datos restringidos	Acceso no autorizado para interceptar e interferir con datos	Acceso no autorizado a material computacional
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 2°. -**El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo (...).[1]	**Art. 153 bis Código Penal argentino:** (...) el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.[2]	**Ley Contra la Criminalidad Económica: Art. 202a Código Penal Alemán:** (1)Quien sin autorización se procure para sí o para otro, datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado. (2) Datos en el sentido del inciso 1, son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible.[3]	**Ley N° 88-19 Ley sobre Fraude Informático: Art. 462-2.-** Cualquier persona que haya accedido fraudulentamente o permanezca en todo o en parte a un sistema automatizado de procesamiento de datos (...).[4]	**Ley del Cibercrimen: Art. 478.1.-** Una persona es culpable de un delito si: (a) causa cualquier acceso no autorizado, o modificación de datos restringidos; (b) tiene la intención de causar el acceso o la modificación: (c) sabe que el acceso o modificación no es autorizado (...).[5]	Capítulo XIII Ley de Transacciones y Comunicaciones Electrónicas: (1) Una persona que intencionalmente accede o intercepte cualquier dato sin autorización o permiso para hacerlo, es culpable de un delito...[28]	Capítulo 18 Ley de Usos Incorrectos de Computadoras: Una persona es culpable de un delito si (a) Causa que un ordenador realice cualquier función con la intención de garantizar el acceso a cualquier programa o datos contenido en cualquier ordenador; (b) el acceso pretendido no está autorizado...[29]
PENA	De uno (1) a cuatro (4) años y con treinta a noventa días-multa.	De quince (15) días a seis (6) meses.	Hasta tres (3) años o con multa.	De dos (2) meses a un (1) año y una multa.	Dos (2) años de prisión efectiva.	Hasta cinco (5) años de prisión efectiva.	Pena de multa.
AGRAVANTES		La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.		Cuando esto resulta en la eliminación o modificación de los datos contenidos en el sistema, o en una alteración del funcionamiento de este sistema, la pena será de dos (2) meses a dos (2) años y una multa.			

Tabla 11:

PAÍS	Perú	Argentina	Alemania	Francia	Australia	Sudáfrica	Gran Bretaña
DELITO	Acceso Ilícito	Acceso Ilícito	Acceso Ilícito	Acceso Ilícito	Acceso no autorizado o modificación de datos restringidos	Acceso no autorizado para interceptar e interferir con datos	Acceso no autorizado a material computacional
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 2°. -**El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo (...).[1]	**Art. 153 bis Código Penal argentino:** (...) el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.[2]	**Ley Contra la Criminalidad Económica: Art. 202a Código Penal Alemán:** (1)Quien sin autorización se procure para sí o para otro, datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado. (2) Datos en el sentido del inciso 1, son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible.[3]	**Ley N° 88-19 Ley sobre Fraude Informático: Art. 462-2.-** Cualquier persona que haya accedido fraudulentamente o permanezca en todo o en parte a un sistema automatizado de procesamiento de datos (...).[4]	**Ley del Cibercrimen: Art. 478.1.-** Una persona es culpable de un delito si: (a) causa cualquier acceso no autorizado, o modificación de datos restringidos; (b) tiene la intención de causar el acceso o la modificación: (c) sabe que el acceso o modificación no es autorizado (...).[5]	Capítulo XIII Ley de Transacciones y Comunicaciones Electrónicas: (1) Una persona que intencionalmente accede o intercepte cualquier dato sin autorización o permiso para hacerlo, es culpable de un delito...[28]	Capítulo 18 Ley de Usos Incorrectos de Computadoras: Una persona es culpable de un delito si (a) Causa que un ordenador realice cualquier función con la intención de garantizar el acceso a cualquier programa o datos contenido en cualquier ordenador; (b) el acceso pretendido no está autorizado...[29]
PENA	De uno (1) a cuatro (4) años y con treinta a noventa días-multa.	De quince (15) días a seis (6) meses.	Hasta tres (3) años o con multa.	De dos (2) meses a un (1) año y una multa.	Dos (2) años de prisión efectiva.	Hasta cinco (5) años de prisión efectiva.	Pena de multa.
AGRAVANTES		La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.		Cuando esto resulta en la eliminación o modificación de los datos contenidos en el sistema, o en una alteración del funcionamiento de este sistema, la pena será de dos (2) meses a dos (2) años y una multa.			

Tabla 12:

PAÍS	Perú	Colombia	Honduras	Argentina	España	Australia	Alemania
DELITO	Interceptación de datos informáticos	Interceptación de datos informáticos	Interceptación ilícita	Interceptación ilícita	Interceptación ilícita	Posesión o control de datos con la intención de cometer un delito	[Interceptación de datos informáticos]
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos:** El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos (...).[1]	**Ley de Protección de la Información y de los Datos. Art. 269C Código Penal colombiano:**El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte (...).[2]	**Art. 214° Código Penal hondureño:** Quien, sin la debida autorización judicial, con cualquier propósito, se apoderare de los papeles o correspondencia de otro, intercepta o hace interceptar sus comunicaciones telefónicas, telegráficas, soportes electrónicos o computadoras, facsimilares o de cualquier otra naturaleza, incluyendo las electrónicas (...).[3]	**Art. 153° Código Penal argentino:** (...) el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.	**Art. 197.2 Código Penal español:** El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte **transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos** (...).[4]	Ley del Cibercrimen: Art. 478.3.- Una persona es culpable de un delito si: (a) tiene la posesión o el control de datos; (b) tiene la posesión o el control con la intención de utilizar los datos, por sí mismo o por otra persona en: (i) la comisión de un delito o (ii) facilitar la comisión de un delito[36].	Ley Contra la Criminalidad Económica: Art. 202b Código Penal Alemán: Quien ilegalmente intercepte datos no destinados para él por medios técnicos de instalación de procesamiento de datos privada o de la emisión electromagnética de una instalación de procesamiento de datos...[35]
PENA	De tres (3) a seis (6) años.	De tres (3) a seis (6) años.	De seis (6) a ocho (8) años.	De quince (15) días a seis (6) meses.	De tres (3) a doce (12) meses.	De tres (3) años de prisión efectiva.	Hasta dos (2) años de prisión efectiva o con multa.
AGRAVANTES	-La pena privativa de libertad será no menor de cinco (5) ni mayor de ocho (8) años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial (...). -Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.		De ocho (8) a doce (12) años si se tratase de funcionario o empleado público.	-La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. -Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena.			

