Priorización : una política y herramienta para enfrentar la delincuencia informática -cibercriminalidad- en Colombia

Luis Jairo Bernal Cifuentes

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

PRIORIZACIÓN: UNA POLÍTICA Y HERRAMIENTA PARA ENFRENTAR LA DELINCUENCIA INFORMÁTICA -CIBERCRIMINALIDAD- EN COLOMBIA

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

PRIORIZACIÓN: UNA POLÍTICA Y HERRAMIENTA PARA ENFRENTAR LA DELINCUENCIA INFORMÁTICA -CIBERCRIMINALIDAD- EN COLOMBIA

ALUMNO: LUIS JAIRO BERNAL CIFUENTES

DIRECTOR: EDWIN ORLANDO CAMACHO

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

Nota de aceptación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Nota obtenida: _____

Bogotá, D. C., ... de enero de 2020

A Dios, gracias por siempre.

A mí madre, fallecida 17/AGO/2019.

¡A todos!, su tiempo fue mi tiempo!

¡Amis amigos mas cercanos, que estuvieron siempre ahí!

Al personal de profesores y administrativos de ESDEGUE.

Agradecimientos

Al Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia, a la Escuela Superior de Guerra - ESDEGUE- del Ministerio de Defensa Nacional, pues gracias a su apoyo he podido realizar y culminar con éxito este proceso académico. De la misma manera, un reconocimiento a la Fiscalía General de la Nación, pues el cocimiento y experiencia que me ha dado durante veinticinco años, me han servido de base para la estructuración de este proyecto e implementación gradual del mismo.

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

Resumen

En el marco de la globalización instaurada mediante las tecnologías de la información y la comunicación (TIC's) emergen delitos informáticos que desafían a las instituciones gubernamentales encargadas de determinar responsabilidades civiles, administrativas y penales. Así las cosas, trataremos de resolver la pregunta de investigación cualitativa ¿En qué consistiría una metodología de priorización para la investigación de cibercriminalidad dentro de la Fiscalía General? En este contexto la cibercriminalidad comprende un conjunto de crímenes de naturaleza transnacional que puede involucrar ordenamientos jurídicos internacionales y nacionales, incluso contradictoriamente. En este sentido, afrontarla institucionalmente disciplinaria, judicial y penalmente -implica registrar los incidentes informáticos y diseñar e implementar instrumentos conceptuales y metodológicos investigativos y judiciales-, eficientes contra este crimen de escala nacional y transnacional. Este artículo propone y desarrolla la pertinencia de una política y la propuesta de una herramienta metodológica de investigación criminal diseñada para la Fiscalía General de la Nación (FGN) en Colombia, teniendo en cuenta la priorización, como un mecanismo que permite abordar ciertos desafíos sociales, políticos y judiciales que plantea la cibercriminalidad. El primer capítulo define la cibercriminalidad y los desafíos que plantea a los marcos legales, nacionales e internacionales; el segundo capítulo define la priorización y desarrolla su pertinencia investigativa en términos políticos, sociales y judiciales; el tercer capítulo, aborda la propuesta de una herramienta metodológica de priorización para las investigaciones contra la cibercriminalidad que atentan contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos. Así las cosas, se propone la

creación de una Mesa Técnica contra la Cibercriminalidad -**MTCC**-. Finalizando encontraremos algunos mapas de calor por departamentos, donde se observará el número de denuncias recibidas por la Fiscalía General de la Nación, por delitos informáticos para los periodos 2016, 2017, 2018 y desde enero a julio de 2019, nombrando los Top 5 por año. A partir de lo anterior nos permite concluir, la importancia de la implementación de la herramienta metodológica de priorización para la investigación de cibercriminalidad dentro de la Fiscalía General de la Nación, en pro de abordar civil, administrativa y penalmente la cibercriminalidad mediante marcos conceptuales y metodológicos que comprendan su naturaleza sociohistórica y de este modo sus posibles y diversos tipos de manifestación.

Palabras Clave: *delito informático*, *instituciones políticas*, *derecho internacional*, *administración de justicia, investigación cualitativa*

Abstract

In the context of globalization established through information and communication technologies (ICTs), IT crimes emerge that challenge government institutions responsible for determining civil, administrative and Criminal. Thus, we will try to solve the qualitative investigation question What would be a prioritization methodology for the investigation of cybercriminality within the Attorney General's Office? In this context, cybercriminality comprises a set of crimes of a transnational nature that may involve international and national legal systems, even contradictoryly. In this sense, confronting it institutionally, judicially and criminally - involves recording computer incidents and designing and implementing conceptual and methodological tools - investigative and judicial - efficient against this crime nationally and transnationally. This article proposes and develops the relevance of a policy and the proposal of a methodological criminal investigation tool designed by the Attorney General's Office (FGN) in Colombia, taking into account prioritization, as a mechanism that allows address certain social, political and judicial challenges posed by cybercriminality. The first chapter defines cybercriminality and the challenges it poses to legal, national and international frameworks; the second chapter defines prioritization and develops its investigative relevance in political, social and judicial terms; the third chapter addresses the proposal for a methodological tool of prioritization for cybercriminality investigations that violate the confidentiality, integrity and availability of data and computer systems. Thus, it is proposed to create a technical table against Cybercrime -MTCC-. Completing we will find some heat maps per department in front of the number of complaints of computer crimes for the periods 2016, 2017, 2018 and from January to July 2019, received by the Attorney

General's Office, naming the Top 5 per year. And, in conclusion, the importance of implementing the methodological prioritization tool for cybercriminality investigation within the Attorney General's Office is highlighted, in order to address civil, administrative and criminal cybercriminality through conceptual and methodological frameworks that understand its sociohistorical nature and thus its possible and various types of manifestation.

Keywords: *Computer crime, political institutions, international law, administration of justice, qualitative research*

Introducción

Frente a los delitos que han emergido con la consolidación y convergencia[1] global de las tecnologías de la información y la comunicación (TIC's) como medios de producción e intercambio de distintos bienes y servicios, se han formulado diversas iniciativas y estrategias regulativas y normativas a nivel internacional (Consejo de Europa de la Unión Europea. la Comunidad de Estados Independientes o la Organización de Cooperación de Shanghai, las Organizaciones Intergubernamentales Africanas, la Liga de los Estados Árabes y las Naciones Unidas) y nacional (CONPES 3701, 2011; CONPES 3854, 2016). No obstante, tanto estas iniciativas como las distintas investigaciones adelantadas por organizaciones de seguridad digital recomiendan fortalecer las políticas, metodologías y conceptos de investigación criminal como mecanismos legítimos que permitan afrontar los desafíos sociales, políticos y judiciales que plantean los delitos informáticos no solo a nivel nacional, sino también transnacionalmente, de acuerdo a la naturaleza de estos ilícitos y de los derechos expuestos, tales como la libertad de expresión, la privacidad y el *hábias data*, e incluso, la seguridad y defensa nacional (CEPAL, 2010; ONU, 2010; UNODC, 2013; Temperini, 2014).

Estas prácticas criminales contemporáneas emergen en el marco de la globalización de prácticas financieras y sociales institucionalizadas y ejecutadas a nivel organizacional, gubernamental y civil mediante la implementación y uso generalizado de las TICs (Manjarrés I & Jiménez F, 2012; ONU 2013). De este modo, la digitalización de distintas actividades económicas y sociales, y de las funciones de seguridad y defensa nacional facilitan el empleo

[1] En el presente documento las TIC's van a ser comprendidas como un fenómeno vinculado a la convergencia, que según Jenkins H (2006) y el DNP (2011), comprende las tecnologías previamente separadas como el internet, la telefonía, los datos (y usos de la productividad) y tecnologías audiovisuales que comparten recursos en red y operan de manera recíproca.

de un medio (v.gr.: el uso de métodos electrónicos como computadores, dispositivos electrónicos vinculados mediante Internet[2], etc.), un escenario (v.gr.: el ciberespacio o las redes vinculadas por servidores de banda ancha), y un objetivo o fin criminal (v.gr.: el dispositivo, el programa o software, los datos e información almacenada, etc.) (CEPAL, 2010, p. 22).

En este contexto la *cibercriminalidad* es concebida como un conjunto de crímenes de naturaleza transnacional que supone el solapamiento, contradictorio en ocasiones, entre ordenamientos jurídicos internacionales y nacionales (CEPAL, 2010). Este escenario sociológico exige un imperativo político y jurídico que lo comprehenda y afronte, no sólo como mero incidente, sino particularmente como un tipo de conducta criminal que representa riesgos sujetos a gestión institucional en términos de acción penal y judicial (CONPES 3854, 2016), en el marco de la seguridad y la defensa nacional de las naciones modernas y democráticas, en la medida en que este expone no sólo derechos civiles sociales y económicos, sino también las infraestructuras críticas del país (Manjarréz et. al., 2012; UNODC, 2013).

En este sentido, la adopción de prácticas institucionales que afronten -disciplinaria, judicial y penalmente- a la *cibercriminalidad,* debe perseguir los siguientes propósitos: (1) registrar los "incidentes informáticos" y, (2) diseñar e implementar instrumentos conceptuales y metodológicos -investigativos y judiciales- eficientes para afrontar este crimen de escala nacional y transnacional (CEPAL 2010; UNODC, 2013). En virtud de este propósito y recomendación para los países vinculados mediante el Derecho Internacional

[2] La Real Academia Española en su Diccionario de la lengua española define «Internet»: 1.m,of. Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación. Disponible en: http://dle.rae.es/?id=LvskgUG. [Consultado el 24 de agosto de 2017].

Humanitario y el reconocimiento de los Derechos Humanos (CEPAL 2010; UNODC, 2013), entre otros tratados internacionales, se diseñó un estudio de investigación cualitativo basado en la teoría fundamentada (Corbin y Strauss , 1998), según el cual el método de consulta de fuentes bibliográficas se realiza hasta alcanzar la saturación teórica de las categorías de análisis provisionalmente propuestas, es decir, que culminó cuando éstas no aportaron información nueva a las categorías o categorías emergentes durante el estudio (Strauss & Corbin, 1998).

Como resultado de este análisis cualitativo en el primer capítulo se define la *cibercriminalidad* y la forma en la que constituye un desafío para las instituciones que administran justicia y, por tanto, para los marcos legales internacionales y nacionales, encargados de enfrentarla en el mundo occidental moderno democrático y globalizado. El segundo capítulo desarrolla la estructura y el contenido conceptual de una herramienta y política concebida por la Fiscalía General de la Nación en Colombia, a saber, la *priorización,* y propone su pertinencia social, política y judicial, teniendo en cuenta las políticas en Ciberseguridad y Ciberdefensa en Colombia, frente a la *cibercriminalidad.* En este capítulo se describe la aplicación de la *priorización* para abordar civil, administrativa y penalmente la *cibercriminalidad.* En el tercer capitulo, se realizará una propuesta a la Fiscalía General de la Nación, consistente en adoptar una herramienta metodológica de priorización para las investigaciones contra la cibercriminalidad.

Finalmente como conclusión se resalta la importancia de la *priorización* para la administración de justicia ya que fortalece los mecanismos institucionales de comprensión de este tipo de crimen y de su naturaleza social y criminal, que amenaza derechos financieros y civiles, pero también políticos, en la medida en que expone la soberanía nacional en términos de afectación a las Infraestructuras Críticas de la nación (entidades o instituciones

que prestan servicios de suministro eléctrico, acueducto y alcantarillado, transporte masivo y público, entre otros) (UNODC, 2013).

Justificación

En la actualidad los Grupos de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP), el CSIRT de la Policía Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y C4 (Centro de Comando, Control, Comunicaciones y Cómputo), creados en Colombia, tienen el propósito de atender los diferentes incidentes ciberneticos del los sectores públicos y privados y no de la judicialización de los ciberatacantes.

Así las cosas, los ciberdelincuentes, siguen realizando ataques a personas o entidades públicas o privadas sin ser judicializados e investigados por la Fiscalía General de la Nación, estos atacantes se cambian de ciudad o en algunas ocaciones de país, sin que exista freno a estos delincuentes, solo la reciliencia que hacen los CSIRT. Es por ello que se realizará una propuesta en el capitulo tercero del presente documento académico.

Problema

Por lo anterior, en los grupos de respuesta creados en el país, no se cuenta con fiscales y policía judicial que filtren cada uno de los incidentes reportados a estas entidades y se realicen unas valoraciones técnico jurídicas, con el proposito de poder investigar y denunciar ante la Fiscalía General de la Nación, aquellos casos en los cuales se determine la viabilidad de judicializar a los ciberatacantes o los ciberdelincuentes.

Pregunta de investigación

El presente trabajo pretende resolver: ¿En qué consistiría una metodología de priorización para la investigación de cibercriminalidad dentro de la Fiscalía General?

Objetivo General

Proponer una herramienta metodológica de priorización para las investigaciones en contra de los cibercriminales, y con el apoyo de otras entidades públicas y privadas la ejecución y puesta en marcha de la conformación de la Mesa Técnica Contra la Cibercriminalidad -**MTCC**- y generar los lineamientos necesarios entre todas las entidades, con el proposito de frener la ciberdelicuencia y los ataques cibernéticos.

Objetivos Específicos

- Contextualizar las definiciones de los delitos informaticos Nacional e Internacionalmente.
- Determinar el papel de la Fiscalía General de la Nación en los delitos informaticos.
- Proponer a la Fiscalía General de la Nación y a las entidades involucradas en atender los incidentes cibernéticos, una herramienta metodológica de priorización para adelantar investigaciones contra los cibercriminales.

1. Hacia una definición del delito informático: una pretensión conceptual y metodológica a escala transnacional

Las tecnologías de la información y la comunicación (TIC's) han emergido y consolidado relevancia no sólo en los países desarrollados sino también en las naciones de la región Latinoamericana y del Caribe (CEPAL 2010). Así, según la base de datos de la Organización de las Naciones Unidas, en el año 2015, 44 de cada 100 personas en el mundo tuvo acceso a Internet[3], en Latinoamérica, por su parte más de la mitad de la población tuvo acceso a la red y, la tasa de crecimiento de usuarios se encuentra entre las más altas del mundo (OEA; 2016). Estas transformaciones sociales se han visto reflejadas también en las resoluciones emitidas por el Consejo de Derechos Humanos de las Naciones Unidas, que protegen como derechos humanos básicos tanto el acceso al Internet como la libertad de expresión, el anonimato y el cifrado en esta plataforma digital y, además, exhortan a los Estados a promover y facilitar el acceso y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información (ONU, 2012).

En este sentido, entre las ventajas sociales y económicas que ha tenido el reconocimiento social, institucional, y por tanto, moral y legal del uso de estas tecnologías, se encuentran la extensión del comercio internacional y nacional mediante la transferencia electrónica de divisas, el almacenamiento y comercialización de datos e información, el fortalecimiento de redes de comunicación e información, así como en la administración y

[3] Datos obtenidos de la UNdata a World of Information, Web Site Url: http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3AIT.NET.USER.P2. [Consultada el 28 de agosto de 2017]

suministro de bienes y servicios como acueducto y alcantarillado, energía eléctrica, transporte público, entre otros considerados como parte de las infraestructuras críticas de un país[4] (Sood & Enbody, 2013).

La importancia de las TIC se ha resaltado desde finales del siglo pasado, así, por ejemplo, la Organización de las Naciones Unidas mediante la Comisión de Ciencia y Tecnología para el Desarrollo publicó el informe *Knowledge Societies: Information Technology for Sustainable Development* (Mansell &Whn, 1998), proponiendo una relación asertiva entre el desarrollo social y económico y las posibilidades de crear "sociedades del conocimiento" innovadoras[5]. Este concepto de *sociedades del conocimiento* ha sido adoptado también por las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2005), "va más allá de la tecnología y hace hincapié en los procesos de desarrollo humano que transforman la información en conocimiento y permiten que los *gobiernos, los individuos y las organizaciones* hagan cambios duraderos en la economía y la sociedad." (ONU, 2014). De esta forma las TIC configuran interrelaciones que definen las nuevas prácticas sociales, institucionales e individuales, y que por tanto reclaman el ejercicio deliberado entre distintos actores que se encuentran relacionados por las tendencias que socialmente estas perfilan, a saber:

> "Las cinco tendencias que marcaron a las TIC entre el año 2005 y 2010 y que incidieron profundamente en las inversiones, la adopción y el potencial de desarrollo de las TIC: a) El avance hacia el acceso móvil universal; b) La transición de las redes de banda

[4] La infraestructura crítica es definida por la Resolución 2258 de 2009, emitida por Comisión de Regulación de Comunicaciones (CRC, 2009), como el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación.

[5] Del mismo modo el En el *Informe sobre el desarrollo mundial 1998-1999*, el Banco Mundial también citó el conocimiento como motor esencial del crecimiento económico y del bienestar social del próximo siglo; disponible en http://www.rrojasdatabank.info/wdr98/overview.pdf

estrecha a las bandas anchas; c) La computación en la nube; d) Internet móvil y las aplicaciones para teléfonos móviles; d) Las redes sociales y el contenido generado por los usuarios en Internet." (ONU, 2014)

Estas tendencias involucran bienes, servicios y derechos movilizados a través de las TICs, y en especial de la red electrónica o digital que constituye el conjunto de protocolos TCP/IP, es decir, el Internet, y que puede incluir el "envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea, la transmisión de contenido multimedia -telefonía (Voz-lp), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea"[6]. Estas nuevas formas de relacionarse, interactuar, intercambiar, procesar, almacenar y comercializar bienes, mercancías e información se encuentran sujetas a accesos y manejos no autorizados e ilegítimos en términos morales, sociales, jurídicos y políticos (Williams, 2001). Bienes y derechos como la propiedad intelectual, la intimidad, la integridad moral, los datos e información personal y confidencial, la libertad de expresión y la privacidad, se encuentran en el núcleo de la discusión regulativa y normativa en torno a los delitos informáticos y las respuestas institucionales que deben asumirlos.

Por consiguiente, el desafío de proteger los derechos, bienes, servicios, datos e información de las personas y organizaciones surge en la medida en que el Estado asume como principal responsable y garante de la disponibilidad de estos servicios prestados a través de Internet, pues representan tanto herramientas de transacciones económicas importantes a nivel individual y organizacional, como un vehículo importante para distintas prácticas de orden, control y seguridad social que comprenden el manejo, almacenamiento y

[6] «Internet, n.» *Oxford English Dictionary* Marzo de 2009. Consultado el 26 de agosto de 2017. "7.76 Terms like 'web' and Internet", *Chicago Manual of Style,* University of Chicago.

transferencia de datos e información (CEPAL, 2010). De esta forma, en estas *sociedades del conocimiento* la gestión y ejecución de los gobiernos en los Estados-nación modernos se ha concebido bajo el concepto de *gobierno electrónico*, que, aunque varía según su implementación, puede resumir sus funciones en:

> "(a) mejorar la calidad y el acceso a los servicios, (b) reducir costos administrativos, (c) restablecer la confianza de los ciudadanos, (d) evitar el desperdicio de recursos. (e) efectuar reingeniería de procesos, (f) mejorar la infraestructura de tecnologías de información y comunicación, (g) entender la relación entre política y resultados, (h) decidir dónde gastar y cuándo, (i) rediseñar la entrega de servicios con calidad, transparencia y rendición de cuentas, (j) mejorar la capacidad de gobernar para atender los anhelos y expectativas de la sociedad, recuperando con ello la confianza en sus autoridades, (k) facilitar la implementación de la administración por objetivos, la creación de organizaciones más flexibles, el funcionamiento de estructuras menos piramidales y la creación de oficinas de gobierno más pequeñas y eficientes." (CEPAL, 2010, p. 16)

Así mismo, la Organización para la Cooperación y Desarrollo Económico (OCDE), "el gobierno electrónico se refiere al uso de las tecnologías de la información y comunicación, particularmente de Internet, como una herramienta para alcanzar un mejor gobierno" (OCDE, 2004). Estas funciones de *gobierno electrónico* pueden encontrar distintas manifestaciones normativas y distintas formas de enfrentar las prácticas delictivas que pueden incidir negativamente en la ejecución de dichas funciones. De este modo, con el propósito de enfrentar estas amenazas y gestionar el riesgo que representan a nivel local, regional e internacional, se han formulado, según los marcos normativos de cada país, en primer lugar, definiciones del crimen o delito informático ceñidas a los códigos penales tradicionales, por lo tanto, limitadas por la naturaleza de delitos o crímenes no relacionados necesariamente al uso de las TICs como plataforma, herramienta y objetivo delictivo (CEPAL, 2010, p. 29;

Manjarrés & Jiménez, 2012). En segundo lugar, reconociendo la eventual naturaleza transnacional de los delitos informáticos, se han propuesto definiciones que pretenden fortalecer la articulación y cooperación entre los Estados y el sector privado contra estos (UNODC, 2013).

Por tanto, en virtud del reconocimiento y el valor político -democrático- de las organizaciones intergubernamentales que promueven la cooperación internacional, los Derechos Humanos y el Derecho Internacional Humanitario, se describen: (1) la definición de delito informático que propone el Consejo de Europa en la Convención sobre el Cibercrimen en Budapest, celebrada el 23 de noviembre del año 2001; y, (2) las dificultades y al mismo tiempo la relevancia, para las políticas y prácticas de ciberseguridad y ciberdefensa, de una definición amplia que permita su abordaje político, judicial, su comprensión social y su gestión en términos del riesgo (CONPES 3701, 2011; CONPES 3854, 2016).

1.1. Una definición de delincuencia informática: asunto nacional de relevancia transnacional

En el año 2011, según el "Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno", realizado por la United Nations Office on Drugs and Crime (2013, p. 2), más de un tercio de la población total del mundo tuvo acceso a Internet. más del 60% de estos usuarios se encuentran en países en desarrollo y, para el 2017 se estima que las suscripciones a la banda ancha móvil serán del 70% de la población mundial. La globalización de las tecnologías de la información y la comunicación es entonces reconocida también a nivel regional, e incluso nacional, y de este modo, la implementación de los *gobiernos electrónicos* se ha consolidado institucionalmente en los Estados latinoamericanos vinculados mediante el Derecho Internacional Humanitario (DIH), los Derechos Humanos (DH) y la Organización de los Estados Americanos (OEA, 2004 y 2015; CEPAL, 2010; Temperini, 2014). De igual forma la digitalización e incorporación en la red de las instituciones no gubernamentales, corporaciones y organizaciones privadas, así como de individuos y colectivos civiles, es reconocida como una realidad sociológica que si bien facilita actividades productivas, sociales e interpersonales y gubernamentales, expone a riesgos determinados bienes, servicios y derechos movilizados mediante las TIC, e incluso, la seguridad y defensa nacional, comprendiendo el "ciberespacio" como plataforma y escenario de guerra (Lewis, 2002; Lee 2012; Raymond, 2011).