Tabla 13:

PAÍS	Perú	Colombia	Francia	Alemania	México
DELITO	Ataque a la integridad de datos informáticos	Daño Informático	Ataque a la Integridad de Datos Informáticos	Alteración de datos [informáticos]	Alteración de datos informáticos
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 3.-** El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos (...).[1]	**Ley de Protección de la Información y de los Datos. Art. 269D Código Penal colombiano:** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos (...).[2]	**Ley N° 88-19 Ley sobre Fraude Informático: Art. 462-3.-**Cualquier persona que, intencionalmente y sin tener en cuenta los derechos de otros, directa o indirectamente, ingrese datos en un sistema de procesamiento automatizado o elimine o modifique los datos que contiene (...).	**Ley Contra la Criminalidad Económica: Art. 303a Código Penal alemán:** Quien borre, suprima, inutilice, o cambie antijurídicamente datos [informáticos] (...).[3]	**Art. 211 bis 1 Código Penal Federal:** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad (...).[4]
PENA	De tres (3) a seis (6) años y con ochenta a ciento veinte días-multa.	De cuatro (4) a ocho (8) años y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.	De tres (3) meses a tres (3) años y con multa.	Hasta dos (2) años o multa.	De seis (6) meses a dos (2) años y de cien a trescientos días-multa
AGRAVANTES					**Art. 211 bis 2 Código Penal Federal:** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán

Tabla 14:

PAÍS	India	Australia	Sudáfrica	Gran Bretaña
DELITO	Manipulación de documentos informáticos	Modificación no autorizada de datos para causar deterioro	Ataque a la integridad de datos informáticos	Modificación no autorizada de material computacional
NORMATIVA	**Ley de Tecnología de la Información: Art. 65° Código Penal:** El que a sabiendas o intencionalmente, oculte, destruya o altere o intencionalmente o con conocimiento provoque que otra persona oculte, destruya o altere cualquier código fuente utilizado en una computadora, programa informático, sistema informático o red informática, cuando el código fuente se requiere se guarde o mantenga por ley...[1]	**Ley del Cibercrimen: Art. 477.2.-** Una persona es culpable de un delito si: (a) la persona causa cualquier modificación no autorizada de datos contenidos en una computadora: (b) la persona conoce que la modificación no es autorizada: (c) la persona es imprudente acerca de si la modificación perjudico o perjudicara (...).[2]	**Capítulo XIII Ley de Transacciones y Comunicaciones Electrónicas: (2)** Una persona que intencionalmente y sin autorización para hacerlo, interfiera con datos de una manera que cause que dichos datos sean modificados, destruidos o de alguna manera los haga ineficaces, es culpable de un delito.[3]	**Capítulo 18 Ley de Usos Incorrectos de Computadoras:** Una persona es culpable de un delito si (a) realiza cualquier acción que cause una modificación no autorizada al contenido de cualquier computadora, y (b) en el momento de realizado el acto tiene la intención y el conocimiento.[4]
PENA	Hasta tres (3) años de pena privativa de libertad y pena de multa.	Diez (10) años de prisión efectiva.	Hasta cinco (5) años de prisión efectiva.	
AGRAVANTES				

PAÍS	Perú	Colombia	República de Panamá	España	India
DELITO	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Penalización por daños a computadoras y sistemas informáticos
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 4.-** El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios (...).[5]	**Ley de Protección de la Información y de los Datos. Art. 269B Código Penal colombiano:** El que, sin estar facultado para ello, impida u obstaculice el	**Ley 53/07 contra el delito cibernético: Art. 11.-** El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, liar o destruir un sistema electrónico, informático, telemático o de	**Art. 264.2 Código Penal español: (**1) Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o	**Ley de Tecnología de la Información: Art. 43° Código Penal:** Si una persona sin el permiso del propietario o de cualquier otra persona encargada del sistema informático o red informática, (a) ingresa o garantiza el acceso al equipo, sistema informático o una red informática; (b)

Tabla 15:

PAÍS	India	Australia	Sudáfrica	Gran Bretaña
DELITO	Manipulación de documentos informáticos	Modificación no autorizada de datos para causar deterioro	Ataque a la integridad de datos informáticos	Modificación no autorizada de material computacional
NORMATIVA	**Ley de Tecnología de la Información: Art. 65° Código Penal:** El que a sabiendas o intencionalmente, oculte, destruya o altere o intencionalmente o con conocimiento provoque que otra persona oculte, destruya o altere cualquier código fuente utilizado en una computadora, programa informático, sistema informático o red informática, cuando el código fuente se requiere se guarde o mantenga por ley...[1]	**Ley del Cibercrimen: Art. 477.2.-** Una persona es culpable de un delito si: (a) la persona causa cualquier modificación no autorizada de datos contenidos en una computadora: (b) la persona conoce que la modificación no es autorizada: (c) la persona es imprudente acerca de si la modificación perjudico o perjudicara (...).[2]	**Capítulo XIII Ley de Transacciones y Comunicaciones Electrónicas: (2)** Una persona que intencionalmente y sin autorización para hacerlo, interfiera con datos de una manera que cause que dichos datos sean modificados, destruidos o de alguna manera los haga ineficaces, es culpable de un delito.[3]	**Capítulo 18 Ley de Usos Incorrectos de Computadoras:** Una persona es culpable de un delito si (a) realiza cualquier acción que cause una modificación no autorizada al contenido de cualquier computadora, y (b) en el momento de realizado el acto tiene la intención y el conocimiento.[4]
PENA	Hasta tres (3) años de pena privativa de libertad y pena de multa.	Diez (10) años de prisión efectiva.	Hasta cinco (5) años de prisión efectiva.	
AGRAVANTES				

PAÍS	Perú	Colombia	República de Panamá	España	India
DELITO	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Ataques a la Integridad de Sistemas Informáticos	Penalización por daños a computadoras y sistemas informáticos
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 4.-** El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios (...).[5]	**Ley de Protección de la Información y de los Datos. Art. 269B Código Penal colombiano:** El que, sin estar facultado para ello, impida u obstaculice el	**Ley 53/07 contra el delito cibernético: Art. 11.-** El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, liar o destruir un sistema electrónico, informático, telemático o de	**Art. 264.2 Código Penal español: (1)** Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o	**Ley de Tecnología de la Información: Art. 43° Código Penal:** Si una persona sin el permiso del propietario o de cualquier otra persona encargada del sistema informático o red informática, (a) ingresa o garantiza el acceso al equipo, sistema informático o una red informática; (b)

Tabla 16:

PAÍS	Perú	Argentina	Colombia	España	Sudáfrica
DELITO	Abuso de Mecanismos y Dispositivos informáticos	Abuso de Mecanismos y Dispositivos informáticos	Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas	Abuso de Mecanismos y Dispositivos informáticos	Abuso de Mecanismos y Dispositivos informáticos
NORMATIVA	**Ley N° 30096 Ley de Delitos Informáticos: Art. 10.–** El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos. Programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la [Ley N° 30096 Ley de Delitos Informáticos], o el que ofrece o presta servicio que contribuya a ese propósito (...).[1]	**Art. 183° Código Penal argentino 2do párrafo:** (...) el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado en el artículo 10° de la Ley N° 26.388, B.O. 25/6/2008)[2]	**Art. 193° Código Penal colombiano:** El que, sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas (...). (Ley N° 599 del año 2000)[3]	**Art. 400° Código Penal español:** La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores (...) (Se refiere a todos los delitos descritos en el Código Penal)[4]	**Capítulo XIII Ley de Transacciones y Comunicaciones Electrónicas: (3)** Una persona que ilegalmente produzca, venda, ofrezca para la venta, adquiere para su uso, diseños, adapte para su utilización, distribuya o posea cualquier dispositivo, incluido un programa de computación o un componente, diseñado principalmente para superar las medidas de seguridad para la protección de datos, o realice cualquiera de esos actos con relación a una contraseña, código de acceso o cualquier otro tipo similar de datos similares con la intención de utilizarlos ilegalmente, es culpable de un delito.[5]
PENA	De uno (1) a cuatro (4) años y con treinta a noventa días multa.	De quince (15) días a un (1) año.	Pena de multa.	Se castigarán con la pena señalada en cada caso para los autores.[6]	Hasta cinco (5) años de prisión efectiva.
AGRAVANTES					

Tabla 17:

PAÍS	Perú	Colombia	Guatemala	Alemania	España	Japón
DELITO	Fraude informático	Transferencia no consentida de activos	Fraude informático	Fraude informático	Estafa informática	Fraude informático
NORMATIVA	Ley N° 30096 Ley de Delitos informáticos: Art. 8.- El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.	Art. 69K Ley N° 1273 de 2009: El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave (...).	Art. 274E Código Penal: (...)al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.	Ley Contra la Criminalidad Económica: Art. 263a Código Penal alemán: Quien, con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso (...).	Art. 248° Código Penal español: (1) Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, aduciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. (2) También se considera reos de estafa: a) los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro; b) los que fabricaren, introdujeren, poseyeren o faciliten programas informáticos, específicamente destinados a la comisión de estafas previstas en este artículo (...)".	Ley de Acceso Computarizado y Acta de Crimen Computacional: Art. 246-2 Código Penal: (...)persona que haya obtenido o cause que otra obtenga un beneficio mediante la creación de un registro electromagnético falso relativo a la adquisición, pérdida o alteración de los derechos de propiedad al introducir datos falsos o dar comandos no autorizados a un equipo utilizado para negocios de otra persona, o por poner un falso registro electromagnético relativo a la adquisición, pérdida o alteración de los derechos de propiedad en el uso de la administración de los asuntos de otro...
PENA	De tres (3) a ocho (8) años y con sesenta a ciento veinte días-multa.	De cuatro (4) a diez (10) años y con multa de 200 a 1500 salarios mínimos legales mensuales vigentes.	De uno (1) a cinco (5) años y multa de quinientos a tres mil quetzales.	De cinco (5) años o con multa.	De un (1) año a seis (6) años y multa de seis a doce meses.	Hasta diez (10) años de pena privativa de libertad y trabajos forzados.
AGRAVANTES	La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.			Art. 263 inc. 3 Código Penal alemán: En casos especialmente graves, el castigo será de pena privativa de la libertad de uno hasta diez años: 1. actúe profesionalmente o como miembro de una banda que se ha asociado para la comisión continuada de falsificación de documentos o estafa, 2. ocasione una pérdida patrimonial de grandes dimensiones o actúe con el propósito de conducir a un gran número de personas al peligro de la pérdida de activos mediante la comisión continuada de estafa, 3. conduzca a una persona a necesidad económica, 4. abuse de sus competencias, de su posición como titular de cargo (...).		

Tabla 18:

PAÍS	Perú	Colombia	Guatemala	Alemania	España
DELITO	Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Pornografía infantil	Pornografía infantil	Pornografía infantil	Publicación de información obscena en forma electrónica
NORMATIVA	Ley N° 30096 Ley de Delitos informáticos: Art. 5.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación (...) Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación...	Art. 128° Código Penal argentino: (...) el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. -Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. -Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.	Art. 149C Código Penal hondureño: Comete el delito de pornografía, quien por cualquier medio sea directo, mecánico o con soporte informático, electrónico o de otro tipo financie, produzca, reproduzca, distribuya, importe, exporte, ofrezca, comercialice o difunda material donde se utilice la persona e imagen de personas menores de dieciocho (18) años de edad en acciones o actividades pornográficas o eróticas (...). -La tenencia de material pornográfico de niños, niñas y adolescentes será sancionado con pena de cuatro (4) a seis (6) años de reclusión.	Art. 241a Ley N° 8069, del 13 de julio de 1990, modificada por la ley N° 10.764 del 12 de noviembre de 2003: Ofrecer, intercambiar, poner a disposición, transmitir, distribuir, publicar, o difundir por cualquier medio, incluso a través de una computadora o sistema telemático, fotografías, videos u otro registro que contenga escenas de sexo explícitas o pornografía que involucre a un niño o adolescente.	Ley de Tecnología de la Información: Art. 67° Código Penal: Cualquiera que publique o transmita o cause que se publique en formato electrónico, cualquier material lascivo o que apele a interés lascivo o si su efecto es tal que tienda a pervertir y corromper a las personas que puedan, teniendo en cuenta todas las circunstancias pertinentes, leer, ver o escuchar el tema contenido o consagrados en ella (...).
PENA	-Menor de catorce años: De cuatro (4) a ocho (8) años e inhabilitación. -De catorce a diecisiete años: De tres (3) a seis (6) años e inhabilitación.	De seis (6) meses a cuatro (4) años.	De diez (10) a quince (15) años de reclusión y multa de doscientos (200) a trescientos (300) salarios mínimos.	De tres (3) a seis (6) años y multa.	-Si es su primera condena: Hasta cinco (5) años de pena privativa de libertad y pena de multa. -En el caso de una segunda o subsecuente: Hasta diez (10) años de pena privativa de libertad y con pena de multa.
AGRAVANTES					La comisión del delito de dos a más veces es agrava la pena.

Instituciones y servicios desde el Estado peruano

La conectividad a internet acelera el crecimiento económico y crea oportunidades para los negocios y el comercio; sin embargo, estas oportunidades siempre traen consigo riesgos, principalmente porque las tecnologías de internet están en constante evolución, debilidad que los delincuentes pueden explotar fácilmente. Por esta razón, la maximización del valor del Internet y el ciberespacio debe ser una parte central de la planeación gubernamental (BID & OEA, 2016).

Existe un desequilibrio entre el tiempo de comercialización de innovaciones tecnológicas y el "tiempo de seguridad", a pesar de ser una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto. La pandemia de la COVID-19 y el incremento de la actividad digital que ha generado en la región, ha dejado aún más en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe (BID & OEA, 2020). Diversos informes identifican a América Latina como un foco para el ciberdelito no tan solo por su potencial mercado sino también por los niveles de informalidad y desconocimiento.

El hecho de que en el Perú aún se tenga menos de un 50% de conectividad a internet, demuestra un mercado grande de nuevos usuarios que no tienen la experticia necesaria para mediar con ataques cibernéticos. Diariamente se registra un aumento de las ciber amenazas, además de una globalización de la ciberdelincuencia, ya que esta traspasa fronteras nacionales. Por lo que las acciones para enfrentar la amenaza deben basarse en la cooperación.

El Perú se encuentra suscrito al convenio de Budapest desde el 2019, mecanismo de cooperación entre los estados miembros del Consejo de Europa y las demás economías firmantes o suscriptoras, que tienen como finalidad proteger a la sociedad frente a la ciberdelincuencia particularmente mediante la adopción de una legislación adecuada, la capacitación y la mejora de la cooperación internacional. Además del Convenio Iberoamericano de Cooperación sobre Investigación Aseguramiento y Obtención de prueba en materia de Ciberdelincuencia del cual es parte desde el 2014 .