Así, aunque las iniciativas políticas y judiciales se encuentran circunscritas en los marcos legales y normativos de cada Estado en Latinoamérica, existe en occidente moderno y democrático una propuesta o pretensión legislativa de alcance internacional y transnacional,

que tiene en cuenta acuerdos como el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966), el Convenio de 1981 del Consejo de Europa, la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999). Dicha pretensión legislativa se actualiza en la Convención de Budapest (Consejo de Europa, 2001), pues reconoce, como lo hace la CEPAL en el año 2010, que los crímenes cometidos *a través de* las TIC y *en* las TIC comprenden un "conjunto de los varios crímenes que se denotan por la presencia de alguna tecnología, es un fenómeno global, como es global la red, y por tanto, si se quiere limitarlo, la coordinación a nivel internacional es una necesidad imprescindible" (Consejo de Europa, 2001). Es así como se formuló en Europa esta primera iniciativa de legislación o regulación internacional que recoge dentro de las "Medidas que deberán adoptarse a nivel nacional" dentro del Derecho Penal Sustantivo, la tipificación de los *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*, que, resumiendo, son clasificados así: en el "Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos", los Artículos:

> (2) Acceso ilícito: acceso deliberado e ilegítimo a todo o parte de un sistema informático; (3) Interceptación ilícita: interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos; (4) Ataques a la integridad de los datos: todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos; (5) Ataques a la integridad del sistema: obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la

introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos; (6) Abuso de los dispositivos: comisión deliberada e ilegítima de (a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de (i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio; (ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático [...](CEPAL, 2010, p. 6)

En el "Título 2 - delitos informáticos" este mismo documento clasifica en los siguientes Artículos:

(7) Falsificación informática: introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos [...]; (8) Fraude informático: actos deliberados que causen perjuicio patrimonial a otra persona mediante (a) la introducción, alteración, borrado o supresión de datos informáticos y (b) cualquier interferencia en el funcionamiento de un sistema informático. (CEPAL, 2010, p. 6)

El "Título 3 -Delitos relacionados con el contenido", por su parte, comprende los delitos relacionados con información o datos que exponen o vulneran los derechos y la integridad física y moral de terceros, y contiene el artículo (9) Delitos relacionados con la pornografía infantil: comisión deliberada e ilegítima de actos de producción, oferta o disposición, adquisición y posesión de pornografía infantil. Por su parte, el "Título 4 -Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines", clasifica los crímenes vulnerados o expuestos deliberadamente según el Acta de París de 24 de julio de 1971, y el Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor, la Convención Internacional sobre la Protección de los Artistas Intérpretes o

Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma) (CEPAL, 2010, p. 6).

De esta forma comienza a gestarse en las naciones occidentales democráticas pretensiones legislativas legítimas en términos políticos, sociales e históricos, pues la globalización de las TIC emerge como una realidad sociológica y un imperativo de gobernabilidad y justicia penal propio de las *sociedades del conocimiento* y los *gobiernos electrónicos*.

Así, a pesar de esta necesidad o exigencia de principios de Derecho Penal Internacional (Lyal S, 1997), el desarrollo de un concepto o definición del delito informático, internacionalmente compartido, se encuentra frente a una serie de prácticas criminales que por su naturaleza -cibernética o digital- se transforma continuamente, tanto de acuerdo a las tecnologías implementadas, como a los bienes, derechos y servicios que de este modo son involucrados, por lo tanto, su definición se encuentra circunscrita a nivel prevalentemente nacional (CEPAL, 2010, p. 22). De esta forma, las "definiciones" de delito informático o cibernético se encuentran condicionadas por la *intención* con la que se utiliza este concepto y el contexto legal nacional. Debido a esto, en un sentido general y amplio, la CEPAL (2010) a partir de la aclaración de Casabona asume las nociones de *delincuencia informática, delincuencia relacionada con la informática, delincuencia de alta tecnología o delincuencia cibernética,* pues conservan un significado común en cuanto se refieren a: "a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles." (CEPAL, 2010, p. 22).

Adoptar esta noción permite comprender que el factor o el elemento común a estos crímenes es su vinculación, de alguna manera, con los computadores, pues "ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho

delictivo presenta siempre características semejantes...el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes" (Casabona, 1987 [Citado por CEPAL, 2010, p. 23]).

En síntesis, la delincuencia informática o la cibercriminalidad emerge como un conjunto de prácticas delictivas que se agrupan en delitos contra la propiedad intelectual, delitos contra la intimidad, delitos relativos al contenido y delitos económicos, acceso no autorizado y sabotaje. (CEPAL, 2010). Según la UNODC (2013), la expansión de la conectividad global surge en un momento de "transformaciones económicas y demográficas, con disparidades de ingresos crecientes, estrechamiento de gasto del sector privado y reducción de la liquidez financiera" (UNODC, 2013, p.)

Estos delitos, en las jurisdicciones norteamericanas, latinoamericanas y europeas continúan produciendo ingresos y al mismo tiempo demostrando la limitación de los marcos normativos existentes para regularlas, tipificarlas, judicializarlas y penalizarlas, debido a su alta frecuencia y sofisticación (UNODC, 2013; OEA; 2016). La iniciativa normativa de Budapest, adelantada por el Consejo de Europa, especialmente, se ha implementado en conjunción con otras medidas no legislativas, tales como la creación de unidades nacionales especializadas; la formación permanente y especializada de policías y personal de la administración de la justicia; la armonización de las normas de contabilización en materia policial y judicial, así como la creación de instrumentos adaptados para el análisis estadístico de la criminalidad informática; creación de acciones realizadas por entidades e instituciones privadas y públicas para registrar, tipificar y judicializar los delitos informáticos; y, la implementación de proyectos en el ámbito de la investigación y el desarrollo tecnológico. (CEPAL, 2010., p.24).

En América Latina, en particular, en el año 2004 los Estados Miembros de la OEA aprobaron la Estrategia Interamericana Integral para combatir la Amenazas a la Seguridad Cibernética, que propone coordinar esfuerzos entre las múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio y proporciona un marco inicial para guiar este enfoque. Esto "ha fortalecido la capacidad de los gobiernos electrónicos para responder y mitigar incidentes cibernéticos y reforzado nuestra resiliencia individual y colectiva frente a amenazas cibernéticas" (OEA, 2016). Recientemente, con el mismo propósito, la misma OEA ha implementado el Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE), logrando suministrar apoyo a los Estados Miembros en la elaboración de estrategias de seguridad cibernética nacional, capacitación otorgada a los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacionales y regionales, facilitación de ejercicios de gestión de crisis con operadores de la industria nacional crítica y los activos de respuesta a emergencias, la sociedad civil y el sector privado y, finalmente, ha creado conciencia sobre las amenazas y las oportunidades relacionadas con la seguridad cibernética en la región (OEA, 2016). No obstante, sigue siendo urgente y necesario el fortalecimiento de la cooperación multilateral, la creación de capacidad de prevención, respuesta y resiliencia frente a un conjunto de delitos de naturaleza transnacional y cibernética. De esta forma, la OEA (2016) plantea que la "madurez cibernética" de cada país debe implementarse en cinco dimensiones: "1) política y estrategia de seguridad cibernética; 2) cultura y sociedad cibernética; 3) educación, formación y competencias en seguridad cibernética; 4) marcos jurídicos y reglamentarios; y 5) normas, organizaciones y tecnologías." (OEA, 2016). Igualmente se han desarrollado grupos, convenciones o conversaciones que en la agenda internacional han diseñado e implementado estrategias en contra de estos delitos. Entre estos se encuentran el Grupo de Expertos

Gubernamentales de las Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN, por sus siglas en inglés), y la OEA.

De manera que, en el marco de estas fórmulas y estrategias institucionales internacionales y regionales, para abordar la cibercriminalidad, surgen también en Colombia, como respuesta a la inminente interrelación entre el avance y la implementación de las TIC y la exposición al riesgo, de la seguridad y defensa nacional, a la delincuencia informática en cualquiera de sus expresiones, iniciativas legislativas y normativas que permitan a las entidades e instituciones públicas, e incluso privadas, afrontarla y prevenirla. Por lo tanto, en virtud de alcanzar la "madurez cibernética" que formula la OEA en Colombia se gestan marcos jurídicos y reglamentarios, normas, organizaciones y tecnologías que configuran entre sí una política y estrategia de seguridad cibernética; la formulación de una cultura y sociedad cibernética; y, directrices para la educación, formación y competencias en seguridad cibernética.

1.2. Definición del crimen cibernético y las políticas en seguridad y defensa en Colombia

En Colombia las iniciativas políticas y legislativas en torno al crimen cibernético han emergido como resultado de dos dinámicas. En primer lugar, las relacionadas con la implementación de mecanismos de prevención y protección jurídicos en torno a derechos, bienes y servicios de tipo civil y económico que son producidos, distribuidos y consumidos "en línea" o digitalmente, y, por otro lado, las de respuesta institucional frente a la ocurrencia de incidentes informáticos de escala transnacional en el país (v.gr.: los incidentes digitales[7] más recientes reconocidos públicamente son el "Chimera", "Petya"; y el "Wannacry"). La primera se expresa en las múltiples demandas registradas en organismos de control, vigilancia, investigación y penalización y, la otra, en íntima relación con aquella, en el diseño e implementación de políticas de seguridad y defensa digital, y, por ende, de la consolidación de instituciones que a nivel nacional buscan la reducción de la cibercriminalidad. Cabe anotar que esta relevancia civil y política es también pronunciada por los distintos medios de comunicación, nacionales e internacionales, que circunscriben el crimen cibernético como una de las manifestaciones delictivas contemporáneas de mayor impacto social, político e incluso militar (Ureña, 2015). Sobre este último punto el Departamento Nacional de Planeación (DNP, 2011) en Colombia señala, como ejemplo, el ataque ejecutado durante el primer semestre de 2011 por el grupo *hacktivista* autodenominado Anonymous, a los portales

[7] Los incidentes digitales se basan, generalmente, en el uso de algún software malintencionado, diseñado para perjudicar o hacer un uso no lícito de los sistemas de información de las organizaciones y/o los individuos. En particular, el *malware* (del inglés *malicious software*, empleado para denominar cualquier programa digital malicioso) es un tipo de programa informático que tiene como propósito acceder y dañar determinado sistema de información sin el consentimiento legítimo de sus propietarios.

de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior, de Justicia, de Cultura y de Defensa, dejando fuera de servicio sus páginas web por varias horas (DNP, 2011). Este tipo de práctica criminal si bien no se encuentra en el marco de protección y garantía de derechos socioeconómicos, sí hace parte de los objetivos de la política de seguridad y defensa que el Estado colombiano debe garantizar, reconociendo su legitimidad política, social y jurídica para proteger la soberanía nacional y, por tanto, las instituciones -digitales o no- que realizan funciones administrativas, financieras, entre otras (DNP, 2016).

De tal modo que el diseño, gestión y ejecución de leyes y normas que regulen el uso de las TIC, por un lado, y la tipificación de los delitos informáticos asociados con estas, por otro lado, se han concebido en virtud de estos dos grandes propósitos de la política pública, a saber, la garantía de la seguridad y defensa nacional y de derechos sociales, económicos e incluso, de derechos fundamentales de los niños y las niñas de Colombia (DNP, 2011; 2016).

En este apartado, en primer lugar, se describen los elementos legales o normativos que constituyen la definición que adopta el Estado colombiano de crimen o delito informático, en segundo lugar, desarrollamos los desafíos sociales, políticos y judiciales que señalan estas mismas estrategias institucionales y, finalmente, resaltamos la pertinencia de elaborar e implementar herramientas y políticas judiciales e investigativas para afrontar el crimen desde la entidad que en Colombia se encarga de administrar justicia, la Fiscalía General de la Nación (FGN).

La gestión legislativa y penal en Colombia ha estado caracterizada, en términos generales, por concebirse en el seno de una problemática globalizada y emergente del uso y la implementación de tecnologías de la información y la comunicación a escala global, regional y local (Manjarrés et. al., 2012). En este sentido las obligaciones que el Estado

colombiano asume de este modo son también parte de los distintos convenios o tratados internacionales, y, fundamentalmente, de la forma como los Estados modernos responden a los riesgos que producen las mismas dinámicas históricas, sociales, políticas, militares y científico-técnicas de las sociedades contemporáneas, sociedades de producción del riesgo mundial (Beck, 2007).

En medio de estas condiciones sociológicas, históricas y legales en las que se concibe el *delito informático* se gestan también las distintas consecuentes respuestas políticas y legales. En Colombia la primera expresión institucional registrada y relacionada con el acceso, uso y comercio de datos e información digital y electrónica es la Ley 527 de 1999. Esta ley "define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" (Congreso de Colombia 1999: p. 1). Esta regulación comienza a recoger y afrontar las demandas civiles y gubernamentales en torno a la información digital y electrónica, a su uso y comercialización según el ordenamiento constitucional.

De esta forma define los distintos elementos que en el área de la informática resultan oportunos para cumplir el susodicho propósito: *mensaje de datos*; *comercio electrónico*; *firma digital*; *entidad de certificación*; *intercambio electrónico de datos (EDI)* y *sistema de información.* Estas definiciones empiezan a reglamentar un bien que socialmente es adquirido a finales del siglo XX, a saber, los datos informáticos que devienen en un bien jurídicamente protegido, incluso, por el DIH y el DH, que es, el derecho a la autodeterminación, o lo que es lo mismo, a la propiedad privada, el derecho a la intimidad y el libre desarrollo de la personalidad, recogido, si se quiere, en un derecho contemporáneamente reconocido como

habeas data[8] (Ley N°1266, 2008). Esta última ley "dicta las disposiciones generales del *habeas* data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" (Ley N° 1266, 2008). Igualmente, la Ley Estatutaria N° 1581 de 2012 tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma". Este conjunto de leyes termina de conformar la normatividad relacionada con los datos e información digital, considerados como bienes jurídicos tutelados, y, por tanto, protegidos constitucionalmente.

Por consiguiente, tanto la Ley N° 527 de 1999 como la Ley N° 1266 de 2008 y la Ley Estatutaria 1581 de 2012 tienen un propósito normativo, pero no penal, pues no tipifican el delito del crimen cibernético o la cibercriminalidad y, sin embargo, resaltan la importancia jurídica, política y socioeconómica de los bienes, derechos y deberes que emergen con la implementación y uso de tecnologías de la información y la comunicación en el país.

Solo hasta la implementación de la Ley N° 1273 de enero del 2009 se incorporan en la Ley N°599 del 2000, el Código Penal Colombiano, las nociones de delitos informáticos concernientes a las cuatro dimensiones generales en las que se han tipificado, internacionalmente, estas conductas delictivas, a saber, *delitos contra la propiedad*

---

[8] El *habeas data* hace parte de la necesidad del Estado Social de Derecho, fundado en el respeto de la dignidad humana, de garantizar un espacio -cibernético- propio de la intimidad y otros derechos fundamentales, ante la inminente presencia de las TIC's. En términos generales, el *Habeas Data* le permite al ciudadano conocer, actualizar y rectificas las informaciones que se hayan recogido sobre él en bancos de datos y en archivos de entidades públicas y privadas.

intelectual, delitos contra la intimidad, delitos relativos al contenido y delitos económicos, acceso no autorizado y sabotaje. Según esta ley, "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones [...]", se tipifican en Colombia dos tipos de conductas delictivas relacionadas con los computadores o las redes informáticas: (1) los atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos; y, (2) los atentados informáticos y otros (Ley N° 1273, 2009). En el Capítulo I de esta ley se tipifican los siguientes delitos informáticos: ART.269A *Acceso abusivo a un sistema informático*; ART. 269B *Obstaculización ilegítima de sistema informático o red de telecomunicación;* ART. 269C *Interceptación de datos informáticos*; ART. 269D *Daño Informático*; ART. 269E *Uso de software malicioso*; ART. 269F *Violación de datos personales*; y, ART. 269G *Suplantación de sitios web para capturar datos personales*. Por su parte, el Capítulo II comprende los siguientes atentados informáticos: ART. 169I: *Hurto por medios informáticos y semejantes*; y, ART. 269J *Transferencia no consentida de activos*.

Finalmente, el Documento del Consejo Nacional de Política Económica N° 3701 de 2011, titulado *Lineamientos de política para ciberseguridad y ciberdefensa*[9], tiene el fin de "abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales y contrarrestar el incremento de las amenazas informáticas que afectan al país y desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad

[9] Por ciberseguridad se entiende, según el CONPES 3701 (DNP, 2011, p. 2), la "capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética"; y, por ciberdefensa la "capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

cibernética", representando la primera iniciativa de política económica relacionada con la seguridad y la defensa en el ciberespacio en Colombia (Manjarrés et. al., 2012).

En términos generales, el objetivo de este Documento CONPES fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético. Para cumplir este se formularon tres objetivos específicos:

> (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y (iii) fortalecer el cuerpo normativo y de cumplimiento en la materia.

Este documento, como señalamos arriba, emerge en el marco de dinámicas legislativas internacionales que pretenden afrontar las consecuencias sociales, políticas y económicas de distintos ataques cibernéticos. Entre estos se encuentran, en primer lugar, el acaecido en Estonia, en el cual se afectaron la presidencia, el parlamento, parte de los ministerios, los partidos políticos y dos bancos. En segundo lugar, el sucedido en Estados Unidos en julio de 2009, en el que se afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio. Y, en tercer lugar, señala el ataque desmantelado por la Guardia Civil española en el año 2010, distribuido en 190 países en el mundo, entre los cuales se encontraba Colombia en el quinto puesto de los más afectados (DNP, 2011, p. 6). En el marco de estos acontecimientos históricos este documento formula las directrices para la articulación entre el Grupo de Respuesta a Emergencias Cibernéticas de Colombia

(colCERT), grupo adscrito al Ministerio de Defensa y coordinador a nivel nacional de los aspectos de ciberseguridad y ciberdefensa, con el Centro Cibernético Policial -CCP- y el Comando Conjunto Cibernético -CCOC-.

Luego, en el año 2013 el Ministerio de Relaciones Exteriores de Colombia solicitó adhesión al Convenio de Budapest (DNP, 2016). En este mismo año se estableció un convenio multilateral con el Foro Económico Mundial para identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, cada vez mayor, entre personas, procesos y objetos. (CONPES 3854: p. 15). De esta forma el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA, 2016), se ha logrado trabajar con varios equipos de respuesta ante incidencias de seguridad (CSIRT) en la región de América Latina. De esta forma Colombia hace parte de una red de alerta que proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernético, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente. (CONPES 3854: p. 15) Este documento recoge no solo los objetivos de defensa del país y lucha contra el cibercrimen, sino que además enmarca la Política Nacional de Seguridad Digital en las prácticas de gestión del riesgo en el entorno digital (DNP, 2016). Este nuevo enfoque demanda una mayor *planificación, prevención y atención* por parte de las instituciones públicas del país, ya que contempla:

> [...] la defensa y seguridad nacional en el entorno digital, incluidas las infraestructuras críticas cibernéticas nacionales, incluye componentes como la gobernanza, la educación, la regulación, la cooperación internacional y nacional, la investigación y desarrollo, y la innovación. Adicionalmente, amplía la población objetivo, del Estado (política de ciberseguridad y ciberdefensa) a todos los ciudadanos, sectores económicos y organizaciones (múltiples partes interesadas). Lo anterior, reconociendo la necesidad de diferenciar los objetivos de ciberseguridad y

ciberdefensa, de los de prosperidad económica y social, fortaleciendo este último. (DNP, 2016, p. 10)

De esta forma, la política en seguridad y defensa digital en el país se hace sofisticada y, de un modo u otro, demanda mayor articulación entre los distintos actores, institucionales y civiles, que pueden estar sujetos a riesgos o amenazas cibernéticas. En la siguiente tabla, que aparece publicada en este mismo documento, se agrupan las denuncias registradas por iniciativa "Te Protejo en Colombia", entre los años 2012 al 2015, para un total de 21.271, de las cuales 11.506 se encuentran relacionadas con "Pornografía Infantil", lo cual expone los derechos de un grupo social etario en condición de vulnerabilidad.

Tabla 1 Denuncias procesadas por la iniciativa Te Protejo en Colombia, 2012 - 2015

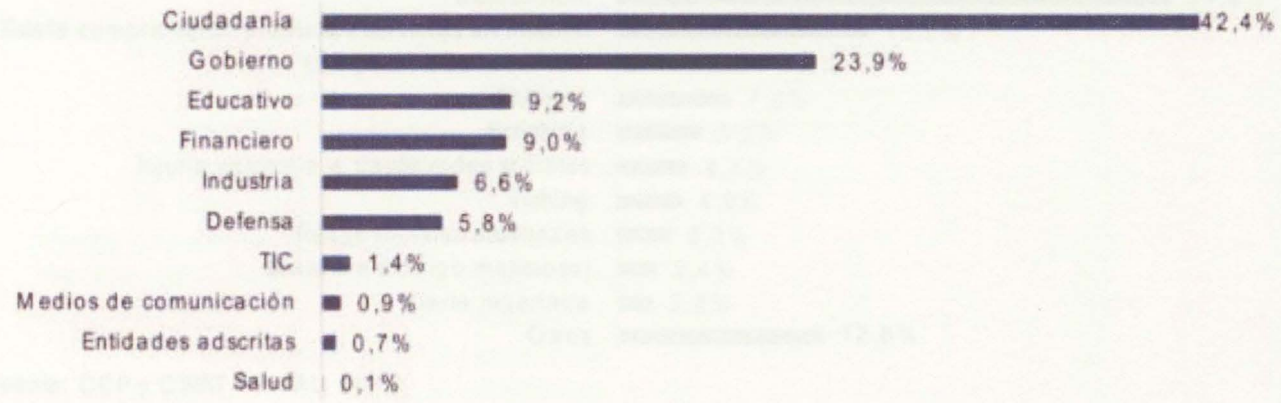
Tipo de denuncia	2012	2013	2014	2015	Total
Pornografía Infantil	462	1.493	3.724	5.827	11.506
Maltrato, trabajo y abuso infantil	101	1.041	988	1.311	3.441
Otros	918	405	606	435	2.364
Ciberacoso	0	0	491	539	1.030
Contenidos inapropiados	145	263	245	175	828
Venta de alcohol	143	212	143	150	648
Intimidación escolar	129	126	187	143	585
ESCNNA	0	0	36	127	163
No aplica	294	381	32	0	707
Total	2.192	3.921	6.452	8.707	21.272

Fuente: www.teprotejo.org, 2015.