Los datos recogidos por la OEA y el BID mediante el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) del 2020, en comparación al del 2016, muestra que en el eje de Política y Estrategia de Seguridad Cibernética no ha habido muchos avances, los únicos puntos de mejora fueron el modo de operación para la respuesta de incidentes, manejo de la crisis, organización de la defensa cibernética y comunicaciones. En el

eje de Cultura Cibernética y Sociedad se observa mejoras en la comprensión de los usuarios de la protección de la información en línea. En el eje de Estándares, Organizaciones y Tecnologías, se observa mejoras en la calidad de softwares, controles técnicos de seguridad, controles criptográficos y seguro cibernético en el mercado de seguridad cibernética. Por último, uno de los ejes con más avances ha sido el eje de Marcos Legales y regulatorios, con la incorporación de marco legal para la protección de datos, protección infantil en línea, protección del consumidor y propiedad intelectual. Además, se registra mejoras en los marcos de cooperación formales e informes para combatir el delito cibernético, prueba de ello el proyecto "Mejoramiento y Ampliación de los servicios de soporte para la Provisión de los Servicios a los Ciudadanos y las Empresas a Nivel Nacional", financiado mediante el Contrato de Préstamo BID Nº 4399/OC-PE que busca dentro de sus objetivos fortalecer la ciberseguridad nacional.

Entre las instituciones estatales que vienen desarrollando acciones en materia de control y persecución de los ciberdelitos, se encuentra la Policía Nacional del Perú que desde el 2005 crea la División de Investigación de delitos de alta tecnología (DIVINDAT) para atender de forma exclusiva los delitos cibernéticos. Por su parte, aunque todavía no contamos con fiscalías y juzgados penales avocados especialmente al tratado de ciberdelitos, sí destacamos la creación de una Fiscalía Especializada en Ciberdelincuencia, trabajo que viene siendo desarrollado por una comisión especial del Ministerio Público, mediante Resolución FN N°1025-2020-MP-FN-UCJE, de fecha 18 de setiembre de 2020.

Por otro lado, entre las instituciones dedicadas a la prevención, se destaca a la Secretaría de Gobierno Digital que viene trabajando en la Estrategias de Co-Diseño para la Política y Estrategia Nacional de Transformación Digital con la colaboración del sector público, privado, sociedad civil, academia y los ciudadanos para impulsar la transformación digital del país.

Asimismo, la Coordinadora de respuesta a emergencia en redes teleinformáticas de la administración pública del Perú (PECERT), cuya misión es coordinar la prevención, el tratamiento y la respuesta a incidentes de seguridad cibernética de instituciones del sector público, así como elaborar estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado. Se encuentra a cargo de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y es miembro del Equipo de Respuesta ante Emergencias Informáticas (CSIRT).

Tabla 19:

Sector	Institución	Acciones
Interior	División de Investigación de delitos de alta tecnología (DIVINDAT) - PNP	Investigación de delitos cibernéticos.
Ministerio Público	Fiscalías penales y mixtas	Investigación de delitos cibernéticos.
Poder Judicial	Juzgados penales y mixtos	Sanción a casos de delitos cibernéticos
Presidencia del Consejo de Ministros	Secretaría de Gobierno Digital	Lidera los procesos de innovación tecnológica y de transformación digital del Estado. Es el ente rector del Sistema Nacional de Transformación Digital y administra las Plataformas Digitales del Estado Peruano.
Presidencia del Consejo de Ministros	Oficina Nacional de Gobierno Electrónico eInformática (ONGEI)	Encargado de dirigir como ente rector, el Sistema Nacional de Informática y de implementar la Política Nacional de Gobierno Electrónico e Informática.
Presidencia del Consejo de Ministros	Coordinadora de respuesta a emergencia en redes teleinformáticas de la administración pública del Perú (PECERT) - Presidencia del Consejo de Ministros	Encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los Ciberdesafíos y coordinar la defensa ante los Ciberataques, con el fin de proveer a la Nación de una postura Segura en el Ámbito de la Seguridad Digital.

Tabla 20:

Acciones en el mundo

La Unión Internacional de Telecomunicaciones (UIT), con la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) constituyeron la primera iniciativa de cooperación a nivel global que divulga conocimientos y recursos sobre ciberseguridad para que los Estados Miembros interesados puedan detectar, analizar y responder eficazmente a las ciberamenazas .

El Foro Económico Mundial (WEF), lanza cada año el reporte de riesgo global, donde cada año se reporta que los 5 riesgos más altos en el mundo están relacionados con la ciberseguridad. Por lo que crea la plataforma "ShapingthefutureofCybersecurity and Digital Trust" que busca a través de la acción colaborativa y la asociación de la red público-privada, Foro de líderes de las empresas, el gobierno, la sociedad civil, el mundo académico y los mejores expertos, promover un futuro digital seguro y próspero para todos

Iniciativas del sector privado

El sector privado ofrece alternativas tecnológicas para contrarrestar los cibedelitos, siendo un caso emblemático el de IBM Security, quienes desarrollaron la plataforma Watson como su primera plataforma cognitiva, capaz de detectar amenazas cibernéticas y brindar recomendaciones para detenerlas.

Por otro lado, destaca la multinacional Microsoft con el Índice de Civilidad Digital (ICD) que mide, en una escala de 0 a 100, la relación de la exposición al riesgo entre la cortesía en línea. Los datos del 2019 revelan que. a nivel global, la exposición de riesgos on line aumentó significativamente, registrando los siguientes 5 principales riesgos: contacto no deseado, engaños/fraude/estafas, sexting no deseado, trato de manera mezquina y trolling. Al interior de dicho registro se encuentra el Perú, país que muestra uno de los índices más bajo de civilidad (81%), mientras los países vecinos obtuvieron un puntaje de 76% (Argentina), 72% (Brasil), 75% (Chile) y 75% (México) .

Capítulo

5 BRECHAS DE LA OFERTA INSTITUCIONAL

Necesidades identificadas en torno a la articulación

En el presente acápite realizaremos una exposición de las necesidades detectadas acerca de los aspectos de articulación y trabajo interinstitucional entre las entidades públicas, así como en el sector privado, respecto a la prevención, control y persecución de los ciberdelitos.

En ese sentido la PNP, a través de la DIVINDAT, tiene como una de sus funciones principales la de ejecutar el análisis informático forense de equipos de cómputo, telefonía móvil y otros equipos electrónicos con capacidad de almacenamiento de información, inmersos en la comisión de delitos informáticos y delitos conexos. Ello lo realiza mediante el uso de hardware y software forense especializado.

Al respecto, se ha podido detectar que existen solo (02) dos dependencias policiales dentro de esta división, una que se encuentra en Lima y otra en la región Arequipa. Es así que hay una evidente brecha en cuanto a la capacidad de persecución de estos delitos, puesto que no se cuenta con la cantidad necesaria de dependencias que puedan asistir a quienes son víctimas de los ciberdelitos.