Tabla 1. Denuncias procesadas por la iniciativa Te Protejo en Colombia, 2012 - 2015 [Tomado de: Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital.* Documento CONPES 3854, Bogotá D.C., Colombia: DNP.

Ahora bien, como afirma este documento, los sectores más afectados en Colombia son, en primer lugar, la ciudadanía con un 42,4% de afectación, seguida por el gobierno con un 23,9%, luego el sector educativo con un 9,2%, en cuarto lugar, se encuentra el sector financiero con 9%, seguido del sector industrial y el sector defensa, en quinto y sexto lugar, respectivamente (DNP, 2016, p.32).

Ilustración 1. Sectores Afectados en Colombia por incidentes digitales



Fuente: colCERT, 2015.

Gráfico 1. Sectores Afectados en Colombia por incidentes digitales, 2015 [Tomado de: Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital*. Documento CONPES 3854, Bogotá D.C., Colombia: DNP.

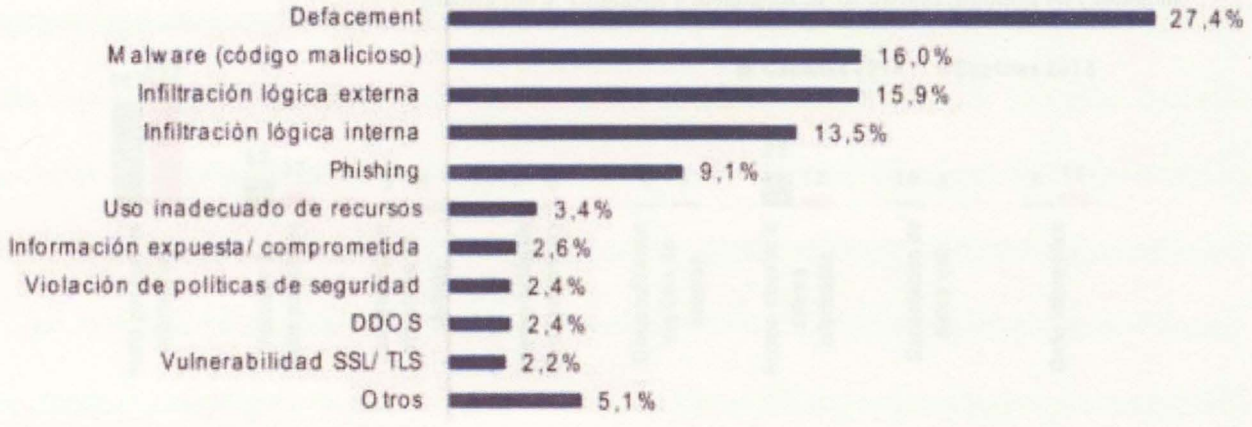
Estos delitos reportados, así como sus consecuentes porcentajes de afectación a cada una de estas esferas o sectores de lo social en Colombia se encuentran en un subregistro en las entidades encargadas de judicializar y penalizar estos delitos que incluyen, según las tendencias para el año 2015 registrados por el CCP y el CSIRT PONAL: *defacement, estafa compra-venta de productos o servicios en internet, usurpación de identidad, phishing, injuria o calumnia en redes sociales, vishing, amenazas en redes sociales, malware, carta nigeriana, entre otros*.

Ilustración 2. Incidentes digitales gestionados por CCP y CSIRT PONAL

Gráfico 2. Incidentes digitales gestionados por CCP y CSIRT PONAL en el entorno digital en Colombia, 2015[Tomado de: Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital*. Documento CONPES 3854, Bogotá D.C., Colombia: DNP.

Ahora bien, en el mismo documento CONPES 3854, frente a ataques específicos nos muestran en el grafico dos y tres, las tendencias de los ataques específicos para el año 2015, así:

Ilustración 3. Incidentes digitales gestionados por CCOC y el colCERT



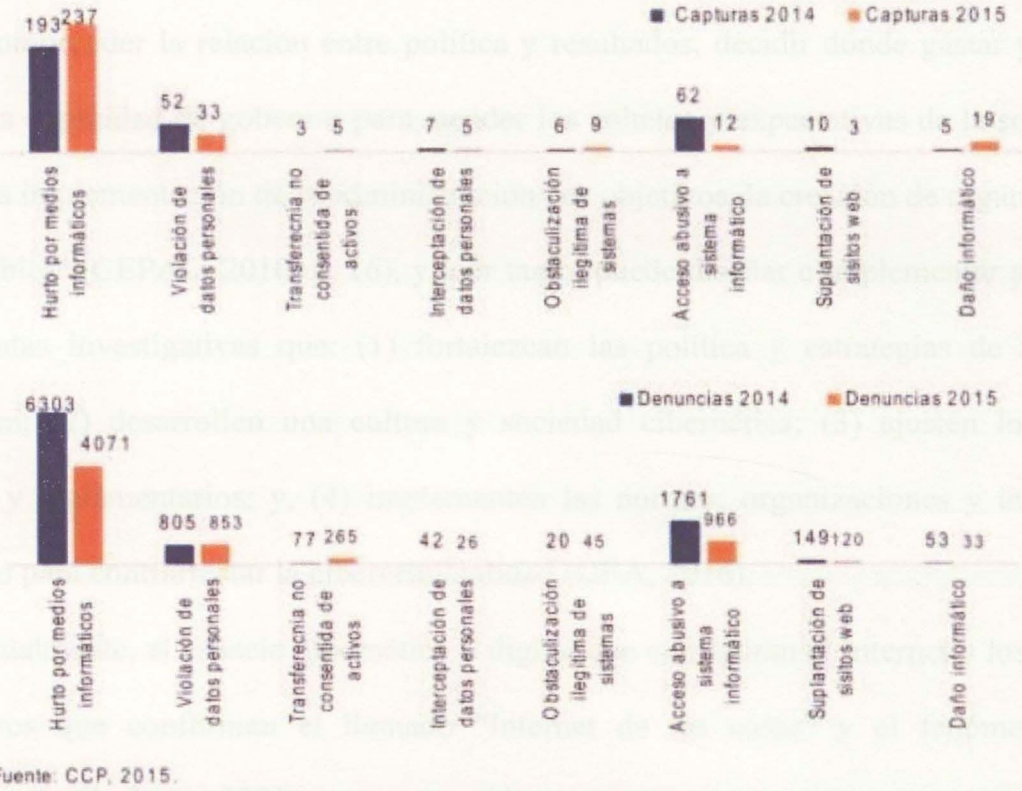
Fuente: CCOC y colCERT, 2015.

Gráfico 3. Incidentes digitales gestionados por CCOC y el colCERT en el entorno digital en Colombia, 2015[Tomado de: Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital*. Documento CONPES 3854, Bogotá D.C., Colombia: DNP.

Estos tipos de ataques cibernéticos, como se ha afirmado arriba, pueden darse a nivel local, regional o internacional -transnacional-, por lo cual la articulación interinstitucional entre las entidades encargadas de registrar y documentar los incidentes informáticos, y las encargadas de investigar, judicializar y penalizar estos delitos emerge como un imperativo social, político y económico, reconocido en instancias internacionales (OEA, 2016; UNODC, 2013), pero también en el mismo CONPES 3854, a nivel nacional.

Sin embargo, como muestra la Gráfica número 4, el número de denuncias de incidentes informáticos no se encuentra relacionado de manera directamente proporcional con el número de capturas de los incidentes en Colombia para el año 2015.

Ilustración 4. Capturas y denuncias de incidentes digitales en Colombia



Fuente: CCP, 2015.

Gráfico 4. Capturas y denuncias de incidentes digitales en Colombia, 2015 [Tomado de: Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital.* Documento CONPES 3854, Bogotá D.C., Colombia: DNP].

Esto permite afirmar que gran parte de los incidentes informáticos presentados y registrados por parte del CSIRT, colCERT de la Policía Nacional y colCERT del Ejército, no son judicializados y penalizados, por lo cual, se propone la adopción e implementación de una política y herramienta de *priorización* en la investigación que adelanta la FGN como ente encargado de investigar las responsabilidades civiles, administrativas y judiciales de los ciudadanos y funcionarios públicos en Colombia. Esta política criminal tendría que permitir la efectiva articulación de las entidades responsables en registrar los incidentes, reportarlos a la FGN y ésta los investigaría, judicializaría y penalizaría adecuadamente.

En este sentido, se afirma que la Fiscalía General de la Nación junto con el Ministerio de Justica, en orden con las funciones que la CEPAL atribuye a un buen gobierno electrónico, deben "comprender la relación entre política y resultados, decidir dónde gastar y cuándo, mejorar la capacidad de gobernar para atender los anhelos y expectativas de la sociedad y, facilitar la implementación de la administración por objetivos, la creación de organizaciones más flexibles" (CEPAL, 2010, p. 16), y, por tanto, puede diseñar e implementar políticas y herramientas investigativas que: (1) fortalezcan las política y estrategias de seguridad cibernética; (2) desarrollen una cultura y sociedad cibernética; (3) ajusten los marcos jurídicos y reglamentarios; y, (4) implementen las normas, organizaciones y tecnologías necesarias para contrarrestar la cibercriminalidad (OEA, 2016).

Igualmente, el espacio cibernético o digital que configuran el Internet y los distintos dispositivos que conforman el llamado "Internet de las cosas" y el fenómeno de la convergencia (Jenkins, 2006), es reconocido como un nuevo escenario y medio para implementar la guerra a nivel nacional y transnacional, reduciendo los riesgos a los que se exponen ciertos principios del DIH y los DH en la guerra convencional (Bradley, 1998; Arkin, 1999; Lewis, 2002; Cyrus, 2007; Kelsey, 2008; Foester, 2016).

De esta forma, las entidades encargadas de investigar, judicializar y penalizar el delito informático pueden ajustar las tipificaciones de este delito en virtud de dar cumplimiento en las dos direcciones en las cuales se gestiona el riesgo de ataques cibernéticos, a saber, hacia la seguridad y defensa nacional y, hacia la protección de derechos sociales y económicos (Ibrahim, 2016). De igual forma es de importancia para Colombia crear y contar con los enlaces de cooperación, mediante estas instituciones, entre entidades destacadas en Ciberseguridad y Ciberdefensa en el país y en el exterior, con el propósito de desarticular organizaciones e individuos que ponen en riesgo estos dos propósitos de la política en

seguridad y defensa digital en el país (Foester, 2016). Entonces, con esta propuesta se pretende impactar positivamente en los sectores civiles e institucionales, públicos y privados de Colombia.

A continuación resaltamos el papel de la FGN como institución encargada de la investigación y acusación de los presuntos infractores en delitos informáticos, ante los juzgados y tribunales correspondientes, y, formulamos la relevancia de la *priorización* y sus componentes -contexto, patrones de macro criminalidad y criterios subjetivos, objetivos y complementarios-, como parte de una política y herramienta judicial -criminal- que puede fortalecer los mecanismos de investigación interinstitucionales y, por ende, reducir las brechas existentes entre los registros de incidentes informáticos y la judicialización de los responsables.

2. La cibercriminalidad como un asunto social, político y judicial para el estado colombiano: el papel de la FGN y la priorización

Como parte de las instituciones democráticas que configuran el Estado Colombiano se consagra en la Constitución Política de Colombia, en el Título VIII que trata de la Rama Judicial, Capítulo 6 titulado 'De la Fiscalía General de la Nación' (FGN), la creación de esta entidad, que con autonomía administrativa y presupuestal debe asumir, en términos generales, la obligación de "adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo". (Corte Constitucional, 1991, Art., 250). Para este efecto la entidad debe:

> 1. Solicitar al juez que ejerza las funciones de control de garantías las medidas necesarias que aseguren la comparecencia de los imputados al proceso penal, la conservación de la prueba y la protección de la comunidad, en especial, de las víctimas [...]; 2. Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones [...]; 3. Asegurar los elementos materiales probatorios, garantizando la cadena de custodia mientras se ejerce su contradicción [...]; 4. Presentar escrito de acusación ante el juez de conocimiento, con el fin de dar inicio a un juicio público, oral, con inmediación de las pruebas, contradictorio, concentrado y con todas las garantías [...]; 5. Solicitar ante el juez de conocimiento la preclusión de las investigaciones cuando según lo dispuesto en la ley no hubiere mérito para acusar; 6. Solicitar ante el juez de conocimiento las medidas judiciales necesarias para la asistencia a las víctimas, lo mismo que disponer el restablecimiento del derecho y la reparación integral a los afectados con el delito; 7. Velar por la protección de las víctimas, los jurados, los testigos y demás intervinientes en el proceso penal [...]; 8. Dirigir y coordinar las funciones de Policía Judicial que en forma permanente cumple

la Policía Nacional y los demás organismos que señale la ley; 9. Cumplir las demás funciones que establezca la ley. (Corte Constitucional, 1991, Art., 250)

De este modo, se afirma que la FGN asume responsabilidad penal y judicial que, traducida en el ámbito de las asignaciones constitucionales, corresponde a una función política, pues permite el ejercicio de una democracia articulada mediante la creación de instancias -judiciales y penales- pertinentes para la conformación de una *sociedad del conocimiento* y para la instauración de un *gobierno electrónico* en términos democráticos (Ley N° 1341 de 2009).

En la primera parte de este capítulo se resalta la relación que existe entre la responsabilidad política y judicial de la FGN y las leyes y políticas que regulan en Colombia el delito informático, la ciberseguridad y ciberdefensa nacional (DNP, 2016). La segunda parte de este capítulo propone la pertinencia de una política y herramienta diseñada por la FGN, la *priorización,* para afrontar los desafíos sociales, políticos e investigativos judiciales- que plantea la cibercriminalidad a la seguridad y defensa nacional, y, por tanto, a la protección de derechos civiles, económicos y políticos que éstas implican.

2.1. La Fiscalía General de La Nación y el delito informático: una prioridad política y judicial

En Colombia la Constitución Política declara que "las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertadas, y para asegurar el cumplimiento de los deberes sociales del Estado y particulares" (Corte Constitucional, 1991, Art. 2). En el marco de estos fines políticos, que afirman contractualmente los derechos y deberes que deben asumir las instituciones y ciudadanos en este orden democrático, la FGN, en términos de protección judicial de estos derechos de los asociados, la Constitución no reclama que todos los delitos tengan que ser investigados simultáneamente ni con la misma celeridad, por el contrario, su actividad investigativa debe responder a los dos principios de la justicia distributiva y de la justicia como imparcialidad, a saber, el principio de igual libertad y, el principio de diferenciación o discriminación positiva (Osorio, 2010).

> Principio de igual libertad: "Cada persona ha de tener un derecho igual al más extenso sistema total de libertades básicas compatible con un sistema similar de libertad para todos". Principio de diferencia: "Las desigualdades sociales y económicas habrán de ser conformadas de tal modo que a la vez: a) se espera razonablemente que sean ventajosas para todos, y, b) se vinculen a empleos o cargos asequibles para todos." (Rawls [1997] Citado por Osorio, 2016, p. 151)

El primer principio postula la igualdad democrática como mecanismo político para acceder, en términos de una justicia equitativa o distributiva, a los derechos, bienes y servicios que ofrece una sociedad democrática y liberal que concibe la igualdad de condiciones como condición de posibilidad para el desarrollo económico, social y político.

El segundo principio, por su parte, si se quiere formula las condiciones políticas para la consecución de un ordenamiento democrático basado en la Justicia Social, que emerge de la capacidad de las personas, según su conciencia moral, de formar mecanismos de cooperación social voluntaria basada en un ordenamiento lexicográfico en el cual las libertades se encuentran en un ordenamiento superior a los bienes "secundarios" (Osorio, 2016, p. 151). De este modo, según los dos principios de una teoría de la justicia como imparcialidad y como equidad, que rigen la Carta Política en Colombia, el deber de protección que recae sobre las instituciones públicas deba ser ejercido en función de asegurar, por un lado, el acceso igualitario de los ciudadanos a las funciones judiciales y penales que desempeña la FGN y, al mismo tiempo, una diferenciación o discriminación positiva en virtud de los menos aventajados o de las víctimas, en el abordaje penal y judicial de un delito, que en este caso, corresponde al delito informático. Por tanto, el desempeño de las funciones de la FGN se encuentra bajo un modelo que exige el tratamiento igualitario de los procedimientos investigativos y simultáneamente la discriminación, según criterios basados en la vulneración o condición de vulnerabilidad o desventaja de las personas afectadas por ilícitos informáticos, se trata, en últimas, de cierto un examen de medios afines, que exige priorizar entre unos casos o demandas, sobre otros (FGN, Directiva N° 001 de 2012: p. 20). Así, afirma esta misma entidad que:

> [...] la adopción de un modelo de gestión judicial de la investigación penal soportado sobre la aplicación de unos criterios de priorización transparentes se ajusta a la cláusula constitucional del cumplimiento de los fines constitucionales, en tanto y en cuanto, permite racionalizar la actividad investigativa, y en esa medida, se está en presencia de un medio idóneo para alcanzar el fin. (FGN, Directiva N° 001 de 2012, p. 20)

De esta forma el Estado asegura, mediante esta institución, una administración de justicia en términos igualitarios, materializada en cuatro mandatos a cargo del Estado colombiano:

> (i) tratar de forma idéntica a ciudadanos que se hallen en iguales circunstancias; (ii) tratar de forma completamente diferente a destinatarios cuyas situaciones no compartan ningún elemento común; (iii) un mandato de trato paritario a personas cuyas situaciones presenten similitudes y diferencias, siendo más relevantes aquéllas que éstas (trato igual a pesar de la diferencia); y (iv) un mandato de trato diferenciado a destinatarios que se encuentren también en una posición, en parte similar y en parte diversa, pero cuyas diferencias sean más relevantes que las similitudes (trato diferente a pesar de la similitud). (FGN, Directiva Nº 001 de 2012, p. 20)

En este sentido, la jurisprudencia constitucional, de acuerdo con los dos principios de la justicia como imparcialidad y como equidad, ha considerado que la igualdad propone una doble dimensión inherente a la actividad investigativa y sancionatoria, una objetiva y otra subjetiva. Según aquella, emerge como un "mandato de optimización dirigido al legislador y a la administración, según la cual se deben proferir leyes y adoptar políticas públicas que garanticen, en la mayor medida posible, un trato igual entre los ciudadanos" (FGN, Directiva Nº 001 de 2012, p. 19). Y, según la dimensión subjetiva, "el ciudadano es titular del derecho a exigir un trato igualitario al momento de ejercer un derecho, tal y como sucede, por ejemplo, con el derecho fundamental de acceso a la administración de justicia" (Directiva 001 de 2012: p. 19)

> En este orden de ideas, la concreción del derecho fundamental de acceso a la administración de justicia en condiciones de igualdad le impone al Estado en general, y a la Fiscalía General de la Nación en particular, el deber de adoptar instrumentos de política criminal que permitan acordar un trato diferente entre demandas ciudadanas de justicia distintas. Lo anterior por cuanto ni todos los delitos presentan el mimo

> impacto social, gravedad o relevancia, ni todos los reclamantes de justicia se encuentran en la misma posición. (Directiva 001 de 2012: p. 19)

De manera que desde la perspectiva política, constitucional legislativa, la adopción e implementación de "criterios racionales, transparentes y democráticos de priorización para la atención de casos, antes que vulnerar el derecho fundamental de acceso a la administración de justicia en condiciones de igualdad, configura un medio justificado e idóneo para garantizarlo", pues se ajustan a los susodichos principios de la justicia como imparcialidad y equidad y, por ende, garantiza un derecho reconocido por la Carta Política colombiana. Por el contrario, brindar "idéntica atención a peticiones de justicia diferentes constituye, eso sí, un desconocimiento del derecho a la igualdad" (Directiva 0001 de 2012: p. 19), en términos de una justicia equitativa, es decir, política y judicialmente correcta. Del mismo modo, esta Directiva de la FGN establece que el derecho fundamental de acceso a la administración de justicia (Corte Constitucional, 1991, Art. 229) no es absoluto (Sentencia C-652 de 1997; Sentencia C-1195 de 2001), sino que, como lo anotó la Corte, se encuentra bajo las condiciones y limitaciones del aparato encargado de administrar justicia y, por el contrario, deben considerarse, diseñarse y ejecutarse ciertos criterios de priorización, que de un modo eficiente y eficaz establecería las condiciones bajo las cuales se ejecutan las actividades investigativas y penales que realiza la FGN (FG; Directiva N° 001 de 2012, p. 20-21). Estos criterios deben garantizar los derechos que subyacen al derecho fundamental de acceso a la administración de justicia, a saber:

> (i)la existencia en el ordenamiento jurídico, de diversos mecanismos judiciales -acciones y recursos- para la efectiva resolución de los conflictos; (ii) la posibilidad de acción o de promoción de la actividad jurisdiccional, por parte de todo sujeto de ser parte en un proceso y de utilizar los instrumentos que allí se proporcionan para

> plantear sus pretensiones; (iii) el derecho a que la actividad jurisdiccional concluya con una decisión de fondo en torno a las pretensiones que han sido planteadas, y que se produzca dentro de un plazo razonable; (iv) el derecho a que existan procedimientos adecuados, idóneos y efectivos para la definición de las pretensiones y excepciones debatidas; (v) el derecho a que los procesos se desarrollen en un término razonable, sin dilaciones injustificadas y con observancia de las garantías propias del debido proceso. (FGN, Directiva N° 001 de 2012, p. 20)

Por consiguiente, atender de manera diferenciada las demandas y peticiones de administración de justicia, en virtud del abordaje judicial y penal de crimen cibernético, basado en la aplicación de "criterios[10] razonables como son, entre otros, la calidad de la víctima y del victimario, la gravedad de los hechos, la riqueza probatoria del caso y los patrones regionales de comisión de los delitos" (FGN, Directiva N° 001, 2012, p. 21), garantiza no solo el cumplimiento de los dos principios de una teoría de la justicia como imparcialidad y equidad, sino también el derecho de acceder a una justicia que trata de manera igualitaria y, al mismo tiempo, que distingue en virtud de la distribución de justicia en términos de eficiencia, de rentabilidad económica y, de garantía de derechos de los más vulnerables.

Siguiendo estos mismos propósitos, de naturaleza constitucional, la misma Corte Constitucional delega a la FGN, siguiendo los principios de autonomía judicial consagrados

---

[10] Entre los criterios de priorización que formula la FGN mediante la Directiva N°001 de 2012, se encuentran, primero, "los *subjetivos*, que se refieren a la calidad de la víctima y del victimario; segundo, los *objetivos*, que comprenden la representatividad del crimen, en tanto que éste permite ilustrar, de la mejor manera posible, (teniendo en cuenta las limitaciones del derecho penal), el horror y el impacto de los crímenes cometidos, así como facilita el manejo armónico e interconectado de los diferentes criterios; y, tercero, los *complementarios*, que se refieren a la disponibilidad de pruebas, el tiempo estimado de la investigación, la existencia de sospechosos y personas arrestadas, y cuestiones relacionadas con la protección de testigos, entre otras". (FGN, Directiva N°001, 2012, p. 15)

en los artículos 228 y 230 de la Constitución Política de Colombia, la facultad para formular directrices y establecer principios de unidad de gestión y jerarquía. (FGN, Directiva 0001 de 2012: p. 21). Estas directrices pueden referirse "aspectos fácticos o técnicos del proceso de investigación, así como a asuntos jurídicos generales de índole interpretativa, y pueden fijar prioridades, parámetros o criterios institucionales para el ejercicio de las actividades investigativas, así como designar unidades especiales para ciertos temas" (FGN, Directiva N° 001, 2012, p. 21). Esto es reafirmado por el Estado Colombiano mediante la sentencia C979 de 2005 y la C-1260 de 2005, según las cuales estas directrices "pueden enmarcarse dentro de los principios constitucionales que rigen la actuación de la Fiscalía General de la Nación, relativos a la unidad de gestión y jerarquía previstos en el numeral 3 del artículo 251 de la Carta, así como a su autonomía administrativa y presupuestal". (Directiva 0001 de 2012: p. 22). De manera que le corresponde a esta entidad establecer los criterios con base en los cuales administra de manera autónoma los recursos humanos, físicos y financieros destinados a garantizar, mediante procedimientos judiciales y penales, tanto la protección de derechos civiles y económicos, como la seguridad y defensa en el territorio nacional. En este mismo sentido, el Artículo 251 de la Constitución Política de Colombia establece que una de las funciones especiales del Fiscal General de la Nación, consiste en "*participar en el diseño de la política en materia criminal*" (Directiva 0001 de 2012: p. 22). Por esta razón adoptar políticas y herramientas que permitan la adecuada judicialización y penalización de crímenes informáticos, en razón de la emergencia de este tipo de crimen como parte del contexto social, histórico, político y militar, surge como imperativo judicial y político de esta entidad, pues mediante estos mecanismos se garantizan derechos fundamentales (v.gr.: derecho a la igualdad, derecho a la diferencia y, en los mismos términos, derecho al acceso a la administración de justicia y a la judicialización de delitos que, como el delito informático,

exponen derechos civiles, económicos y políticos fundamentales). De esta forma se afirma que el diseño de la política criminal del Estado Colombiano hace parte de un proyecto democrático en el cual esta no representa un monopolio del Congreso de la República, sino que compete a distintas entidades o instituciones públicas encargadas de diseñar e implementar la política de seguridad y defensa informática en términos de gestión del riesgo que esto atañe (DNP, 2016).

Esta facultad que recae en la FGN con respecto a la determinación de prioridades, parámetros o criterios institucionales para la ejecución de actividades investigativas y de la designación de unidades especiales para ciertos temas, según esta directiva (FGN, Directiva N° 001 de 2012, p. 22), no se encuentra limitada al ámbito exclusivo de la justicia transicional, por cuanto, tal facultad deriva "de una interpretación sistemática y teleológica de diversas disposiciones constitucionales, hermenéutica que encuentra además soporte en la jurisprudencia constitucional" (FGN, Directiva N° 001, 2012, p. 23). Por lo tanto, esta política y herramienta puede emplearse en el ejercicio de actividades investigativas que, según los tratados y convenios internacionales y la emergencia social e histórica de determinados crímenes, como el crimen informático, resultan como prioridad en términos de justicia social, pero también, de garantía y acceso a la protección de derechos civiles, económicos, políticos y militares que se movilizan mediante las TIC's.

2.2. La priorización como política criminal y herramienta de ciberseguridad y ciberdefensa: priorizando en seguridad, defensa y protección de derechos civiles, políticos y económicos

Según el CONPES 3854 de 2016 (DNP, 2016, p. 24), se entiende la gestión de riesgos de seguridad digital como "el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades". Sin embargo, según este mismo documento, la FGN en materia de investigación jurídica se encuentra clasificada dentro de un nivel "formativo", pues "el número de fiscales capacitados para lograr construir un caso validado sobre pruebas electrónicas es limitado" (DNP, 2016, p. 42). En este sentido se deben "institucionalizar estos esfuerzos y ampliar mecanismos de colaboración entre la fiscalía y la policía, obteniendo de esta forma un apoyo en la resolución de casos de delitos cibernéticos" (DNP, 2016, p. 42). Con este fin reclama este documento que:

> Se debe encaminar a construir un marco jurídico maduro que apoye los procesos judiciales, juzguen conductas de manera efectiva, apoyen procesos de investigación estructural, y cuente con la capacidad de adaptarse dinámicamente en función de las circunstancias imperantes (DNP, 2016, p. 42).

Estas "circunstancias imperantes" reclaman, por consiguiente, un ejercicio administrativo de la justicia que tenga en consideración no solo los recursos humanos, físicos y financieros de la FGN, sino también la emergencia de grandes redes criminales y de crimen organizado que, mediante el uso de las TIC's, potencializan y amplían sus capacidades delictivas, que exponen, como ya se afirmó arriba, bienes y servicios que garantizan derechos fundamentales, en términos civiles, económicos y políticos.

> El crimen organizado ha escogido como una gran aliada a la tecnología, y en esa medida crimen y mundo digital se funden en una amalgama que, vista desde la perspectiva del riesgo del país, constituye una amenaza contra la seguridad nacional. Por tanto, es indispensable que en el país se dé un entendimiento claro de los fenómenos tales como el ciberlavado de activos, el ciberterrorismo, la ciberdelincuencia, el ciberespionaje o el cibersabotaje. (DNP, 2016, p.42-43).

En este mismo orden de ideas se reconoce que el aumento de estos tipos de comisiones criminales se encuentra relacionado con el "desconocimiento por parte de los administradores de justicia de la conducta criminal informática" (DNP, 2016, p. 43). De manera que la pertinencia de la herramienta política y judicial que representa la *priorización* se encuentra relacionada no solo con la garantizarían de un proceso de gestión y administración de los recursos financieros, humanos y físicos de la FGN, sino también con "las circunstancias imperantes" y, por tanto, con la emergencia de delitos que, como los informáticos, no cuentan con un abordaje conceptual y metodológico que permite a jueces y fiscales comprender, tipificar, judicializar y penalizar la comisión de estos delitos. De esta forma, los conceptos y métodos investigativos que formula la FGN mediante las Directivas N° 001 de 2012 y la N° 002 de 2015, representan una posibilidad que puede soslayar estos desafíos que se le plantean a esta entidad y, en sí, al Estado y el gobierno colombiano, no solo a nivel nacional sino internacional (CEPAL, 2010; UNODC, 2013; OEA, 2016).

De tal modo que la situación fáctica representativa de los patrones de conducta delictiva característicos de determinada organización criminal en el ámbito cibernético puede ser concebida, a partir de la *priorización*, mediante:

> (i) construir el respectivo contexto; (ii) acumular las actuaciones a cargo de la FGN que evidencien la existencia de la organización criminal y la ejecución de las conductas ilícitas que le puedan ser atribuidas a sus presuntos miembros, se trate o no

> de la misma clase de delito; y (iii) emplear los esquemas de imputación penal que resulten legalmente idóneos para investigar, y acusar a los presuntos máximos responsables, colaboradores y financiadores. (FGN, Directiva N° 001, 2012, p. 1)

De igual forma la FGN puede priorizar un caso no imputable a una organización delictiva, teniendo en cuenta que parte de los delitos informáticos son realizados por individuos no articulados a organizaciones delictivas que, no obstante, causan un impacto social, económico, e inclusive, político y militar, en términos de afectación de los derechos fundamentales de la víctima, de los bienes jurídicamente amparados o igualmente de su capacidad para develar la existencia de patrones culturales discriminatorios (FGN, Directiva N° 001, 2012, p. 3). En este sentido, la *priorización* además de permitir el discernimiento entre delitos informáticos en términos de la organización o el individuo que comenten delitos de tipo informático, facilita, mediante la elaboración de Contextos, la comprensión, no solo de la organización criminal y sus estructuras, sino de los marcos de referencia que develan "aspectos esenciales, acerca de elementos de orden geográfico, político, económico, histórico y social" en el que se realizan estos ilícitos por parte de grupos e individuos criminales, incluidos aquellos en los que servidores públicos y particulares colaboran con aquéllos (FGN, Directiva N°001 de 2012, p. 2). Este proceso debe "comprender una descripción de la estrategia de la organización delictiva, sus dinámicas regionales, aspectos logísticos esenciales, redes de comunicaciones y mantenimiento de redes de apoyo, entre otros" (FGN, Directiva N°001, 2012, p. 2). En síntesis, la elaboración del Contexto debe perseguir:

> (1) conocer la verdad de lo sucedido; (ii) evitar su repetición; (iii) establecer la estructura de la organización delictiva; (iv) determinar el grado de responsabilidad de los integrantes del grupo y de sus colaboradores; (v) unificar actuaciones al interior de la FGN con el fin de lograr esclarecer patrones de conducta, cadenas de mando fácticas y *de iure*; y (vi) emplear esquemas de doble imputación penal, entre otros aspectos. (FGN, Directiva N°001, 2012, p. 2)

Esto hace parte de las directrices y orientaciones formuladas en virtud de transformar los mecanismos investigativos empleados para el cumplimiento de las obligaciones constitucionales y legales a cargo de la FGN, maximizando el uso de la información y los recursos a su cargo (FGN, Directiva N° 001, 2012, p. 3). De este modo esta misma directiva establece que los fines de *la priorización* deben perseguir:

> 1. Seguridad Ciudadana: la posibilidad de asociar casos, a partir de la identificación de elementos comunes, permite combatir de manera más efectiva la criminalidad organizada; 2. Conocimiento del contexto de conflicto armado: la construcción de los escenarios delictivos en todas sus dimensiones es necesario para abordar procesos de justicia transicional; 3. Legitimidad y eficacia en la administración de justicia: la racionalización de los recursos de la FGN permite que se administre con eficacia y transparencia hacia la ciudadanía, lo que a su vez posibilita reducir la impunidad; 4. Atender las exigencias de la sociedad civil: los representantes de los distintos sectores de la sociedad han planteado la necesidad de estudiar la criminalidad en su contexto, para así desarticular de manera más efectiva a los grupos que vulneran gravemente los derechos humanos y que atentan contra sus defensores y defensoras. (FGN, Directiva N° 001 de 2012, p. 3)

Teniendo en cuenta que el delito informático representa riesgos para la seguridad ciudadana, que existen deficiencias en el conocimiento y la tipificación de este conjunto de delitos, que el crimen cibernético emerge como un espacio idóneo para la guerra y que se carece de herramientas que permitan conocer el contexto de su comisión, que además la FGN debe legitimar y hacer eficaz sus procedimientos investigativos, y, que esta misma entidad debe atender las demandas de la sociedad civil siguiendo principios de igualdad, diferencia y eficacia en la administración de sus recursos, la *priorización* se formula como una política que permite discernir entre delitos informáticos, y, por ende entre una prioridad investigativa y penal y otro, a partir de la construcción de *contextos, patrones criminales, modus operandi*

y estructuras criminales. En este sentido, *la* priorización se propone no solo como técnica de gestión de la investigación penal que permite establecer un orden de atención entre reclamos ciudadanos de justicia equivalentes, con el fin de garantizar, en la mayor medida posible, el goce del derecho fundamental de acceso a la administración de justicia", sino también como política crimina que permitiría, en este caso en particular, gestionar el riesgo de inseguridad cibernética, mediante la comprensión de un delito en permanente transformación y, que requiere de la intervención de distintas esferas civiles, institucionales públicas y privadas. En el marco de esta relevancia política y social, se reconoce además que, la técnica judicial de priorización de casos:

> "(i) se ajusta a los estándares internacionales de protección de los derechos humanos y del derecho internacional humanitario; (ii) se inspira en el funcionamiento de los tribunales penales internacionales, aunque tomando en cuenta que, por su naturaleza y razón de ser, la actividad de aquéllos implica, de por sí, un proceso de selección de casos; y (iii) encuentra referentes en el derecho comparado" (FGN, Directiva N°001, 2012, p. 4).

Esta concordancia con estándares internacionales de protección del DIH y de los DH se encuentra dada también en la medida en que la *priorización* se ajusta a los textos de la Convención Americana sobre Derechos Humanos y al Pacto Internacional de Derechos Civiles y Políticos, instrumentos normativos internacionales que hacen parte del llamado "bloque de constitucionalidad"; de igual forma se ajusta con la Corte Interamericana de Derechos Humanos, que constituye un "criterio relevante de interpretación" (FGN, Directiva N°001, 2012, p. 6). Así pues, se concluye que el delito informático, como un conjunto de delitos vinculados al uso de dispositivos que convergen en Internet como medio, plataforma y objetivo ilegítimo moral y jurídicamente, posee una naturaleza nacional y transnacional que

expone derechos y bienes civiles, sociales, económicos, políticos y militares, que deben ser abordados mediante herramientas jurídicas, investigativas y penales que permitan comprenderlo, y, consecuentemente judicializar y castigar a los ejecutores de estos crímenes (UNODC, 2013; OEA; 2016).

No obstante, reconoce la FGN (Directiva N°001, 2012, p. 9) que estas iniciativas legislativas internacionales, en materia de derechos humanos, pueden establecer dos limitaciones generales a la *priorización* de casos de delitos informáticos. La primera se deriva de la limitación en los esfuerzos de investigación que adelanta la FGN, pues esto puede implicar cierto descuido en procedimientos judiciales no priorizados por no afectar directamente principios del DIH y los DH. La segunda limitación se deriva de la exhortación al Estado colombiano a investigar violaciones del DIH y los DH, lo cual incluye la comisión de delitos internacionales. No obstante, la *priorización*, mediante el establecimiento de criterios *subjetivos, objetivos y complementarios* establece un orden lexicográfico que, priorizando el segundo de estos, permite evitar contradecir u omitir los instrumentos de derecho internacional. (Directiva N° 0001, 2012: p.9). Además, en el marco de la guerra cibernética, el terrorismo digital o el sabotaje se ha planteado un imperativo "convencional de enjuiciamiento o entrega de personas que han cometido infracciones graves a los Convenios de Ginebra" (FGN, Directiva N° 001, 2012, p. 9) como, por ejemplo, al afectar las infraestructuras críticas de un país, y por ende, al exponer o vulnerar los principios de distinción -entre civiles y objetivos militares- y neutralidad, consagrados en dicho convenio (Kelsey, 2008). Esta norma es llamada *aut dedere aut judicare*, y está consagrada en el artículo 49 del I Convenio de Ginebra, el artículo 50 del II Convenio de Ginebra, el artículo 129 del III Convenio de Ginebra y el artículo 146 del IV Convenio de Ginebra de la siguiente forma (Directiva N° 001, 2012: p. 9). De este modo, en "el caso de violaciones de derecho

internacional humanitario aplicables al conflicto armado no internacional, existe un deber general, más no una obligación de investigación", razón por la cual la *priorización* permitiría, mediante la elucidación de los tres criterios -subjetivos, objetivos y complementarios, priorizar tanto en virtud del derecho internacional humanitario, como de los delitos informáticos cometidos en el marco de la jurisdicción judicial nacional. Estos mecanismos legislativos propios del DIH permiten entonces la priorización de determinados casos siempre y cuando las infracciones críticas a los mismos no permanezcan impunes (FGN, Directiva N°001, 2012, p. 10).

> Las infracciones graves están consagradas en cada Convenio de Ginebra, pero, de manera general, se limitan al homicidio intencional, la tortura o los tratos inhumanos, incluidos los experimentos biológicos; el hecho de causar deliberadamente grandes sufrimientos o de atentar gravemente contra la integridad física o la salud; y la destrucción y la apropiación de bienes no justificadas por necesidades militares y efectuadas a gran escala ilícita y arbitrariamente. (FGN, Directiva N°001, 2012, p. 10)

De manera que, siguiendo los criterios de priorización establecidos por la FGN, se establece que, según los objetivos, se debe determinar la *gravedad* de los efectos generados con la ejecución del crimen y, por tanto, la *importancia* de adelantar su investigación y judicialización efectiva (Directiva 0002 de 2015: p. 24). Dicha gravedad puede valorarse a partir de un análisis de la afectación de los bienes jurídicos penalmente amparados, mediante una indagación de:

> (i) del grado de afectación de derechos fundamentales individuales y/o colectivos; (ii) de la cantidad de víctimas afectadas; (iii) de los costos sociales producidos por los fenómenos criminales y las circunstancias que los determinaron (teniendo en cuenta elementos como los costos económicos; el impacto sobre un grupo o comunidad; la posible extinción de un grupo social étnico o político; la cuantía del daño generado

con la comisión del crimen; el seguimiento o interés que pueda tener sobre un caso o situación otras instancias estatales a nivel interno, tribunales internacionales o la opinión pública, entre otros); (iv) de a modalidad de comisión de los delitos, estudiando, entre otras cosas, si se identifican actos de violencia o patrones de sistematicidad orientados a asegurar la comisión de los crímenes; (v) del grado de protección dado por el legislador al bien jurídico afectado (teniendo en cuenta las penas establecidas en el Código Penal como referencia indicativa), y (vi) de la frecuencia con que es cometido el delito, por ejemplo, si se trata de actos delictivos reiterados o generalizados.

Cabe aclarar que los criterios de priorización deben ser entendidos y aplicados de manera articulada, pues estos deben valorar el *impacto* y la *dificultad* de adelantar la investigación y judicialización de los distintos hechos criminales, teniendo en cuenta los contextos *sociales, económicos* y *territoriales* en los que se desarrolla la acción penal. (FGN, Directiva 0002 de 2015: p. 23). De esta manera la priorización, en concordancia con el CONPES 3854 y las recomendaciones de la OCDE (2015), permite distinguir el objetivo de prosperidad económica y social de los objetivos de defensa y seguridad nacional en el entorno digital, pues facilita, mediante la implementación de estos criterios y sus correspondientes actividades investigativas y penales en materia de DIH y DH, comprender la naturaleza del delito específicamente cometido comprendido en contexto (DNP, 2016, p. 23). Esto quiere decir que una estrategia o política de seguridad digital no debe diseñarse solo para contrarrestar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (problema técnico) (DNP, 2016, p.23). La política debe incorporar de manera diferenciada el objetivo de prosperidad económica y social, en lugar de continuar tratando el riesgo de seguridad digital como un problema meramente técnico que necesita soluciones de la misma naturaleza, por el contrario este debe abordarse como un riesgo económico, social

y político que debe gestionarse en cualquier proceso de toma de decisiones que involucran necesariamente actividades de prevención y afrontamiento concertadas entre instituciones y organizaciones públicas y privadas, basadas en criterios de *priorización* legal y normativamente establecidos en consonancia con los distintos tratados y convenios internacionales que pretenden enfrentar la cibercriminalidad, en cuanto delito de naturaleza transnacional que desafía los marcos normativos anclados a los territorios nacionales y sus correspondientes jurisdicciones.

En conclusión, la *priorización* de casos, como política criminal y herramienta investigativa no contradice los tratados y convenios internacionales de protección de los derechos humanos, ni el derecho internacional humanitario, ni los convenios en materia de delito informático (FGN, Directiva N°001 de 2012: p.11). Por el contrario, mediante la *priorización* y sus herramientas conceptuales y metodológicas, como la elaboración de contextos, patrones y modus operandi, permiten distinguir elementos contextuales que, en cada caso o incidente informático en particular, permiten comprender la naturaleza del ilícito, de sus medios, escenarios y fines o intenciones, que pueden violar o vulnerar derechos, bienes y servicios civiles, económicos, políticos y militares, pues afectan de distinta manera en cada caso, principios como la libertad de expresión, la producción, distribución y consumo de bienes digitales, e inclusive, la estabilidad de infraestructuras que permiten brindar servicios como acueducto y alcantarillado, suministro energético, transporte público y movilidad, entre otros. En este sentido, se afirma que "una adecuada y más efectiva gestión de la investigación de casos en la FGN, encaminada a fortalecer el Estado Social y Democrático de Derecho, implica adoptar instrumentos de política criminal que permitan racionalizar, en función de la aplicación de unos criterios materiales de priorización, el orden de atención de las peticiones ciudadanas de justicia" (FGN, Directiva N°001, 2012), en materia informática o digital, pues

allí convergen distintos dispositivos que, conectados a Internet, permiten desarrollar económica, social y políticamente a un Estado moderno.

3. Propuesta para adoptar una herramienta metodológica de priorización, para los casos investigativos contra la cibercriminalidad en Colombia.

La propuesta para la Fiscalía General de la Nación, es adoptar una herramienta metodológica de priorización para las investigaciones criminales contra la cibercriminalidad, en atención a las conductas delictivas de los delitos informáticos y que atentan contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos, que entre otras cosas, es uno de los objetivos de la seguridad informática, es asegurar la continuidad del negocio, protegiendo uno de los activos más importantes de cualquier empresa, que es su información.

Herramienta que nos permitirá una articulación con las entidades comprometidas con la recepción y documentación de los incidentes informáticos, tales como: Grupo de Respuestas a Emergencias Cibernéticas de Colombia **ColCERT**; Comando Conjunto Cibernético del Comando General de las FF.MM. de Colombia **CCOC**; Centro Cibernético Policía **CCP**; Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**, con la Fiscalía General de la Nación **FGN**, para un abordaje conceptual y metodológico que permita con facilidad la comprensión de los delitos contra la cibercriminalidad, que se puedan tipificar, judicializar y penalizar la comisión de estos hechos punibles y no se queden en solo registro de incidentes y posible resiliencia de los mismos de las entidades requirentes, públicas o privadas, sin que se pueda judicializar, investigar y condenar a los presuntos responsables.