En ese orden de ideas, se ha obtenido información que indica la necesidad de afianzar capacidades y conocimientos al interior de las fiscalías y juzgados, respecto de los delitos informáticos. Si bien son las fiscalías las dependencias que trabajan de cara a los delitos comunes, es importante incorporar componentes de este otro tipo de delitos; y teniendo presente la necesidad de articular en esa labor a la PNP, tanto como al Poder Judicial, por ser quienes participan de la persecución de los delitos cibernéticos. Existen posiciones que reiteran en la necesidad de la creación de Fiscalías Especializadas y Juzgados Especializados en delitos informáticos que a su vez cuenten con sistemas de información integrados.

En cuanto al sector privado, existen deficientes mecanismos por parte de las empresas privadas proveedoras de servicios para mantener registros de la titularidad de sus clientes en cuanto a las asignaciones de las direcciones IP, así como demora para remitir información vinculada a datos registrados en sus sistemas informáticos. Además de ello, para el proceso de entrega y recopilación de información por parte de los actores del sector privado hacia las entidades públicas, se deben seguir procesos, tales como el Levantamiento del Secreto de las Comunicaciones o Levantamiento del Secreto Bancario, procesos que solo se pueden realizar mediante la expedición de una Resolución Judicial, que lleva un tiempo determinado para ser expedida, el cual muchas veces impide que la persecución de los ciberdelitos sea más eficaz.

Finalmente, y no por ello menos importante, es esencial afianzar acciones de sensibilización, con una alianza entre las instituciones públicas y privadas que también incida en la formación y la capacitación de profesionales en distintas disciplinas, a fin de promover actitudes de prevención y de denuncia ante los ciberdelitos; teniendo en cuenta que la no denuncia se ha convertido en una característica todavía persistente alrededor de estos fenómenos criminales.

Necesidades identificadas en torno a los recursos

Cuando hablamos de este tipo de necesidades, identificaremos aquellas referidas a los recursos normativos, recursos de capital humano y recursos logísticos necesarios para la prevención, control y persecución de los ciberdelitos.

En cuanto a los recursos normativos, nos encontramos suscritos desde el año 2019 al Convenio de Budapest el cual indica las directrices que deben seguir los países miembros para incorporar a su legislación los recursos normativos necesarios para combatir la ciberdelincuencia. Además de ello, tenemos la Ley N° 30096 modificada por la Ley N° 30171 Ley de Delitos Informáticos, la cual se ciñe al Convenio de Budapest y persigue los delitos explicados en el Convenio.

También se cuenta con una serie de recursos normativos, tales como la Ley N° 30999 Ley de Ciberdefensa y la Ley N° 29733 Ley de Protección de Datos Personales. Sin embargo, a pesar de toda la normativa mencionada anteriormente, lo que estamos necesitando es la incorporación a nuestra legislación de leyes y convenios que regulen y/o faciliten el acceso a la información de forma oportuna para que las autoridades encargadas de la persecución de estos delitos, puedan manejar con mayor celeridad y efectividad dicha persecución. En ese sentido, aunque existen importantes avances en cuanto a la normatividad que brinda el marco legal frente a los ciberdelitos, sigue siendo un asunto pendiente establecer, a partir de ello, una estrategia clara a nivel nacional que brinde claras pautas de acción a nivel de las instituciones y organizaciones involucradas.

Si hablamos de los recursos de capital humano, se identificó que las escuelas de formación de oficiales de la Policía Nacional del Perú no cuentan con recursos relacionados a la investigación sobre delitos informáticos. Sin embargo, se viene desarrollando una capacitación continua con cursos especializados en la investigación de Delitos Informáticos en el marco del Código Procesal Penal a cargo de la Escuela de Investigación Criminal.

Asimismo, actualmente la División de Investigación de Delitos de Alta Tecnología – DIVINDAT tiene asignado un aproximado de ciento cincuenta (150) efectivos policiales en Lima y un total aproximado de veintitrés (23)

efectivos en la región Arequipa, de los cuales solo setenta (70) de ellos se encuentran capacitados en los cursos relacionados a la investigación de delitos informáticos. Ello resultaría ser insuficiente dada las circunstancias y la coyuntura actual.

En ese sentido, se ha podido detectar la falta de intercambio permanente entre entidades nacionales e internacionales para la capacitación de personal especializado en los ciberdelitos. Asimismo, hay deficiencias en cuanto al Equipo de Respuesta ante Emergencias Informáticas (CSIRT), ello por la misma falta de capacitación necesaria para su fortalecimiento.

Respecto a las fiscalías, se pudo identificar la carencia de un cuerpo especializado de peritos informáticos en el Ministerio Público que brinden apoyo a las diversas fiscalías a nivel nacional, ya que, si bien hay una pequeña cantidad de ellos, estos laboran exclusivamente para el Equipo Especial de Fiscales – Odebrecht. Además, existe una falta de capacitación a los fiscales a nivel nacional respecto a la injerencia de las Tecnologías de la Información y la Comunicación (TICs) en la comisión de delitos informáticos, así como en temas de cooperación judicial internacional respecto al requerimiento de conservación de datos informáticos.

Es necesario precisar que en la dotación de personal, además de considerar a las fiscalías, también se debe considerar personal necesario para la Unidad de Cooperación Judicial y Extradiciones de la Fiscalía de la Nación, toda vez que en su calidad de Autoridad Central y como parte de la Red 24/7 del Convenio de Budapest, es la que tramitará los requerimientos de asistencia judicial internacional activos a fin de solicitar informaciones de los servidores de Facebook, WhatsApp, Instagram o de otros servidores como Apple, los cuales vienen siendo tramitados ya por esta Unidad en base a la Convención Interamericana sobre Asistencia Mutua en Materia Penal.

En cuanto a los recursos logísticos, se ha detectado la falta de software especializado y de última generación, así como de herramientas informáticas forenses para las investigaciones y pericias informáticas. Asimismo, no hay convenios suficientes con empresas nacionales o internacionales en el ámbito tecnológico que puedan proveer al Estado de los recursos mencionados anteriormente.

También hay una necesidad de mejorar la infraestructura de las áreas de trabajo y de implementar manuales estandarizados de cooperación internacional para formular pedidos de asistencia judicial a países extranjeros que cuenten con proveedores de servicios que se encargan de diversas plataformas, tales como Facebook, WhatsApp, Instagram, Twitter, entre otros.

Asimismo, resulta necesario dotar de presupuesto suficiente a fin de potenciar un laboratorio forense con personal especializado en la materia (peritos) y con los equipos tecnológicos necesarios para que puedan ampliar su campo de acción hacia las Fiscalías Provinciales a nivel nacional.

Finalmente, existe una cultura insuficiente para prevenir las acciones de la cibercriminalidad, debido a la falta de difusión en todos los niveles y por medios de comunicación masiva de las principales modalidades delictivas y formas de prevención de los ciberdelitos.