Dicho lo anterior, se hace necesario de la creación de una Mesa Técnica contra la Cibercriminalidad **MTCC**, la cual estaría integrada por:

- Delegado de la FGN, Fiscal Local, Seccional o Especializado.
- Perito Forense de la Fiscalía General de la Nación **FGN**.
- Perito Forense de la Dirección de Investigaciones Criminal e Interpol **DIJIN**.
- Policía Judicial de la Fiscalía General de la Nación **FGN**.
- Policía Judicial de la Dirección de Investigaciones Criminal e Interpol **DIJIN**.
- Delegado Comando Conjunto Cibernético del Comando General de las FF.MM. de Colombia **CCOC**
- Delegado Centro Cibernético Policía **CCP**
- Delegado Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**
- Delegado Grupo de Respuestas a Emergencias Cibernéticas de Colombia **ColCERT**.
- Delegado Ministerio de las TIC´s
- Asesores expertos en el tema.
- Invitados especiales (especialistas nacionales o extranjeros)

La anterior Mesa Técnica contra la Cibercriminalidad -**MTCC**-, podrá invitar, a otras entidades del Estado, privadas o públicas, de acuerdo con las necesidades o especialidades y temas puntuales a tratar, pero en principió funcionará como se nombró inicialmente.

Una vez instalada la **MTCC**, se procederá a la caracterización de los incidentes registrados, estableciendo políticas y dinámicas claras, que permitan identificar cuáles de ellas cuentan con evidencias digitales legalmente obtenidas, que se puedan tipificar como delito dentro del

marco legal colombiano, realizado este ejercicio, permitirá la creación de los protocolos para la obtención de información para la judicialización ante la Fiscalía General de la Nación, como también identificar las falencias en nuestro marco jurídicos de aquellas conductas que se podrían considerar como delito y no están dentro de nuestro código penal colombiano, de tal manera que se postulen para que sean incluidos como delitos informáticos, esto generará la facilidad para la adecuación del delito frente a cada uno de los incidentes reportados y le permita un mejor entendimiento a los señores jueces de garantías o de conocimiento, al momento que la Fiscalía General de la Nación realiza las imputaciones en los delitos informaticos en contra de los cibercriminales.

La caracterización en el marco de priorización de casos, de cada uno de los incidentes permitirá la creación de mapas de calor, identificando información de las diferentes tipologías, modus operandi, por ciudades, departamentos, genero, tipos de delitos, tipos de malware, los sectores más afectados, entre otros, generando la asociación de casos, priorización de uno o varios fenómenos ciberdelincuencia. Lo anterior, permitirá a la **MTCC**, generar estrategias y/o políticas desde el punto de vista de prevención contra la cibercriminalidad o la efectiva judicialización de los delitos cometidos por los cibercriminales, pero también, la creación de estrategias para unir esfuerzos y metodologías para adelantar las diferentes investigaciones del orden nacional y transnacional, en la obtención legal de evidencias electrónicas para su judicialización y llegar a condenar a los responsables de los delitos informáticos.

Hecho lo anterior, permitirá con claridad a las entidades receptoras que se encuentran en la **MTCC** de los incidentes informáticos, para entrar a definir los parámetros para solucionar los incidentes informáticos, identificar cuáles de ellos se pueden judicializar y cuáles quedan en seguimiento para proceder a realizar los reportes de primer respondiente y el manejo de los datos que se convertirán en evidencia digital y de esta manera se determine

con el marco legal vigente colombiano, la tipificación de un presunto delito cometido por los cibercriminales, permitiendo así la apertura de una o varias noticias criminales en la Fiscalía General de la Nación.

A continuación, se mostrará como el Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**, maneja el tema de registro de incidentes:

Ilustración 5Recepción Incidentes CSIRT – PONAL

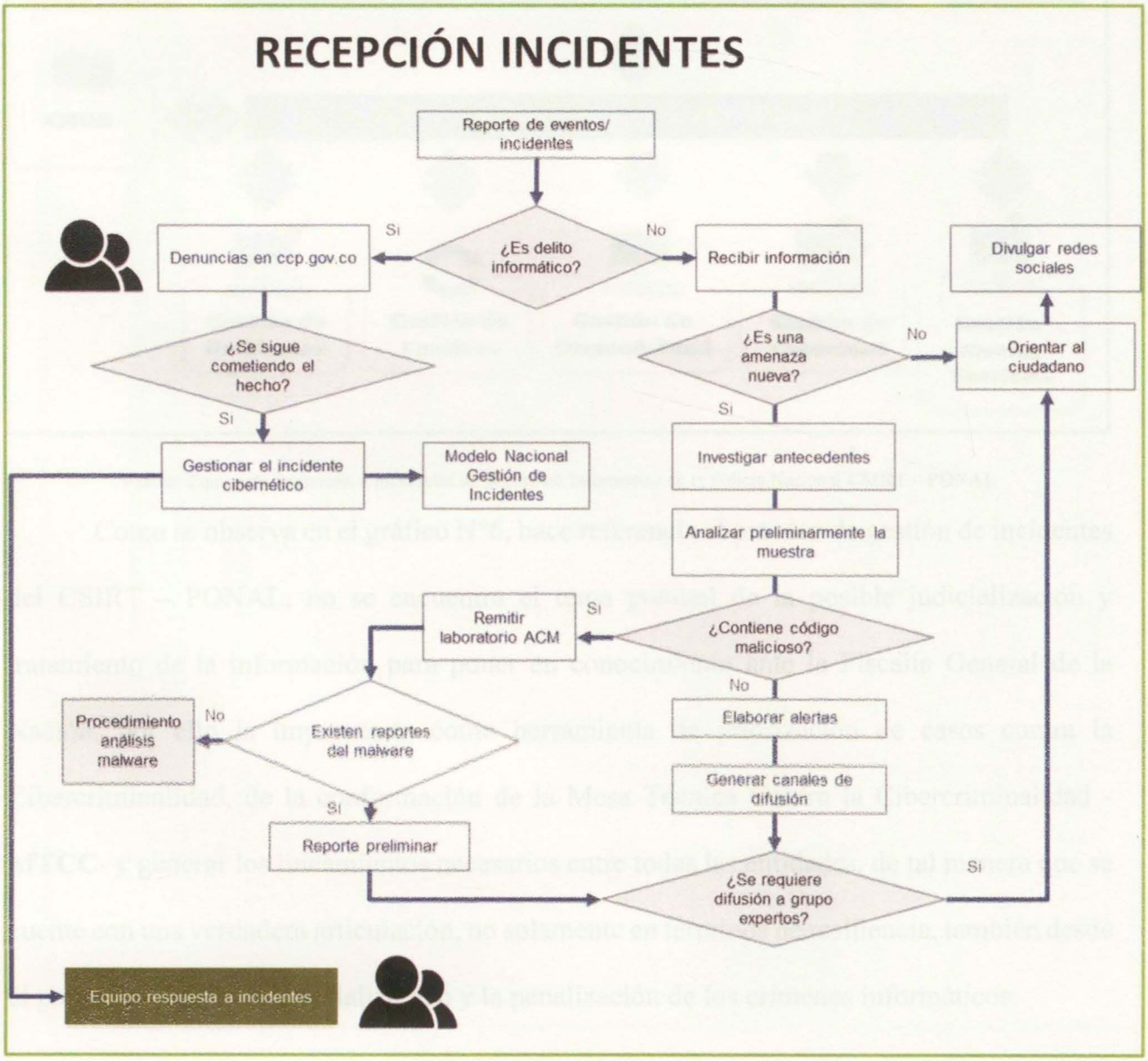
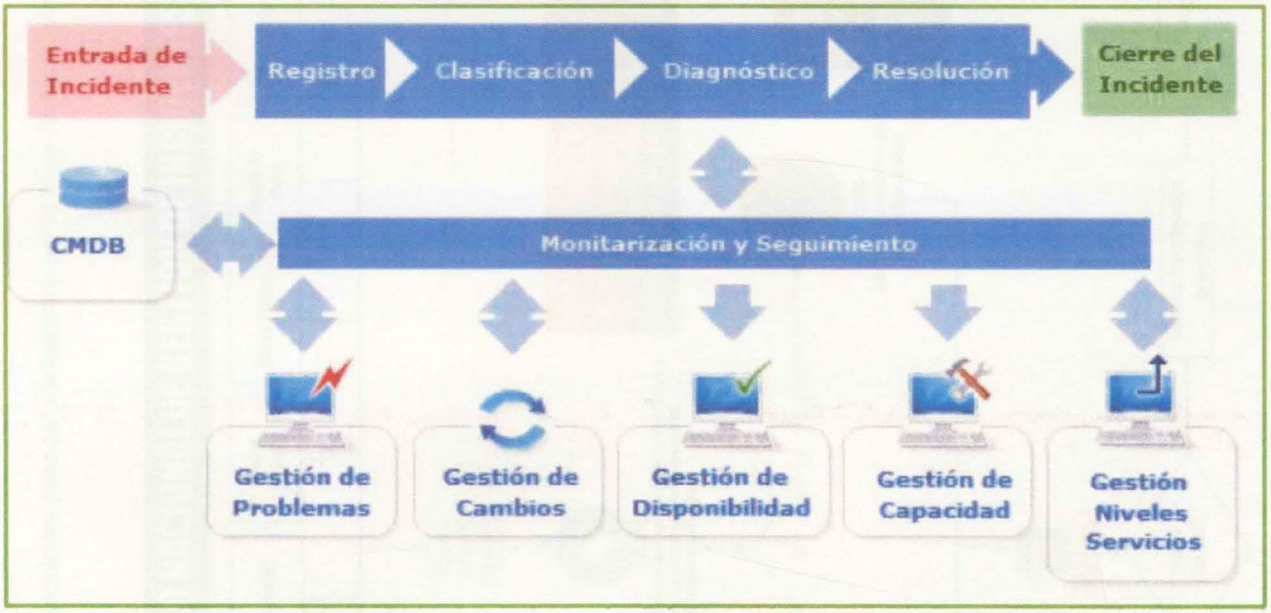


Gráfico N° 5. Recepción Incidentes por el Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL (2018)**

Fuente: Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**

PROCESO DE GESTIÓN DE INCIDENTES CSIRT – PONAL

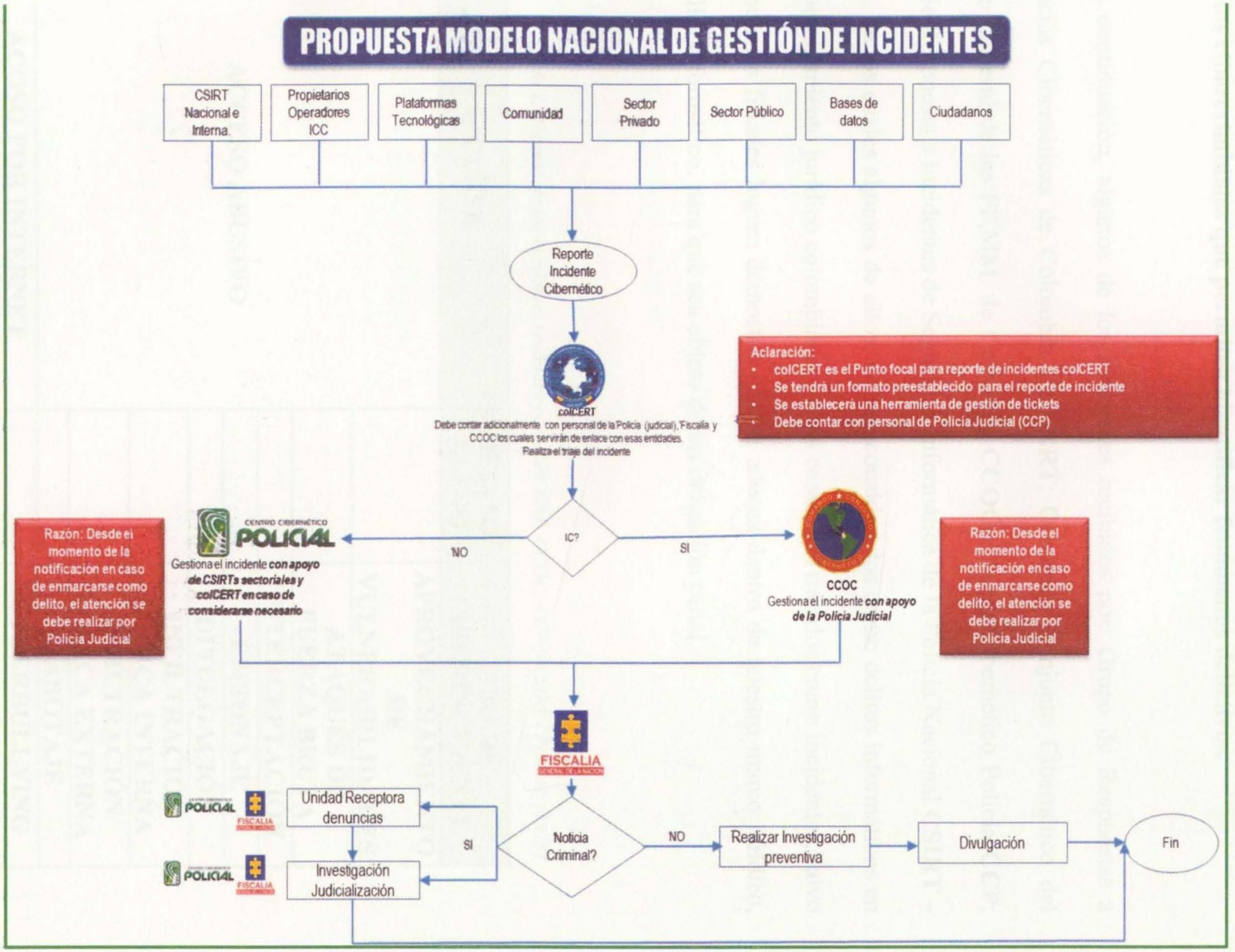
Ilustración 6Proceso de Gestión de Incidentes CSIRT – PONAL (2018)



Fuente: Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**

Como se observa en el gráfico N°6, hace referencia al proceso de gestión de incidentes del CSIRT – PONAL, no se encuentra el tema puntual de la posible judicialización y tratamiento de la información para poner en conocimiento ante la Fiscalía General de la Nación, por ello la importancia como herramienta de priorización de casos contra la Cibercriminalidad, de la conformación de la Mesa Técnica Contra la Cibercriminalidad - **MTCC**- y generar los lineamientos necesarios entre todas las entidades, de tal manera que se cuente con una verdadera articulación, no solamente en términos de resiliencia, también desde el punto de vista de la judicialización y la penalización de los crímenes informáticos.

Ilustración 7. Propuesta Modelo Nacional de Gestión de Incidentes, para que sea integrada por la Mesa Técnica Contra la Cibercriminalidad MTCC



3.1. Algunos incidentes que podrían ser considerados como delitos cometidos por los cibercriminales que permiten identificar fenómenos delictivos.

A continuación, algunos de los incidentes recibidos por: Grupo de Respuestas a Emergencias Cibernéticas de Colombia **ColCERT**; Comando Conjunto Cibernético del Comando General de las FF.MM. de Colombia **CCOC**; Centro Cibernético Policía **CCP**; Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional **CSIRT – PONAL**, de los cuales algunos de ellos, no son considerados como delitos informáticos en nuestro ordenamiento jurídico colombiano, así las cosas, son tratados como incidentes, salvo que los señores fiscales logren demostrar que se adecua dentro de nuestro marco jurídico, como delito informático, para que sea objeto de investigación penal.

Tabla 2. Algunos de los incidentes recibidos por: ColCERT; CCOC; CCP y CSIRT - PONAL [2018]

CLASE	DELITO SI / NO	TIPO DE CIBERINCIDENTE
ACCESO ABUSIVO		APROVECHAMIENTO DE VULNERABILIDADES
		ATAQUES DE FUERZA BRUTA
		INTERCEPTACIÓN
		ESPIONAJE
		DIVULGACIÓN
		INFILTRACIÓN LÓGICA INTERNA
		INFILTRACIÓN LÓGICA EXTERNA
		SABOTAJE
ACOSO POR INTERNET		CYBERBULLYING
CLONACIÓN TARJETA CRÉDITO		SKIMMING
CONTENIDO INDEBIDO WEB		CONTENIDO ILEGAL

CLASE	DELITO SI / NO	TIPO DE CIBERINCIDENTE
		CONTENIDO QUE PROVOCA PÁNICO
		CONTENIDO ABUSIVO
		INYECCIÓN DE CÓDIGO
DEFACEMENT		SQL INJECTION
		XSS/XCRF
		DEFACEMENT
		DEFACEMENT
DENEGACIÓN DE SERVICIO		AMPLIFICACIÓN DE DNS
		DENEGACIÓN DE SERVICIO
		NEGACIÓN DE SERVICIO
		DENEGACIÓN DE SERVICIO (DDoS)
ESTAFA POR INTERNET		TURINET
INGENIERÍA SOCIAL		INGENIERÍA SOCIAL
		INGENIERÍA SOCIAL
		VISHING
		SMISHING
INTENTO DE INTRUSIÓN		SNIFFER
		ESCANEO DE REDES
MALWARE		BACKDOOR
		SHELLCODE
		MALWARE
		SPAMBOOT
		BOTNET
		WORM (GUSANO)
		VIRUS (TROYANO)
		BOTNET
		CONTENIDO MALICIOSO

CLASE	DELITO SI / NO	TIPO DE CIBERINCIDENTE
		CÓDIGO MALICIOSO
		ADWARE: (SOFTWARE PUBLICITARIO)
		EXPLOIT
		GUSANO INFORMÁTICO
		RANSOMWARE
		SCAREWARE
		TROYANO
		VIRUS
		KEYLOGGER
		SPYWARE
		APT
		CRIMEWARE
		C&C
		SPAM-MALWARE
PHISHING		PHARMING
		PHISHING
		SPYWARE
		PHARMING
ROBO, PERDIDA Y/O ALTERACIÓN DE DATOS		ROBO DE DATOS
		PERDIDA DE DATOS
		ALTERACIÓN DE DATOS
		INFORMACIÓN COMPROMETIDA
SEXTING		SEXTING
SEXTORSIÓN		SEXTORSIÓN
SPAM		CARTA NIGERIANA

CLASE	DELITO SI / NO	TIPO DE CIBERINCIDENTE
SPAM-PHISHING		SPEAR PHISHING
SUPLANTACIÓN		SPOOFING
		SUPLANTACIÓN DE IDENTIDAD

Visto la anterior tabla N°2, podemos identificar que muchos de los incidentes que son solucionados por las agencias (ColCERT; CCOC; CCP y CSIRT – PONAL), en búsqueda de una adecuada resiliencia, muchos de ellos, no son considerados como conductas penales en nuestro ordenamiento jurídico colombiano, lo que hace complejo su judicialización, es por ello la importancia de la herramienta de priorización de articulación para los casos de investigación criminal contra la Cibercriminalidad y por otra parte, la propuesta que sean incluidos como delito informático como una actualización de la normatividad penal.

Como se observa a continuación del pantallazo, es la propuesta del CSIRT – PONAL, teniendo como criterio como servicio la atención a los incidentes con la filosofía de "restablecer la operación y mitigar el impacto causado", no el de judicializar los presuntos infractores a la Ley Penal de los delitos informáticos. Y que consultada la página web: https://cc-csirt.policia.gov.co/, en el link de "Nuestros servicios" encontramos la siguiente información:

Ilustración 8. Servicios Ofertados por CSIRT – PONAL

Fuente: Imagen tomada de la página web: https://ccsirt.policia.gov.co/Publicaciones/nuestros_servicios; [consultada agosto de 2019]

3.2. **Mapas de calor por departamento y denuncias por delitos informáticos para los periodos 2016, 2017, 2018 y enero a julio de 2019.**

Ilustración 9 Mapa de calor para el año 2016, denuncias recibidas por la FGN [sistema SPOA]

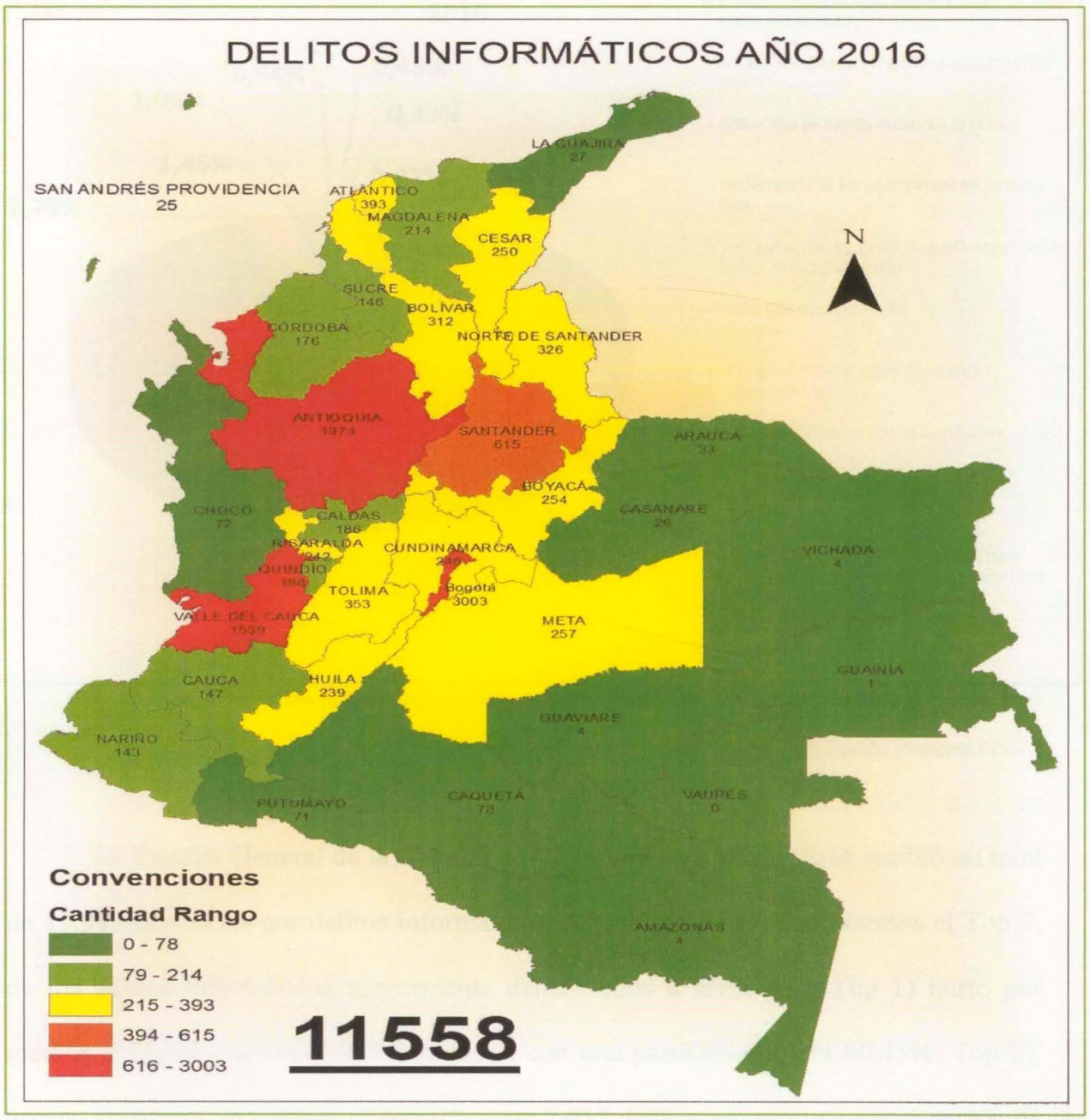
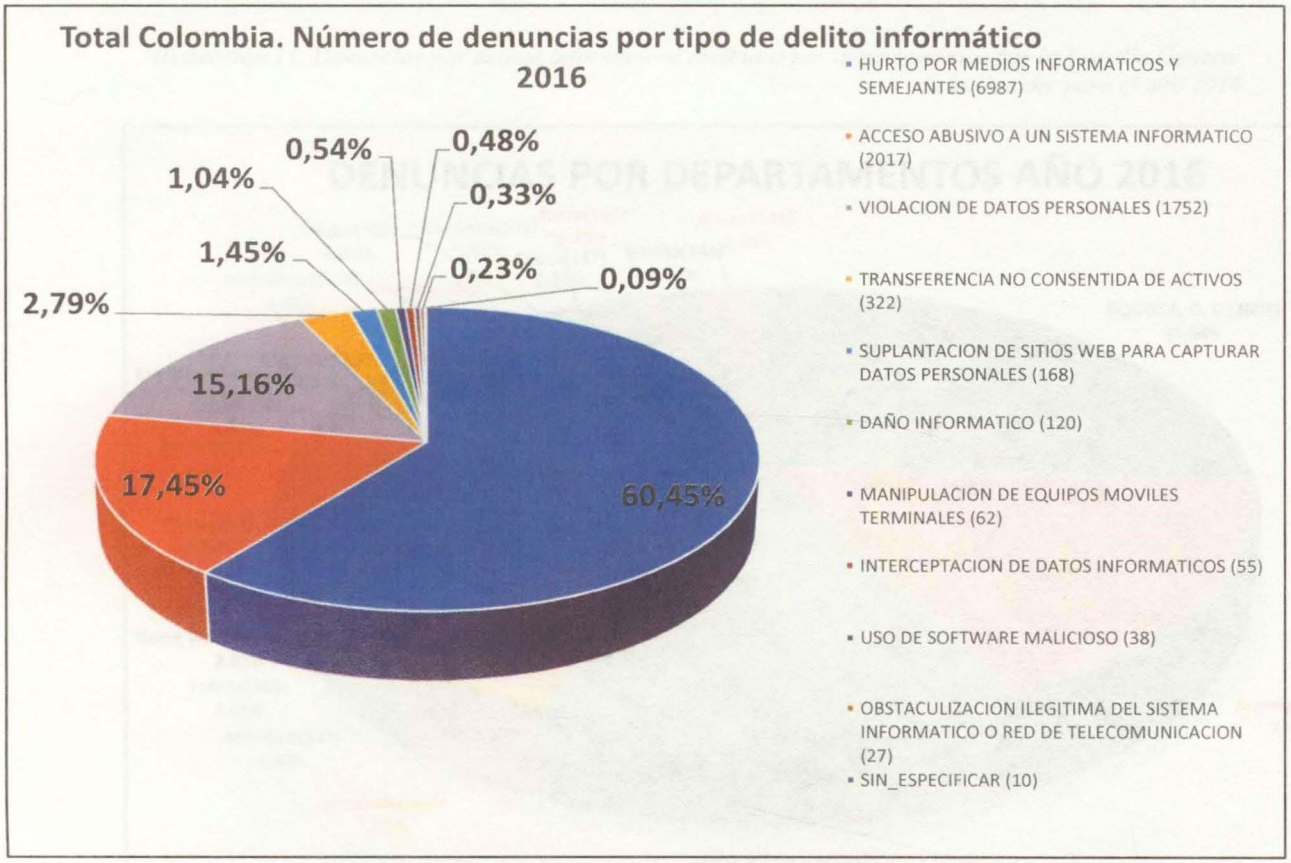


Ilustración 10 Denuncias por delitos informáticos, recibidas a nivel nacional por la Fiscalía General de la Nación, para el año 2016.

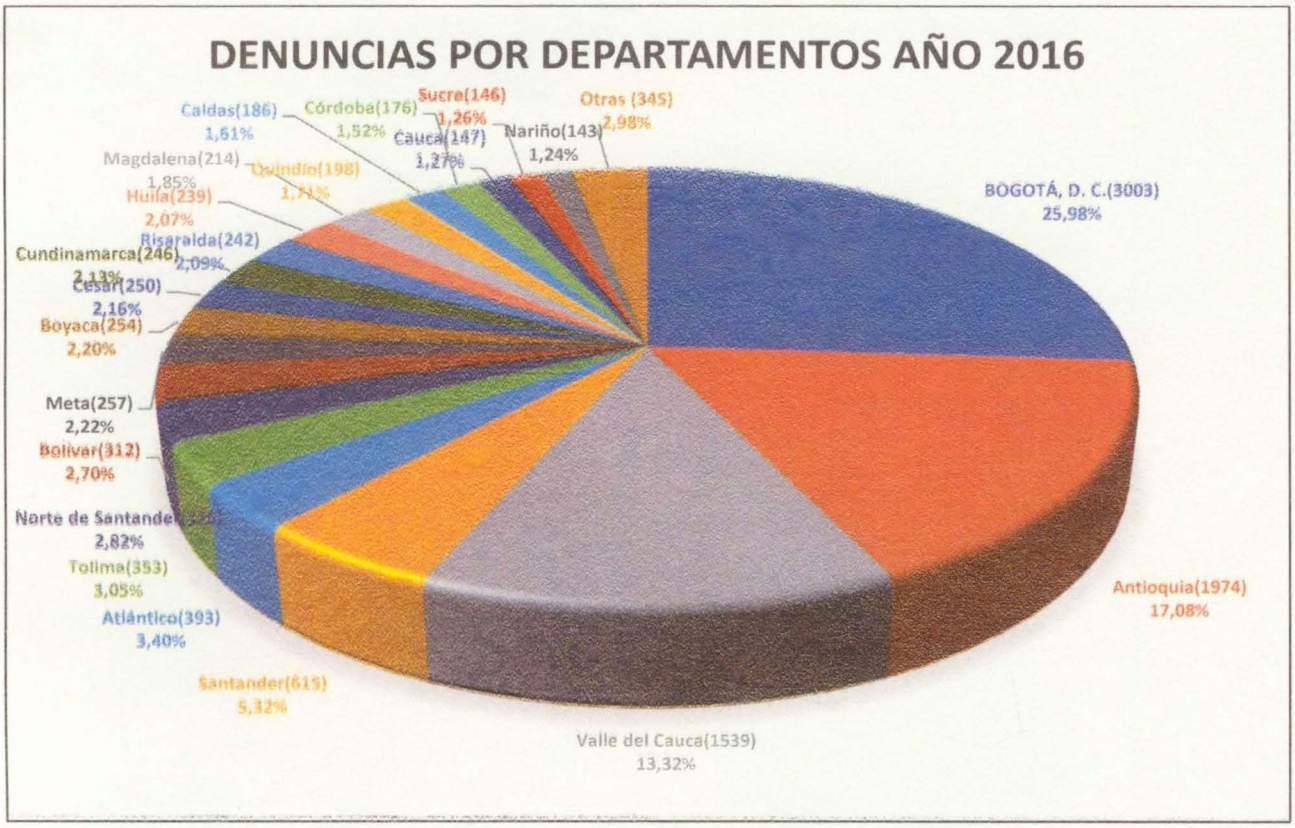


. Denuncias por delitos informáticos, recibidas a nivel nacional por la Fiscalía General de la Nación, para el año 2016. Fuente: Fiscalía General de la Nación [Sistema SPOA]

La Fiscalía General de la Nación, en Colombia para el año 2016 recibió un total de 11.585 denuncias por delitos informáticos. A continuación, nombraremos el Top 5, de los delitos informáticos mayormente denunciados a nivel país: Top 1) hurto por medios informáticos con 6.987 denuncias, con una participación del 60.45%; Top 2), acceso abusivo a un sistema informático con 2.017 denuncias, con una participación de 17.45%; Top 3) violación de datos personales con 1.752 denuncias, con una participación de 15.16%; Top 4) transferencia no consentida de activos con 322 denuncias, con una

participación de 2.79% y Top 5) suplantación de sitios web para capturar datos personales con 168 denuncias, con una participación de 1.45%.

Ilustración 11. Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el año 2016



Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el año 2016. Fuente: Fiscalía General de la Nación [Sistema SPOA]

En la gráfica N° 11, observábamos desde el punto de vista de denuncias por delitos informáticos dentro de nuestro ordenamiento jurídico, enunciando cuáles fueron los más representativos para el año 2016. En la gráfica N° 10, encontraremos las denuncias recibidas por la Fiscalía General de la Nación, por delitos informáticos por departamentos, incluyendo Bogotá D.C., para el año 2016. A continuación, nombraremos el Top 5 por departamentos: Top 1) la ciudad de Bogotá D.C. con 3.003

denuncias con una participación del del 25.98%; Top 2) Antioquia con 1974 denuncias con una participación del del 17.08%; Top 3) Valle del Cauca con 1.539 denuncias con una participación del del 13.32%; Top 4) Santander con 615 denuncias con una participación del del 5.32% y Top 5) Atlántico 393 denuncias con una participación del del 3.40%.

Ilustración 12. Mapa de calor para el año 2017, denuncias recibidas por la FGN [sistema SPOA]

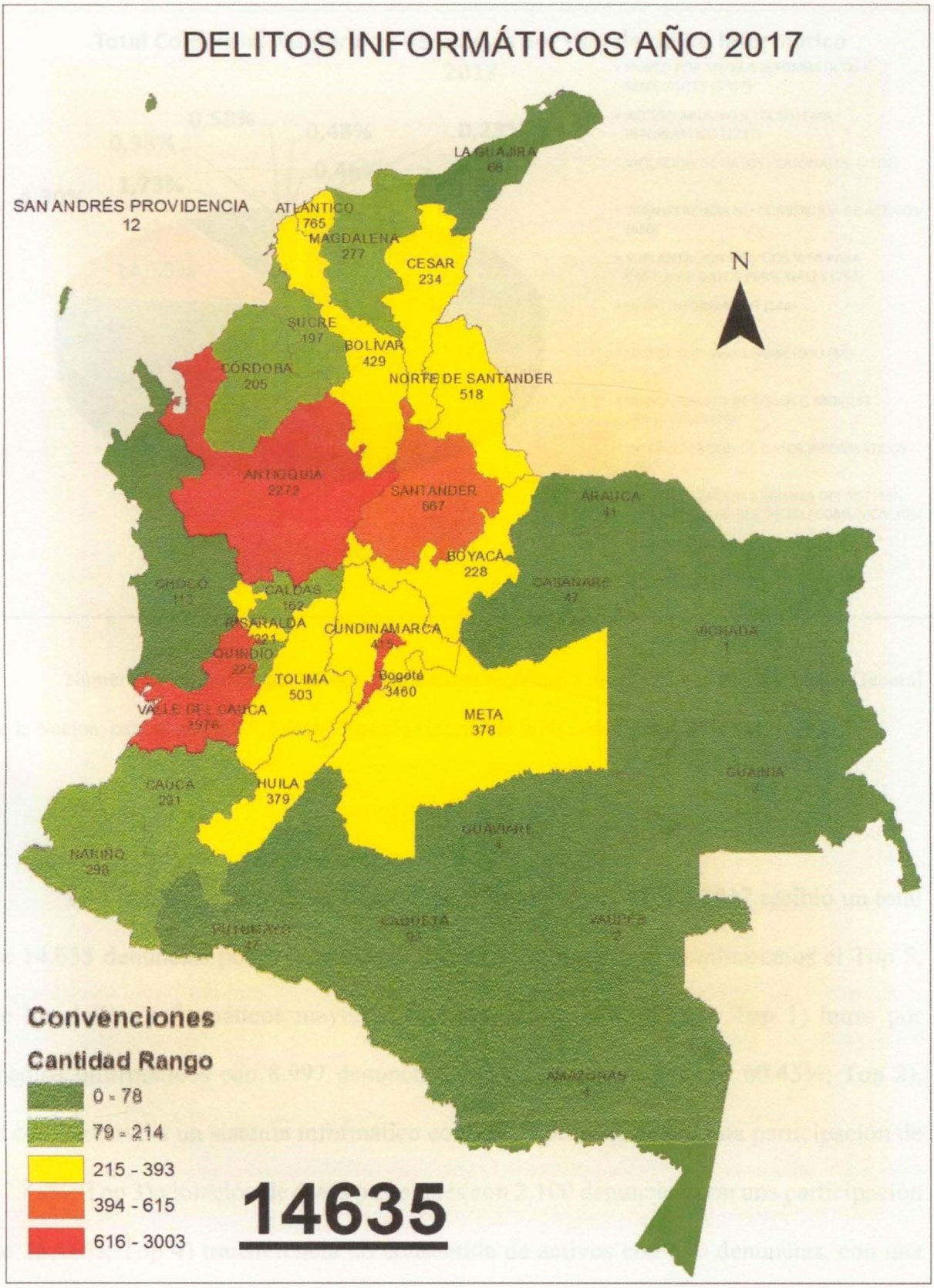
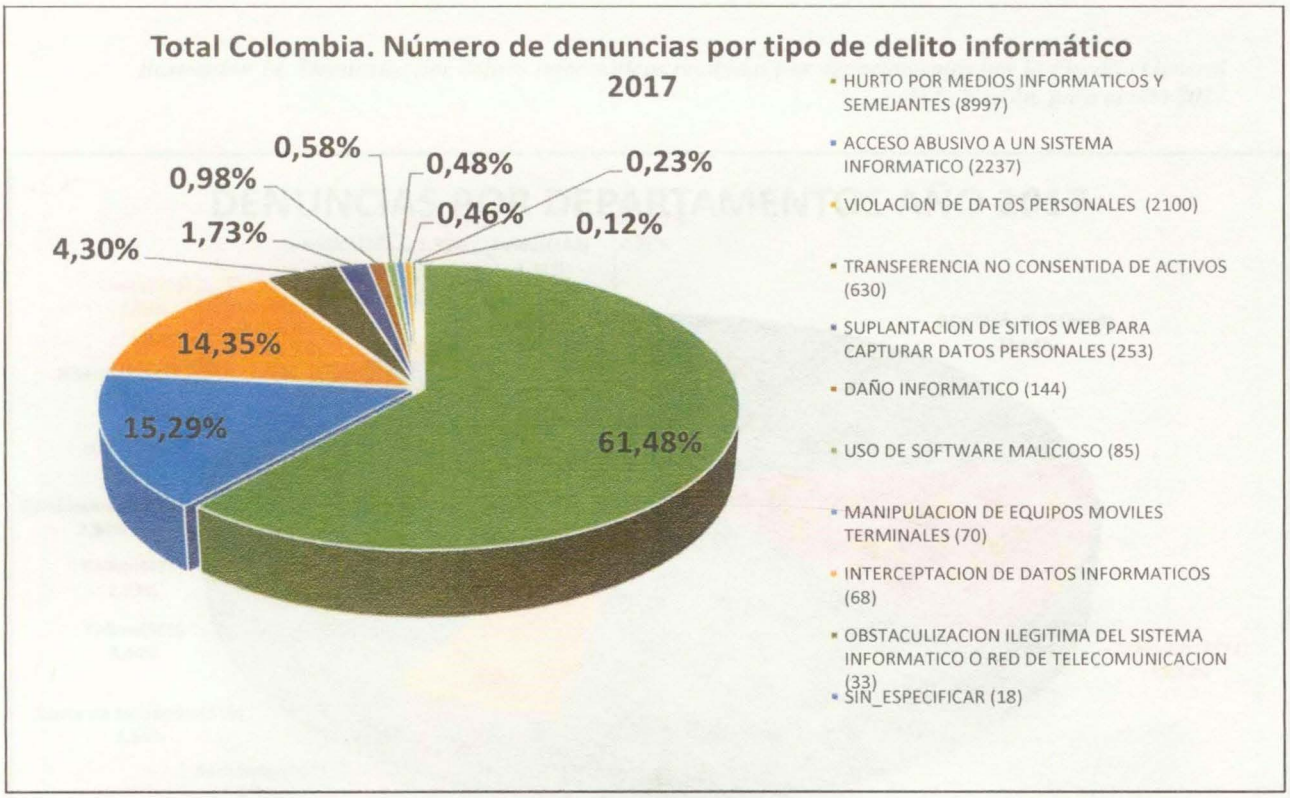


Ilustración 13. . Número de denuncias por delitos informáticos recibidas a nivel nacional por la Fiscalía General de la Nación, para el año 2017. Fuente: Fiscalía General de la Nación. [Sistema SPOA]

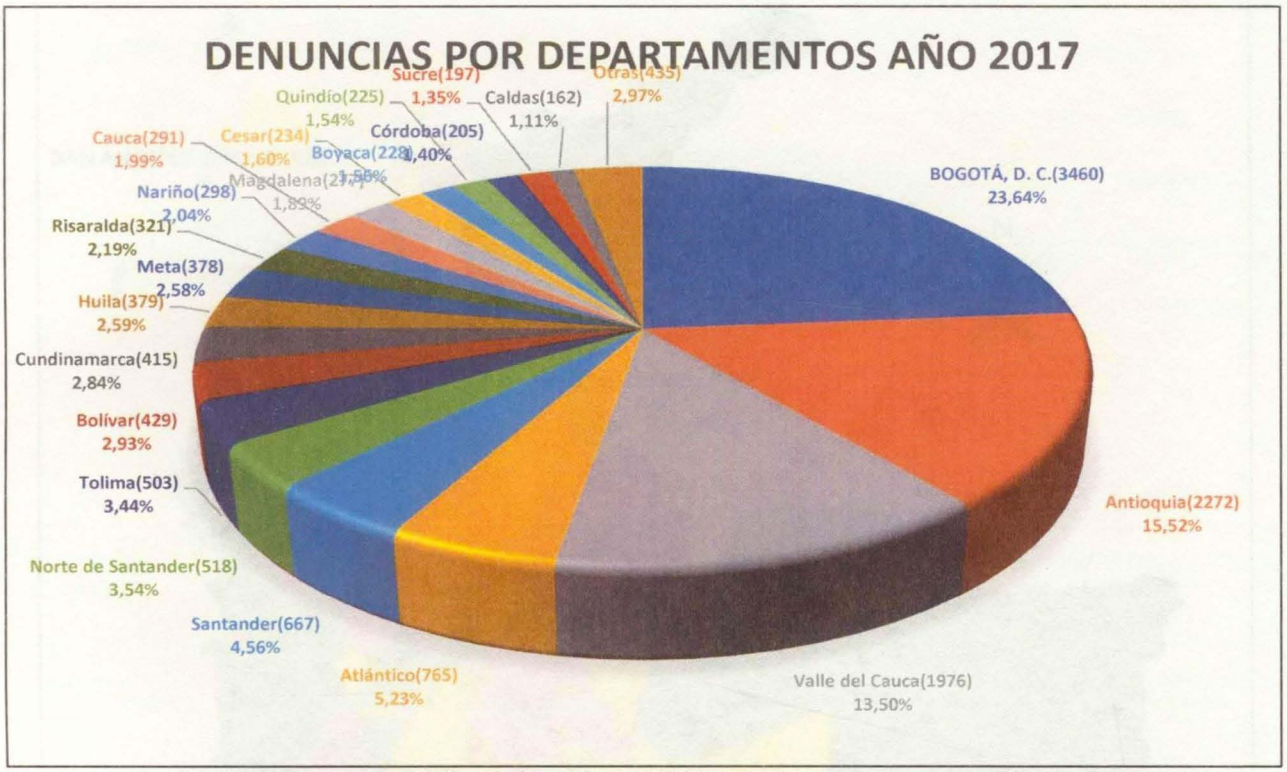


Número de denuncias por delitos informáticos recibidas a nivel nacional por la Fiscalía General de la Nación, para el año 2017. Fuente: Fiscalía General de la Nación. [Sistema SPOA]

La Fiscalía General de la Nación, en Colombia para el año 2017 recibió un total de 14.635 denuncias por delitos informáticos. A continuación, nombraremos el Top 5, de los delitos informáticos mayormente denunciados a nivel país: Top 1) hurto por medios informáticos con 8.997 denuncias, con una participación del 60.45%; Top 2), acceso abusivo a un sistema informático con 2.237 denuncias, con una participación de 17.45%; Top 3) violación de datos personales con 2.100 denuncias, con una participación de 15.16%; Top 4) transferencia no consentida de activos con 630 denuncias, con una

participación de 2.79% y Top 5) suplantación de sitios web para capturar datos personales con 253 denuncias, con una participación de 1.45%.

Ilustración 14. Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el año 2017



Grafica 14. Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el año 2017. Fuente: Fiscalía General de la Nación. [Sistema SPOA]

En la gráfica N° 14, observábamos desde el punto de vista de denuncias por delitos informáticos dentro de nuestro ordenamiento jurídico, enunciando cuáles fueron los más representativos para el año 2017. En la gráfica N° 13, encontraremos las denuncias recibidas por la Fiscalía General de la Nación, por delitos informáticos por departamentos, incluyendo Bogotá D.C., para el año 2017. A continuación, nombraremos el Top 5 por departamentos: Top 1) la ciudad de Bogotá D.C. con 3460 denuncias con una participación del del 23.64%; Top 2) Antioquia con 2.272 denuncias con una participación del del 15.52%; Top 3) Valle del Cauca con 1.976 denuncias con una participación del del 13.50%; Top 4) Atlántico con 765 denuncias con una participación del del 5.23% y Top 5) Santander 667 denuncias con una participación del del 4.56%.