Tabla 21: Cuadro de identificación de brechas estatales frente a los ciberdelitos en el Perú

CAPACIDADES REQUERIDAS	CAPACIDADES REQUERIDAS
Capacidades de articulación	Necesidades en cuanto a la articulación
CONAPOC: Acuerdo del Consejo (XV Sesión) que impulsa la creación de un diagnóstico sobre ciberdelitos en el país, con participación interinstitucional e intersectorial. Autoridad Nacional de Protección de Datos Personales: Que permite trazar una estrategia frente al manejo de bancos de datos personales en el país.	Espacio de articulación público-privado para el intercambio de información y el fortalecimiento de capacidades en servidores públicos, en materia de ciberdelitos. Estrategia de coordinación interinstitucional (PNP, MP-FN, PJ) para la triangulación de información y coordinación en materia de lucha contra los ciberdelitos. Agenda interinstitucional de investigación cualitativapara contar con mayores insumos sobre los ciberdelitos, sus formas y dinámicas.
Capacidades de recursos	Necesidades en cuanto a recursos
•Marco normativo: Convenio de Budapest aprobado Vigencia de la Ley de Delitos Informáticos, Ley de Protección de Datos Personales y Ley de Ciberdefensa. •Recursos humanos: División policial especializada (DIVINDAT), presente en 02 regiones con un total de 173 efectivos (solo 70 capacitados). Unidad de Cooperación Judicial y Extradiciones de la Fiscalía de la Nación, para la asistencia técnica judicial internacional en materia de solicitud de información a prestadores de servicios de telecomunicaciones (Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de pruebas en materia de Ciberdelincuencia). Unidad PeCert (PCM), especializada en la prevención y defensa ante ciberataques, en el marco de la seguridad digital del Estado peruano.	•Marco normativo: Adecuación de la normativa nacional sobre ciberdelitos frente al Convenio de Budapest. Creación de normativa que acelere la entrega de información a las instituciones competentes en la investigación de ciberdelitos. •Recursos humanos: Aumentar la cantidad de efectivos especializados (DIVINDAT), a fin de asegurar la investigación y persecución de los ciberdelitos en todas las regiones del país. Aumentar la cantidad de servidores del MP-FN con conocimientos y acceso a logística y laboratorios que fortalezcan la investigación y atención a casos sobre ciberdelitos. •Recursos de información: Registro unificado de libre acceso para la consulta sobre la situación de casos de ciberdelitos denunciados y atendidos a nivel nacional. Indicadores y data estadística oficial para el monitoreo constante del desempeño de las políticas destinadas a la lucha contra los ciberdelitos. Documentación de reporte periódico sobre los ciberdelitos y sus formas, con participación de los observatorios especializados en la criminalidad y seguridad ciudadana.

Capítulo

6 Conclusiones

1. Aunque la elaboración de este diagnóstico cobra especial relevancia, en tanto se elaboró gracias a la especial articulación y sinergia entre diversas instituciones vinculadas a la Política Criminal, también es cierto que, debido a esta misma oportunidad de generar una mirada conjunta, es que encontramos importantes vacíos por cubrir en torno a la gestión de la información sobre los ciberdelitos. Estas diferencias operativas sobre el manejo de la información ante los ciberdelitos, existente entre las entidades policiales, los fiscales a cargo de los expedientes de investigación, y el poder judicial; dificultan profundamente las acciones preventivas tanto como las persecutorias y de sanción; razón por la cual se hace más necesario orientar los esfuerzos para hacer interoperable el intercambio de datos sobre la ciberseguridad.

2. El repaso por los principales datos y estadísticas que posee el ciberdelito —bajo todas sus formas y expresiones— posee múltiples posibilidades de lectura, sin embargo, el equipo técnico desea llamar la atención que este tipo de fenómenos delictivos, cada vez más recurrentes, no encuentren desde el Estado una oportunidad para ser vistos como hechos criminales trasversales a otras actividades penadas por la ley, dimensionados en sus formas por la falta de información.

3. La normatividad generada para hacer frente a los ciberdelitos en nuestro país, si bien ha conseguido abrirse paso a pesar de ciertas dificultades, tales como la demora en la aprobación del Convenio de Budapest; también encuentra mayores retos para una agenda de puntos pendientes, entre los que destaca la colaboración y la cooperación regional que se hace necesaria entre los países para contrarrestar el avance de la criminalidad organizada que encuentra en los medios y espacios informáticos, un campo infinito de ocasiones para seguir generando daños.

4. Si bien tenemos implementada normativa específica referida a la ciberdelincuencia, tales como la Ley N° 30096 Ley de Delitos Informáticos o la Ley N° 30999 Ley de Ciberdefensa, además de encontrarnos dentro del Convenio de Budapest como país miembro; tenemos todavía un camino importante por recorrer para el mejoramiento de dicha normativa, tomando en consideración la incorporación de diferentes componentes vinculados al análisis de conductas enmarcadas en la delincuencia informática.

5. La incidencia de los ciberdelitos mantiene un innegable crecimiento que se hace notar en la evolución de los datos correspondientes a los registros de denuncias y casos que son tratados por las entidades policiales y de fiscales, principalmente. En esa misma línea, la notable presencia de los ciberdelitos relacionados a la estafa y el fraude informático hacen suficiente eco como para pensar en adecuar las capacidades del Estado frente a los delitos patrimoniales, con el objetivo de que sean incluidas perspectivas y enfoques que prioricen en el análisis de medios y espacios tecnológico-computacionales empleados, a fin de conseguir mejores resultados, especialmente en el ámbito preventivo.

6. A la par de los delitos contra el patrimonio, potenciados o concretados con apoyo de la tecnología de las comunicaciones y de la información, también encontramos que la pornografía con menores, el ciberacoso o la ciberextorsión también han cobrado mayor notoriedad; involucrando y afectando a poblaciones que poseen mayores dificultades para defenderse y resguardarse ante estas formas criminales.

7. Si bien existe un mayor avance en cuanto a la aplicación de medidas y protocolos de protección y de prevención ante los ciberdelitos, por parte de las grandes empresas y entidades bancarias del sector privado; es importante no dejar de ver o atender a aquellos actores menores al interior de este grupo, tales como los micro y pequeños empresarios, quienes no solo se ven afectados por las brechas de accesibilidad a la tecnología y a la información, sino que también suelen contar con menos capacidades financieras y de conocimiento para blindarse ante amenazas cibernéticas, poniendo en riesgo así a sus emprendimientos, más aún si tenemos en cuenta el actual contexto de lenta recuperación económica y de fragilidad de las iniciativas empresariales a pequeña escala.

8. Diferentes actores del Estado tales como la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, entre otros, se encuentran realizando esfuerzos para la prevención, persecución y control de los ciberdelitos en el Perú. En ese sentido, es importante que su labor se encuentre acompañada de los recursos necesarios para el combate de este tipo de delitos, ya que nos enfrentamos a tipos penales que utilizan tecnología especializada y muy avanzada para la comisión de las conductas punibles.

9. Diversas organizaciones internacionales, tales como la Organización de las Naciones Unidas o el Banco Interamericano de Desarrollo, han realizado diagnósticos situacionales de la ciberdelincuencia alrededor de mundo, incluyendo al Perú en sus estudios y exteriorizando los problemas y brechas que aún nos quedan por subsanar, sobre todo en la atención a recursos y cooperación entre los diversos actores involucrados.

10. La ciberdelincuencia lidera la agenda mundial, no solo por su riesgo asociado y su potencial impacto negativo en el PBI de los países, sino también porque reconfigura los actos delictivos que traspasan las fronteras territoriales con gran facilidad y velocidad.El Perú forma parte de los acuerdos mundiales para contrarrestar la Ciberdelincuencia y ha avanzado considerablemente en la legislación asociada, sin embargo, aún carece de herramientas de gestión que le permitan articular efectivamente los esfuerzos del sector público y privado.

Capítulo

7 Recomendaciones

Generación e integración de información útil y oportuna

1. Elaborar un conjunto de indicadores estandarizados para la medición y seguimiento de los ciberdelitos, considerando las recomendaciones internacionales de UNODC, en el marco de la Iniciativa para la Encuesta de Victimización Delictiva en Latinoamérica y el Caribe (VICLAC), tomando en cuenta las Encuestas y otras fuentes existentes, y la necesidad de ejecutar en el país la Encuesta Nacional Especializada sobre Victimización de manera continua en apoyo a las políticas públicas de los sectores involucrados.

2. Elaborar un documento que reporte —de forma semestral— data oportuna y confiable sobre la situación de la ciberdelincuencia en el Perú; involucrando en su elaboración a las siguientes instituciones: Observatorio de la Criminalidad del Ministerio Público, Observatorio del delito y la Criminalidad la Policía Nacional del Perú, Observatorio de Seguridad Ciudadana del Ministerio del Interior, bajo la coordinación del Observatorio Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos.

3. Incorporar una sección dedicada al análisis de la ciberdelincuencia en el Sistema Integrado de Estadísticas de la Criminalidad y de la Seguridad Ciudadana (DATACRIM). Esta sección debería contar con un interfaz amigable y de fácil acceso a funcionarios y servidores públicos, quienes pudieran consultar, a través de un único registro estandarizado, la data estadística oficial sobre los ciberdelitos en nuestro país.

4. Construir una agenda de investigaciones cualitativas que pudieran realizarse en el plazo más inmediato posible, y que a su vez nos permitan contar con mayores detalles sobre el perfil de los perpetradores de los ciberdelitos y de sus víctimas en nuestro país. Estos esfuerzos de investigación científica deben incorporar miradas sobre sus motivaciones, dinámicas de mercado, oferta y demanda, además de contar con una perspectiva trasversal de territorialidad que nos facilite la comprensión de la cibercriminalidad en cada región.

Herramientas normativas para reducir la ciberdelincuencia

5. Plantear en nuestra normativa en los delitos como los de acceso ilícito, ataques a la integridad de datos informáticos y/o ataques a la integridad de sistemas informáticos, que están referidos a delitos contra la

confidencialidad de los datos y sistemas informáticos, que se incorpore no solo a sistemas o datos que se encuentran protegidos, ya sea mediante algún sistema de cifrado o cualquier otro tipo de protección, sino que debe incluirse también a datos o sistemas que no necesariamente hayan incorporado medidas de seguridad, pero que contengan información valiosa para el sujeto pasivo del ilícito.

6. Revisar, y luego de ello, evaluar la posibilidad de aprobación de la Ley de Ciberseguridad. En ese sentido, es pertinente que se tome en cuenta lo dispuesto por el Ejecutivo sobre la redacción de los diferentes artículos de la norma, así como las competencias para la asignación de presupuestos y la creación de un Comité de Ciberseguridad. Asimismo, es importante mencionar que los diversos actores estatales deben considerarse dentro de la norma, en vista de que se trata de un problema público que aqueja a toda la sociedad peruana en su conjunto.

7. Implementar una normativa que regule y simplifique el acceso a la información a las autoridades correspondientes, con el objetivo de agilizar los procesos de investigación cada vez que se trate de casos que involucren ciberdelitos. Esta normativa debe considerar la entrega inmediata de información de las diversas entidades del sector público y privado a las instituciones competentes, como una expresión de compromiso público-privado frente a la cibercriminalidad. Del mismo modo, es importante contar con mejores protocolos de facilitación de información que consolidan las diferentes instituciones y/o sectores involucradas en el tratamiento al fenómeno de la ciberdelincuencia, teniendo en cuenta la necesidad de usar estos recursos de manera responsable y oportuna a las acciones de persecución.

Cooperación internacional y nacional

8. Fomentar la cooperación entre los diferentes organismos del Estado, es decir, los reglamentos de diversas instituciones tales como las de la Administración Tributaria o los de la Administración Aduanera, deben contener las medidas necesarias de protección de sus datos y sistemas informáticos, incorporando a su propia normativa supuestos referidos a la comisión de los diversos delitos informáticos que pueden ser cometidos. Esto puede agregarse, por ejemplo, en las disposiciones complementarias de las normas emitidas.

9. Realizar acciones de intercambio de información y de adecuación normativa entre países de la región, teniendo en cuenta a aquellos que hayan suscrito el Convenido de Budapest. Estas formas de cooperación regional fortalecerán el desempeño de las entidades dedicadas a

la prevención e investigación de los ciberdelitos en nuestro país, y particularmente las áreas de cooperación internacional de la Policía Nacional y del Ministerio Público, quienes, con sus pares en otros países pueden conseguir importantes elementos que impulsen procesos de adecuación de los marcos legales sobre la ciberdelincuencia, más allá de las singularidades sancionadoras de cada país, a fin de reducir los márgenes de escape de la justicia que poseen las organizaciones criminales cuando se mueven en el ciberespacio, aprovechando las diferencias de legislaciones entre los Estados.

10. Crear una estrategia de coordinación integrada entre los diversos actores encargados de la persecución y el control de los ciberdelitos, con énfasis en la PNP, el Ministerio Público y el Poder Judicial. Esta estrategia debería asegurar que las instituciones puedan triangular información útil a la coordinación de posteriores acciones que pretenden prevenir y perseguir a las organizaciones criminales que se encuentran detrás de los hechos ilícitos en el ciberespacio, evitando así la duplicidad y confusión durante el trabajo operativo. Dicha acción de estrategia de coordinación puede informar al Consejo Nacional de Política Criminal – CONAPOC los resultados e impactos que ha tenido el trabajo en termino de detenciones, investigaciones, casos resueltos y sentencias. De igual manera es importante contar con mayores instrumentos de cooperación y articulación con los órganos de gobierno local, en tanto son estos los que brindan el primer acercamiento al ciudadano en situaciones de riesgo.

Diagnóstico de necesidades y fortalecimiento de capacidades

11. Se recomienda elaborar un (1) Diagnóstico de Necesidades y un (1) Plan de Capacitaciones dirigido a operadores del sistema de justicia y seguridad, en especial a: i) policía, ii) fiscalía, iii) jueces, y iv) defensores públicos, con el objetivo de incorporar componentes de análisis de los ciberdelitos en sus enfoques de trabajo, teniendo en cuenta que el este fenómeno criminal se vincula también a la dinámica de otros fenómenos criminales ya tipificados, y sobre los cuales incluso existen ya grandes avances. Esto puede generar mejores resultados que la ampliación o creación de nuevas instituciones, áreas o dependencias estatales específicas en el campo de la persecución, investigación y sanción a los ciberdelitos.