Ilustración 15. Mapa de calor para el año 2018, denuncias recibidas por la FGN [sistema SPOA]

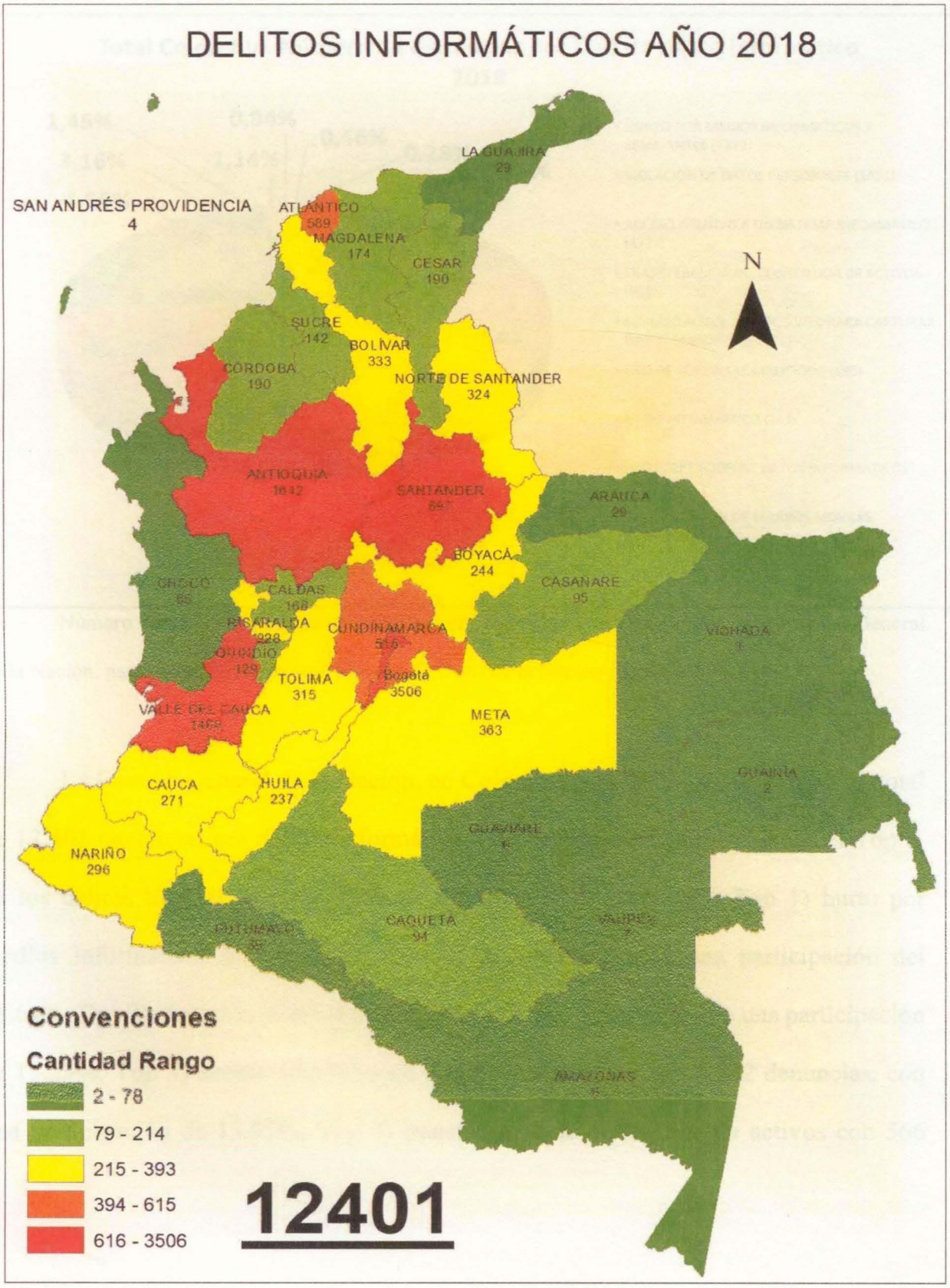
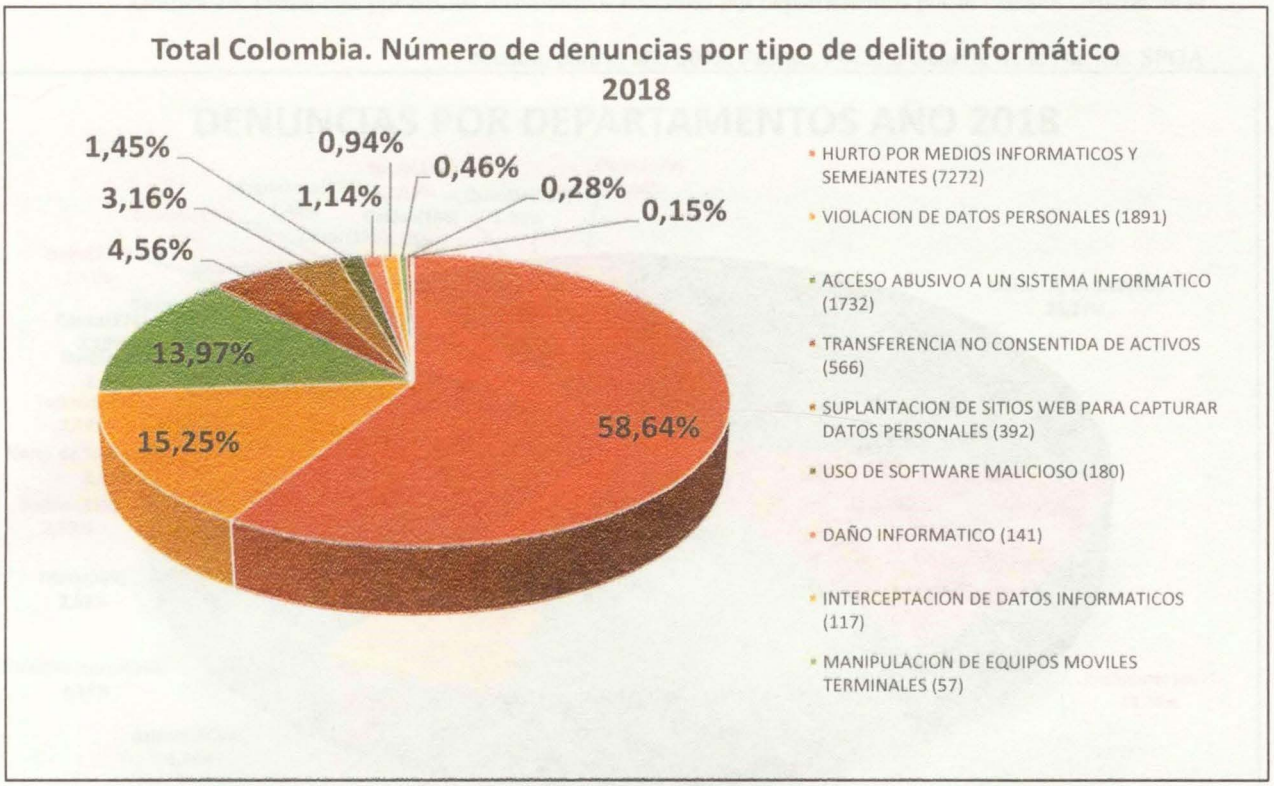


Ilustración 16. Número de denuncias por delitos informáticos recibidas a nivel nacional por la Fiscalía

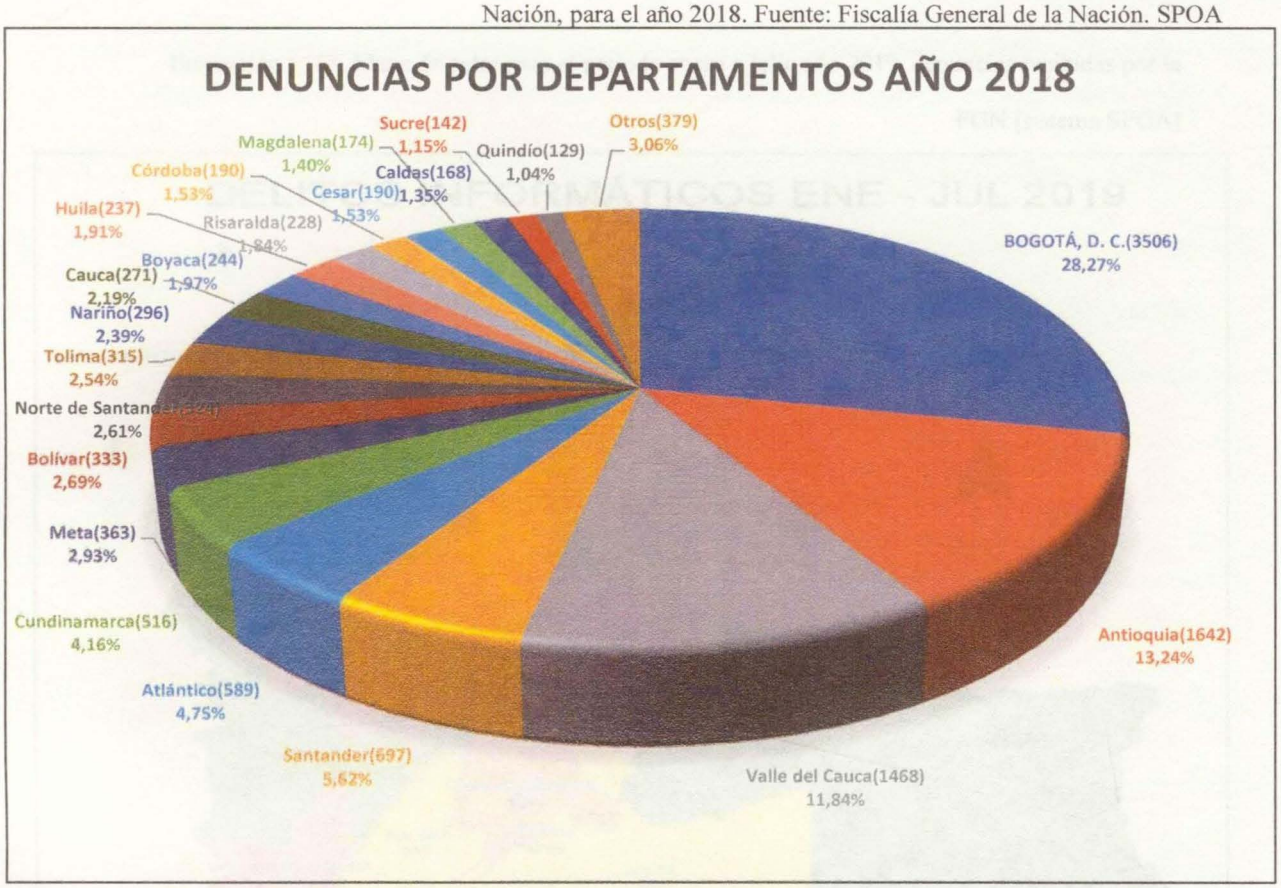


Número de denuncias por delitos informáticos recibidas a nivel nacional por la Fiscalía General de la Nación, para el año 2018. Fuente: Fiscalía General de la Nación [Sistema SPOA]

La Fiscalía General de la Nación, en Colombia para el año 2018 recibió un total de 12.401 denuncias por delitos informáticos. A continuación, nombraremos el Top 5, de los delitos informáticos mayormente denunciados a nivel país: Top 1) hurto por medios informáticos y semejantes con 7.272 denuncias, con una participación del 58.64%; Top 2) violación de datos personales con 1.891 denuncias, con una participación de 15.25%; Top 3) acceso abusivo a un sistema informático con 1.732 denuncias, con una participación de 13.97%; Top 4) transferencia no consentida de activos con 566

denuncias, con una participación de 4.56% y Top 5) suplantación de sitios web para capturar datos personales con 392 denuncias, con una participación de 3.16%.

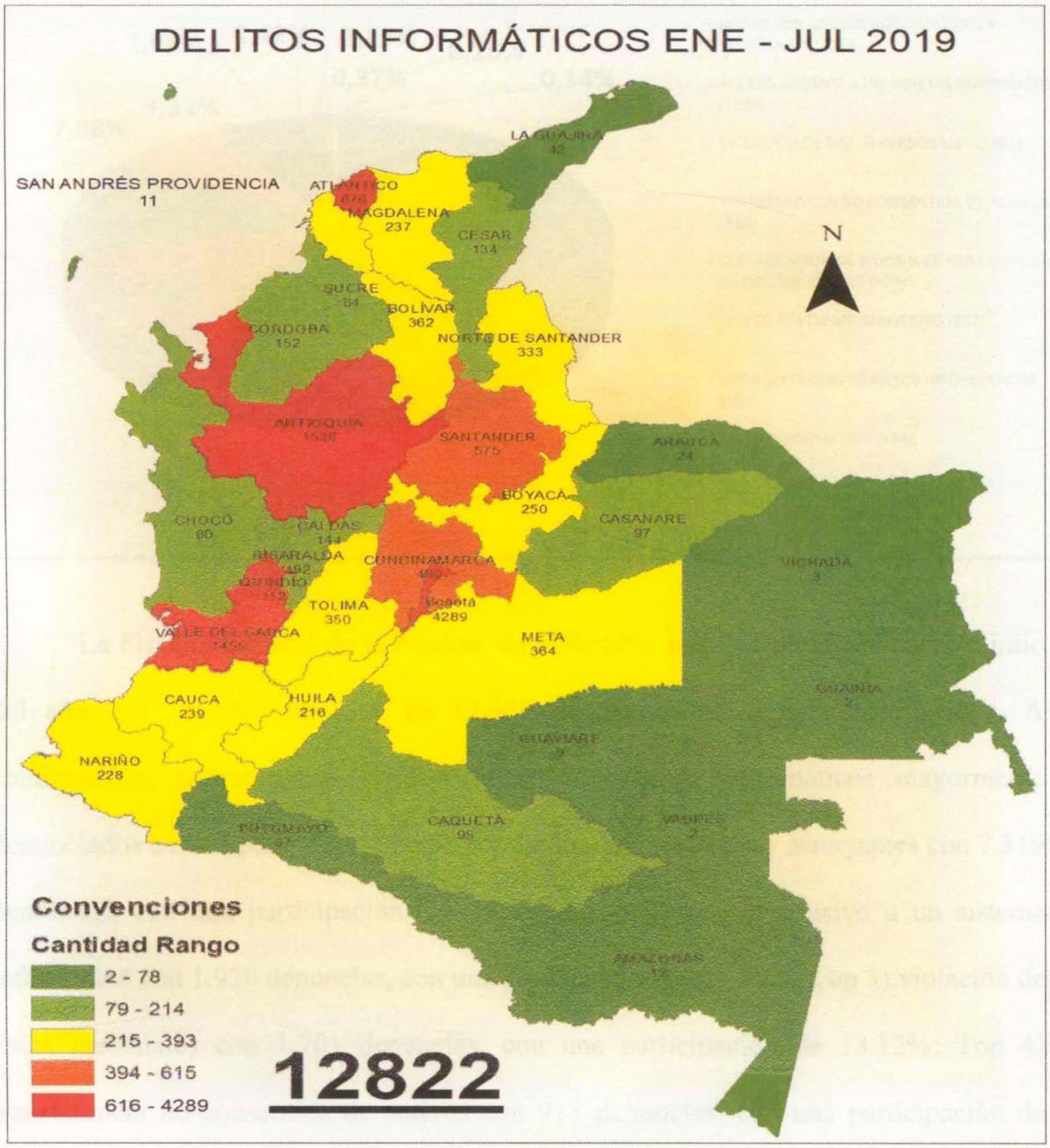
Grafica 16. Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el año 2018. Fuente: Fiscalía General de la Nación. SPOA



En la gráfica N° 16, observábamos desde el punto de vista de denuncias por delitos informáticos dentro de nuestro ordenamiento jurídico, enunciando cuáles fueron los más representativos para el año 2018. En la gráfica N° 16, encontraremos las denuncias recibidas por la Fiscalía General de la Nación, por delitos informáticos por departamentos, incluyendo Bogotá D.C., para el año 2018. A continuación, nombraremos el Top 5 por departamentos: Top 1) la ciudad de Bogotá D.C. con 3.506 denuncias con una participación del del 28.27%; Top 2) Antioquia con 1.642 denuncias con una participación del del 13.24%; Top 3) Valle del Cauca con 1.468 denuncias con una participación del del 11.84%; Top 4) Santander con 697 denuncias con una

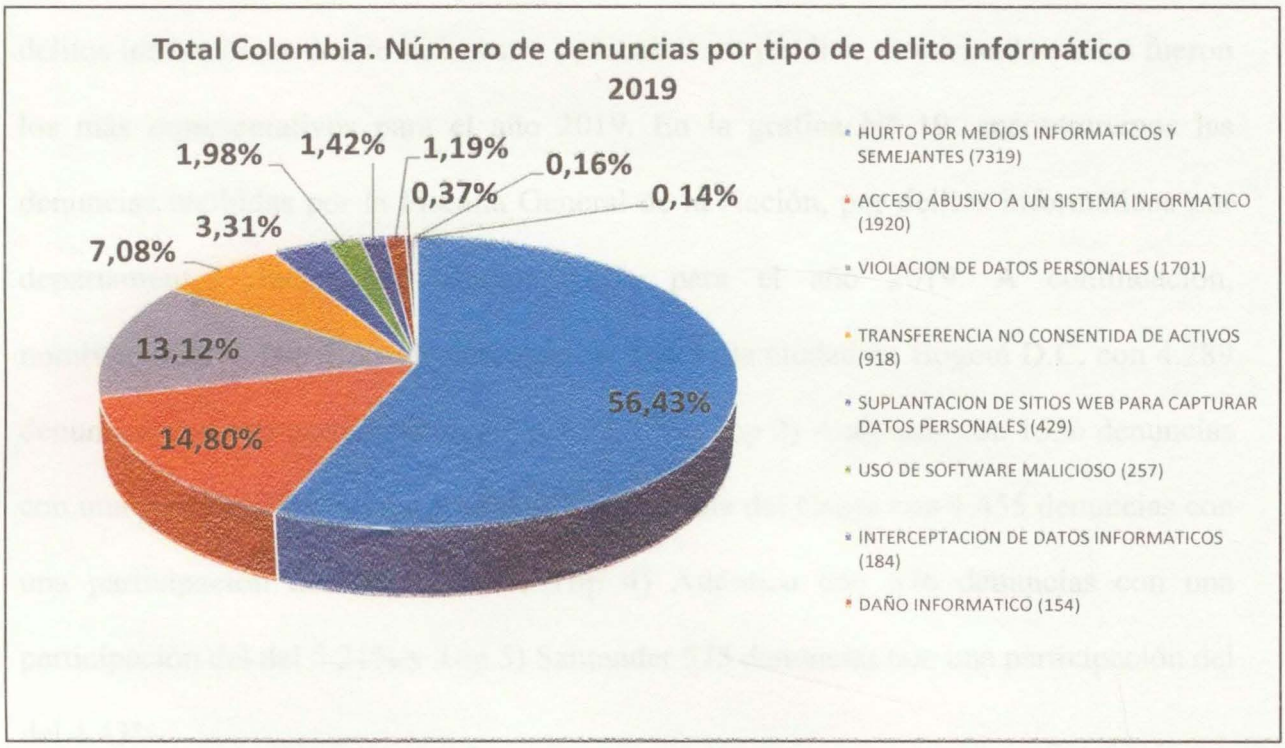
participación del del 5.62% y Top 5) Atlántico 589 denuncias con una participación del del 4.75%.

Ilustración 1748. Mapa de calor para el periodo enero a julio año 2019, denuncias recibidas por la FGN [sistema SPOA]



Mapa de calor para el periodo enero a julio año 2019, denuncias recibidas por la FGN [sistema SPOA]

Ilustración 18~~19~~. Número de denuncias por delitos informáticos recibidas a nivel nacional por la Fiscalía General de la Nación, para el periodo enero a julio del 2019. Fuente: Fiscalía General de la Nación. [Sistema SPOA]



La Fiscalía General de la Nación, en Colombia para los meses de enero a julio del año 2019 recibió un total de 12.969 denuncias por delitos informáticos. A continuación, nombraremos el Top 5, de los delitos informáticos mayormente denunciados a nivel país: Top 1) hurto por medios informáticos y semejantes con 7.319 denuncias, con una participación del 56.43%; Top 2) acceso abusivo a un sistema informático con 1.920 denuncias, con una participación de 14.80%; Top 3) violación de datos personales con 1.701 denuncias, con una participación de 13.12%; Top 4) transferencia no consentida de activos con 918 denuncias, con una participación de

7.08% y Top 5) suplantación de sitios web para capturar datos personales con 429 denuncias, con una participación de 3.31%.

En la gráfica N° 19, observábamos desde el punto de vista de denuncias por delitos informáticos dentro de nuestro ordenamiento jurídico, enunciando cuáles fueron los más representativos para el año 2019. En la gráfica N° 19, encontraremos las denuncias recibidas por la Fiscalía General de la Nación, por delitos informáticos por departamentos, incluyendo Bogotá D.C., para el año 2019. A continuación, nombraremos el Top 5 por departamentos: Top 1) la ciudad de Bogotá D.C. con 4.289 denuncias con una participación del del 33.07%; Top 2) Antioquia con 1536 denuncias con una participación del del 11.84%; Top 3) Valle del Cauca con 1.455 denuncias con una participación del del 11.22%; Top 4) Atlántico con 676 denuncias con una participación del del 5.21% y Top 5) Santander 575 denuncias con una participación del del 4.43%.