12. En cuanto a recursos humanos, es necesario destacar que se requiere mayor personal calificado en las unidades especializadas. De este modo,

se requiere que, en la escuela de formación de oficiales y suboficiales de la Policía Nacional del Perú, se incorpore el contenido de "Investigación de Delitos informáticos" y "Ciberdelincuencia" en los cursos que se estime necesario y pertinente.

13. Asimismo, se requiere fortalecer el intercambio de experiencias y conocimientos entre entidades nacionales e internacionales para personal especializado que trabaja en acciones vinculadas contra los ciberdelitos. Por lo que se considera pertinente tener funcionarios especialistas que lleven formación en de primer nivel en el extranjero.

14. En general, los fiscales requieren herramientas de utilidad para el análisis de la injerencia de las Tecnologías de la Información y la Comunicación (TICs) en la comisión de delitos informáticos.

15. Desarrollar acciones de educación en ciberseguridad con énfasis en riesgo por la ciberdelincuencia, a fin de promover actitudes de prevención y de denuncia ante los ciberdelitos; teniendo en cuenta que la no denuncia se ha convertido en una característica todavía persistente alrededor de estos fenómenos criminales. Al respecto, destacamos la importancia de incluir a los gobiernos locales, entendiendo que a través de estos es posible trasversalizar un conjunto de componentes de prevención y sensibilización frente a la ciberdelincuencia y sus riesgos.

Recursos humanos para enfrentar los ciberdelitos

16. En relación al número de personal, es necesario indicar que se cuenta con aproximadamente ciento cincuenta (150) efectivos policiales en Lima y un total aproximado de veintitrés (23) efectivos en la región Arequipa dedicados a la División de Investigación de Delitos de Alta Tecnología – DIVINDAT, el cual resulta insuficiente al requerido dada la coyuntura pandemia que aceleró las dinámicas en el mundo virtual, y según se advirtió, serán irreversibles. En ese sentido, es fundamental contar con más personal especializado para el tratamiento de los ciberdelitos, más allá de las dependencias policiales. Estos perfiles también deberían encontrarse en entidades tales como el Poder Judicial y el Ministerio Público.

17. Asimismo, se considera necesario el incremento del equipo de la Unidad de Cooperación Judicial y Extradiciones de la Fiscalía de la Nación, el mismo que tramita los requerimientos de asistencia judicial internacional activos

en el marco de la Convención Interamericana sobre Asistencia Mutua en Materia Penal. Dicho documento ha sido invocado, de forma previa al Convenio de Budapest, como herramienta para los requerimientos de información a los Estados Unidos de América, antes de diciembre de 2019.

Instrumentos para combatir los ciberdelitos

18. Se recomienda evaluar la necesidad de implementar manuales estandarizados de cooperación internacional para formular pedidos de asistencia judicial a países extranjeros que cuenten con proveedores de servicios que se encargan de diversas plataformas, tales como Facebook, WhatsApp, Instagram, Twitter, entre otros.

19. Se considera necesario elaborar un (1) informe técnico, por cada institución competente, que permita evidenciar las fortalezas y debilidades de la necesidad de la creación de Fiscalías Especializadas y Juzgados Especializados en delitos informáticos, considerando la experiencia internacional y la realidad peruana.

Infraestructura y presupuesto

20. Resulta necesario dotar de presupuesto suficiente a fin de potenciar un laboratorio forense con personal especializado en la materia (peritos) y con los equipos tecnológicos necesarios para que puedan ampliar su campo de acción hacia las Fiscalías Provinciales a nivel nacional.

21. Evaluar la necesidad de ampliar las dependencias policiales de la DIVINDAT en otras regiones del Perú (fuera de Lima y Arequipa), a fin de ejecutar el análisis informático forense de equipos de cómputo, telefonía móvil y otros equipos electrónicos con capacidad de almacenamiento de información, inmersos en la comisión de delitos informáticos y delitos conexos en estas otras regiones.

22. Elaborar el Plan Anual Interinstitucional 2021-2022 para ejecutar las recomendaciones en orden de prioridad y que permita progresivamente la formulación y puesta en marcha de las políticas públicas contra la ciberdelincuencia.

Capítulo

BIBLIOGRAFÍA

Agencia Andina. (2019, enero 16). Estos son los delitos informáticos más frecuentes en el Perú, según la Policía. https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

Buisan, & Marín. (2001). Cómo realizar un Diagnóstico Pedagógico. Alfa Omega.

CIBER, E. (2016, marzo). Operaciones Militares en el Ciebrespacio. Informe Mensual de Ciberseguridad, 12, 24.

Daigle, L. (2015). Onthenatureofthe internet (N.o 7; Global Commissionon internet governancepaper series, p. 28). CIGI. https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf

IDC. (2019). TheGrowth in ConnectedIoTDevicesIsExpectedtoGenerate 79.4ZB of Data in 2025, Accordingto a New IDC Forecast. IDC: The premier global marketintelligencecompany. https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Jaime, F., & Vaca, P. (2017, agosto). Las políticas basadas en la evidencia como plataformas para la innovación de políticas públicas. Estado abierto, 2(1), 51-76.

Ledo, M. J. V., & Pérez, A. B. A. (2012). Gestión de la información y el conocimiento. Revista Cubana de Educación Médica Superior, 11.

Los ciberdelitos más frecuentes en Perú. (2019). Universia. https://orientacion.universia.edu.pe/infodetail/orientacion/consejos-tecnoversia/los-ciberdelitos-mas-frecuentes-en-peru-4849.html

Mballa, L. V., & López, C. G. (2017). La complejidad de los problemas públicos: Institucionalización de las situaciones problemáticas y anterioridad de la solución a la acción pública. 26.

Montiel Juan, I. (2016, junio). Cibercriminalidad social juvenil: La cifra negra. Revista de internet, derecho y política, 22, 13.

Naciones Unidas. (2000). Delitos relacionados con las redes informáticas: Documento de antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas. 18.

Observatorio de la Ciberseguridad en América Latina y El Caribe. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? (p.

193). Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Observatorio de la Ciberseguridad en América Latina y El Caribe. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y El Caribe. (p. 204). Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

OECD. (2016). OECD Science, Technology and Innovation Outlook 2016. OECD. https://doi.org/10.1787/sti_in_outlook-2016-en

Pedroza Estrada, A. Y. (2018). Los problemas públicos como factor estructural de las políticas públicas. RFCE, 20, 124. https://doi.org/10.30972/rfce.0203258

PWC. (2018). Encuesta Global sobre Delitos Económicos y Fraude 2018 (p. 16). PWC. https://www.pwc.pe/es/publicaciones/assets/brochures/GECS2018_2.pdf

UIT. (2010, noviembre). Ciberseguridad: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilziación de las tecnologías de la información y la comunicación. Actualidades de la UIT, 9, 3.

ISBN: 978-612-4225-39-0