Ilustración 19~~20~~. Denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el periodo enero a julio del 2019. Fuente: Fiscalía General de la Nación. [Sistema SPOA]

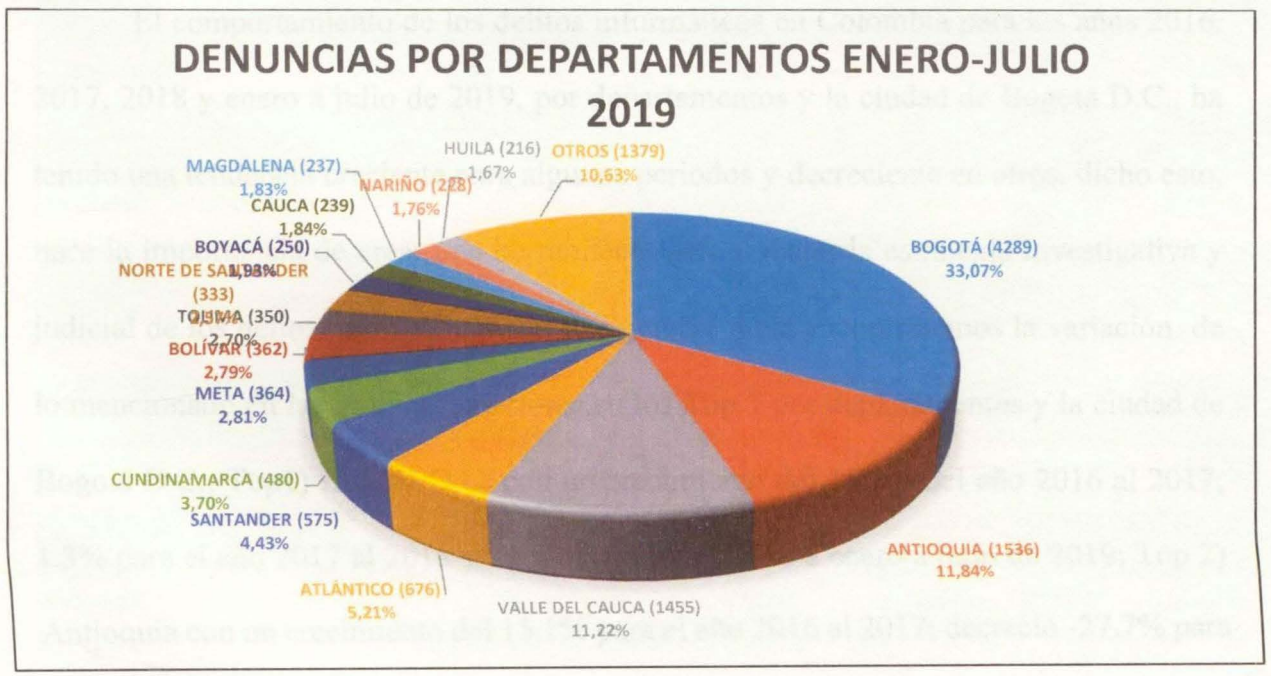
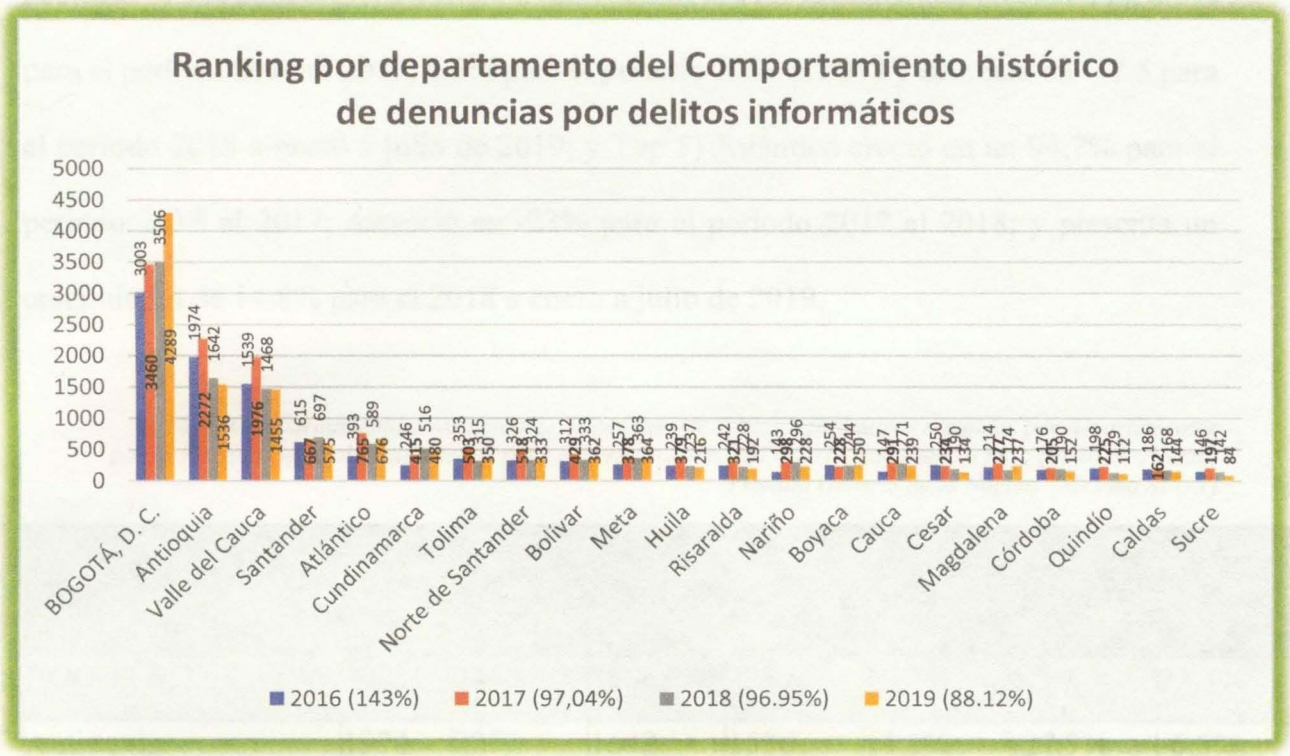


Ilustración 2021. . Rankin por departamentos del comportamiento de denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el periodo 2016, 2017, 2018 y de enero a julio del 2019. Fuente: Fiscalía General de la Nación. [



El comportamiento de los delitos informáticos en Colombia para los años 2016, 2017, 2018 y enero a julio de 2019, por departamentos y la ciudad de Bogotá D.C., ha tenido una tendencia creciente para algunos periodos y decreciente en otros, dicho esto, nace la importancia de crear una herramienta para trabajar la estrategia investigativa y judicial de los delios informáticos. En la siguiente tabla encontraremos la variación de lo mencionado en las gráficas anteriores en los Top 5 por departamentos y la ciudad de Bogotá D.C.: Top1) Bogotá D.C. con un crecimiento del 15.2% del año 2016 al 2017; 1.3% para el año 2017 al 2018 y un 22.3% para el 2018 a enero a julio de 2019; Top 2) Antioquia con un crecimiento del 15.1% para el año 2016 al 2017; decreció -27.7% para

2017 al 2018; y -6.5% para el 2018 a enero a julio de 2019; Top 3) Valle del cauca un crecimiento del 28.4% para el año 2016 al 2017; decreció el -25.7% para el 2017 al 2018; decreció -0.9% para el 2018 a enero a julio de 2019; Top 4) Santander creció en un 8.5% para el periodo 2016 al 2017; 4.5% para el periodo 2017 al 2018 y decreció en -17.5 para el periodo 2018 a enero a julio de 2019; y Top 5) Atlántico creció en un 94.7% para el periodo 2016 al 2017; decreció en -23% para el periodo 2017 al 2018; y presenta un crecimiento de 14.8% para el 2018 a enero a julio de 2019.

Tabla 3. Comportamiento y variación de denuncias por delitos informáticos recibidas por departamentos por la Fiscalía General de la Nación, para el periodo 2016, 2017, 2018 y de enero a julio del 2019. Fuente: Fiscalía General de la Nación. [Sistema SPOA]

DEPARTAMENTOS	2016 (143%)	2017 (97,04%)	2018 (96.95%)	2019 (88.12%)	Variación 2016-2017	Variación 2017-2018	Variación 2018-2019 ENE-JUL
BOGOTÁ, D. C.	3003	3460	3506	4289	15,2%	1,3%	22,3%
Antioquia	1974	2272	1642	1536	15,1%	-27,7%	-6,5%
Valle del Cauca	1539	1976	1468	1455	28,4%	-25,7%	-0,9%
Santander	615	667	697	575	8,5%	4,5%	-17,5%
Atlántico	393	765	589	676	94,7%	-23,0%	14,8%
Cundinamarca	246	415	516	480	68,7%	24,3%	-7,0%
Tolima	353	503	315	350	42,5%	-37,4%	11,1%
Norte de Santander	326	518	324	333	58,9%	-37,5%	2,8%
Bolívar	312	429	333	362	37,5%	-22,4%	8,7%
Meta	257	378	363	364	47,1%	-4,0%	0,3%
Huila	239	379	237	216	58,6%	-37,5%	-8,9%
Risaralda	242	321	228	192	32,6%	-29,0%	-15,8%
Nariño	143	298	296	228	108,4%	-0,7%	-23,0%
Boyaca	254	228	244	250	-10,2%	7,0%	2,5%

DEPARTAMENTOS	2016 (143%)	2017 (97,04%)	2018 (96.95%)	2019 (88.12%)	Variación 2016-2017	Variación 2017-2018	Variación 2018-2019 ENE-JUL
Cauca	147	291	271	239	98,0%	-6,9%	-11,8%
Cesar	250	234	190	134	-6,4%	-18,8%	-29,5%
Magdalena	214	277	174	237	29,4%	-37,2%	36,2%
Córdoba	176	205	190	152	16,5%	-7,3%	-20,0%
Quindío	198	225	129	112	13,6%	-42,7%	-13,2%
Caldas	186	162	168	144	-12,9%	3,7%	-14,3%
Sucre	146	197	142	84	34,9%	-27,9%	-40,8%
TOTAL	**11213**	**14200**	**12022**	**12408**			
Variación		**26,64%**	**-15,34%**	**3,21%**			

4. Conclusiones

El avance, la consolidación y emergencia de tecnologías de la información y la comunicación han traído consigo riesgos exponenciales en el entorno cibernético, informático o computacional. La gestión y prevención de este tipo de riesgos son señalados como una prioridad política, judicial y penal, tanto a nivel internacional como nacional por el tipo de derechos que se pueden encontrar vulnerados, así como por las pérdidas económicas que implica para los Estados, las organizaciones públicas y privadas o cualquier individuo que utilizan las TIC's como medio, plataforma y objeto de actividades comerciales, financieras, civiles, políticas, e incluso, militares.

Así las cosas, se hace necesario que la Fiscalía General de la Nación, despliegue la herramienta metodológica de priorización para las investigaciones en contra de los cibercriminales, y con el apoyo de otras entidades públicas y privadas la ejecución y puesta en marcha de la conformación de la Mesa Técnica Contra la Cibercriminalidad -**MTCC**- y generar los lineamientos necesarios entre todas las entidades.

En Colombia, a pesar de que se cuenta con un desarrollo legislativo y político en materia de ciberseguridad y ciberdefensa, se ha quedado obsoleto en el entendido que los cibercriminales utilizan nuevas metodologías y tecnologías cada día, quedándose corto el articulado actual en nuestro marco jurídico, ahora bien, teniendo en cuenta que la Ley 1273 de 2009 ya lleva diez años y está pendiente de actualización, según los juristas de nuestro país y docentes académicos de diferentes universidades.

De otro lado, se reconoce al mismo tiempo la necesidad de fortalecer los mecanismos investigativos, así como el fortalecimiento entre el soporte y apoyo interinstitucional, pero también transnacional e internacional, e inclusive, de modelos educativos que otorguen

herramientas a los individuos para prevenir ser víctimas de incidentes y delitos informáticos. En este mismo sentido Ibrahim (2016) afirma que existen tres factores que movilizan o motivan al cibercrimen: (1) socioeconómicos, (2) psicosociales y (3) geopolíticos. De esta forma plantea que el proceso de investigación que comprende las etapas de: conocimiento o registro del incidente; autorización; planificación; notificación; buscar e identificar evidencia; recolección de pruebas; transporte de pruebas; examen de la prueba; hipótesis; presentación de la hipótesis; defensa de la hipótesis; y, diseminación de la información, debe incluir un análisis de los elementos de orden social y económico, psicológico y geopolíticos pues permite superar las limitaciones que se reconocen en las definiciones o tipificaciones de un delito que puede variar de acuerdo al marco legal del país en el que se comete el crimen, así como del territorio desde el cual se ejecuta, o inclusive, que puede mutar de acuerdo a las innovaciones tecnológicas que pueden permitir la aparición de delitos informáticos no tipificados para el momento y el lugar del ilícito (UNODC, 2013).

La *priorización*, por tanto, entendida como una técnica de gestión estratégica de toda la carga de trabajo de la FGN, pero sobre todo como una política que abarca procesos de justicia ordinaria y transicional requiere de una serie de criterios comunes que permiten la toma de decisiones al interior de la entidad. *En este sentido, los criterios de priorización actúan como parámetros lógicos que sirven para focalizar la acción investigativa de la FGN hacia determinados fenómenos, situaciones y casos, con el fin de asegurar una mayor efectividad de su trabajo investigativo y un mejor aprovechamiento de sus recursos humanos, administrativos, económicos y logísticos.* (Directiva 0002 de 2015: p. 19).

De tal modo que la *priorización*, además de permitir comprehender los elementos de orden social, económico, psicológico y geopolítico, es decir, los componentes que permiten construir un contexto social y así mismo un patrón de conducta criminal relacionada con este,

permite administrar los recursos "humanos, administrativos, económicos y logísticos" de la entidad, pues permite discernir entre conductas sistemáticas criminales -organizadas-, de aquellos incidentes aislados o de menor relevancia en términos de afectación económica, política, civil, e inclusive militar. Por consiguiente, la *priorización* se perfila como un mecanismo pertinente, en términos sociales, políticos y judiciales, e inclusive, en términos del DH y el DIH, pues esta política fortalece las prácticas de prevención y afrontamiento de riesgos cibernéticos o digitales que afecten las infraestructuras críticas de un país, en la medida en que permite abordar mediante el análisis de las variables o factores sociológicos, antropológicos e históricos -contextuales- los delitos informáticos y, de este modo, investigarlos y castigarlos de acuerdo a la situación espacio-temporal en la que se realizan.

En términos prácticos esta propuesta puede comenzar a gestarse mediante mesas de trabajo implementadas entre las distintas oficinas de delitos informáticos, la Dirección Nacional Fiscalías, Dirección Nacional del Sistema Penal Acusatorio y de la Articulación Interinstitucional en Materia Penal y la Subdirección de Tecnologías de la Información y de las Comunicaciones de la Fiscalía General de la Nación, para identificar y establecer las falencias desde el punto de vista político, investigativo y jurídico que, basadas en un análisis del contexto de la cibercriminalidad, se necesitan fortalecer en materia penal y procedimental, frente a las modalidades de los ciberdelincuentes con la utilización de las nuevas tecnologías y de la utilización de software malicioso altamente especializado, que permite vulnerar derechos civiles y económicos, pero también, expone las infraestructuras críticas del país, y por lo tanto, la defensa nacional en la guerra que se puede llevar a cabo en el espacio digital o cibernético.

Así mismo, la construcción de contextos y patrones de criminalidad cibernética permitiría elaborar tipologías más específicas y correspondientes a las prácticas delictivas

que utilizan los cibercriminales para atacar o amenazar, de tal manera que los fiscales y jueces de los delitos cibernéticos, estarían actualizados y contextualizados para adelantar investigaciones complejas tales como el ciberlavado, ciberterrorismo, cibercrimen, ciberamenazas a las infraestructuras críticas de los sectores públicos y privados, entre otros, que por su complejidad exigen la participación concertada entre Estado, organizaciones e individuos (Policía Judicial, Policía Judicial Especializada, Fiscales, jueces y magistrados, y empresas privadas). Esta propuesta puede, por tanto, eliminar las brechas existentes entre los registros de los incidentes cibernéticos y la judicialización de estos.

Recomendaciones.

Consideramos que se debe actualizar la Ley 1273 del 2009, de delitos informáticos, esto permitirá una efectiva judicialización de los ciberatacantes y ciberdelicuentes ante los jueces de garantias y de conocimiento.

Para coadyudar a la actualización se deberá realizar mesas tecnico jurídicas, para que sean analizados las clases y tipos de incidentes cibernéticos. Esto permitirá que la herramietna propuesta en el presente trabajo académico, sea mucho mas efectiva.

5. Bibliografía

Arkin, W. (1999) *The Cyber Bomb in Yugoslavia*, WASHINGTONPOST.COM, Oct. 25, 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm ***

Beck U (2008) *La sociedad del riesgo mundial en busca de la seguridad perdida*. Ediciones Paidós Ibérica, Barcelona.

Bradley Graham, (1998) *Ciberwar: A New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal,* AWSH. POST. July 8, 1998, at A1.

Brian T. O'Donell & James C. Kraska, (2003) *Humanitarian Law: Developing International Rules for the Digital Battlefield,* 8J. CONFLICT & SECURITY L. 133, 149

Comisión Económica para América Latina y el Caribe (CEPAL) (2010) Panorama del derecho informático en América Latina y el Caribe. Naciones Unidas, Santiago de Chile.

Consejo de Europa (2001) Convenio sobre la Ciberdelincuencia. Serie de Tratados N°185. Budapest, 23 de noviembre de 2001.

Comisión de Regulación de Comunicaciones (CRC) (2009) Resolución 2258 de 2009. República de Colombia, Bogotá D.C.

Corte Constitucional, Consejo Superior de la Judicatura de la República de Colombia (1991) Constitución Política de Colombia. Centro de Documentación Judicial (Cendoj), Bogotá D.C.

Cyrus Farivar, *Ciberwar I: What the Attacks on Estonia Have Taught Us About Online Combat,* SLATE, MAY 22, 2007, http://www.slate.com/id/2166749

Departamento Nacional de Planeación (DNP) (2011) *Lineamientos de política para Ciberseguridad y Ciberdefensa*. Documento CONPES 3701, Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboration.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación (DNP) (2016) *Política Nacional de Seguridad Digital*. Documento CONPES 3854, Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Fiscalía General de la Nación (FGN) (2012) Directiva Nº 001 de 2012. Fiscalía General de la Nación, Bogotá D.C.

Foester L (2016) Cybercrime as a global issue: finding solutions through interdisciplinarity and strengthened cooperation. *Global Politics and Euro-Mediterranean Relations* (GLOPEM) University of Liège. [Artí]

Ibrahim S. (2016) Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*. Vol. 47: 44-57.

Jenkins H. (2006) Convergence Culture Where Old and New Media Collide. New York University Press, New York.

Kelsey J. (2008) Hacking into International Humnitarian Law: The Principles of Distinction and Neutrality in the Age of Ciber Warfare. *Michigan Law Review*, Vol. 106 (7): 1427-1451

LACNIC Latin American and Caribbean Internet Addresses Registry (2013) Ciberdelito en América Latina y el Caribe Una visión desde la sociedad civil. Proyecto Amparo. Prandini P & Maggiore M. [Autores]

Lee M. (2012) Ciber crimes: preparing to fight insider threats. *Computer Fraud & Security*. June 2012

Ley Nº 527 de 1999. Congreso de la República de Colombia, Bogotá D.C., 18 de agosto de 1999.

Ley Nº 599 de 2000. Congreso de la República de Colombia, Bogotá D.C., 24 de julio de 2000

Ley Nº 1266 de 2008. Congreso de la República de Colombia, Bogotá D.C., 31 de diciembre de 2008.

Ley Nº 1273 de 2009. Congreso de la República de Colombia, Bogotá D.C., 05 de enero de 2009.

Ley Nº 1341 de 2009. Congreso de la República de Colombia, Bogotá D.C., 30 de julio de 2009.

Lewis J (2002) Assessing the Risks of Ciber Terrorism, Ciber War and Other Ciber Threats. Center of Strategic and International Studies, Washington, D.C. Disponible en: http://www.steptoe.com/publications/231a.pdf

Lyal S. (1997) The emerging system of international criminal law: developments in codification and implementation. The Hague, Kluwer Law International.

Manjarrés I., & Jiménez F. (2012) Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*. Vol. 5 (9): 71-82

Mansell R. Y Wehn U. (1998) *Knowledge Societies: Information Technology for Sustainable Development*, (Naciones Unidas, Oxford University Press). [Citado por Naciones Unidas Consejo Económico y Social Comisión de Ciencia y Tecnología para el Desarrollo, Ginebra, mayo de 2014. *Tecnologías de la Información y las comunicaciones para un desarrollo social y económico incluyente*.]

Organización de los Estados Americanos (OEA), AG/RES. 2004-XXXIV-O/04

Organización de los Estados Americanos (OEA) (2015) Iniciativa de Seguridad Cibernética de la OEA, Foro Global sobre Experticia Cibernética (GFCE)

Organización de los Estados Americanos (OEA) (2016) Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016.
Observatorio de la Ciberseguridad en América Latina y el Caribe.

Organización de las Naciones Unidas Consejo Económico y Social Comisión de Ciencia y Tecnología para el Desarrollo (ONU) (2014), Ginebra, mayo de 2014. *Tecnologías de la Información y las comunicaciones para un desarrollo social y económico incluyente*.]

Organización de las Naciones Unidas (ONU) (2012) Tema 3 de la agenda Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. Consejo de Derechos Humanos. A/HRC/20/L.13

OCDE (2015) *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity* in Digital Security Management for Economic and Social Prosperity, OCDE Recommendation and Companion Document, OCDE Publishing, Paris, FRancia. Recuperado de: http://www.OCDE.org/sti/ieconomy//digital-security-risk-management.pdf

Osorio S. (2010) John Ralws: Una Teoría de Justicia Social, su Pretensión de Validez para una Sociedad Como la Nuestra. *Rev Relac Int Estrateg Segur* Vol. 5 (1): 137-160

Raymond Kim-Kwang. (2011) The ciber threat landscape: Challenges and future research directions. *Computers & Security* Vol. 30: 719-731

Rojas-Parra J (2016) Análisis de la penalización del cibercrimen en países de habla hispana. *Revista Logos Ciencia & Tecnología* Vol. 8 (1): 220-232

Sassòli, M. (2003)s. Legitimate Targets of Attacks Under International Humanitarian Law 7 (2003). **[TO CHECK]**

Sood, A., and Enbody, R. (2013) *Crimeware as a service A survey of commoditized crimeware in the underground market, International Journal of Critical Infraestructure Portection*

Strauss, A., and Corbin, J. (1998) Basics of qualitative research: Techniques and procedures for developing grounded theory (2nd ed.). Thousand Oaks, CA: Sage.

Temperini M (2014) Delitos Informáticos en Latinoamética: un estudio de derecho comparado. Conferencia dictada e el 14° Simposio Argentino de Informática y Derecho, SID 2014.

UNESCO (2005) *Towards Knowledge Societies: UNESCO Word Report* (París). Disponible en: http//unesdoc.unesco.org/images/0014/001418/141843e.pdf

United Nations Office on Drugs and Crime. UNODC (2013) Comprehensive Study on Cibercrime. United Nations, New York.

Ureña, F. (2015) Ciberataques, la mayor amenaza actual. *Documento de Opinión*. Instituto Español de Estudios Estratégicos, España. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Williams, P. (2001) Organized Crime and Cibercrime: Synergies, Trends, and Responses, International Information Programs. *Electronic Journal of the U.S. Department of State*. Vol. 6 (2).