Evaluación del impacto de un centro cibernético de investigación en la Fiscalía General de la Nación, que permita tanto apoyar las investigaciones judiciales que adelanta la entidad, como coadyuvar en la elaboración de políticas criminales enfocadas a la cibercriminalidad

Miguel Ángel Riveros Restrepo

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

EVALUACIÓN DEL IMPACTO DE UN CENTRO CIBERNÉTICO DE INVESTIGACIÓN EN LA FISCALÍA GENERAL DE LA NACIÓN, QUE PERMITA TANTO APOYAR LAS INVESTIGACIONES JUDICIALES QUE ADELANTA LA ENTIDAD, COMO COADYUVAR EN LA ELABORACIÓN DE POLÍTICAS CRIMINALES ENFOCADAS A LA CIBERCRIMINALIDAD

ALUMNO:
MIGUEL ÁNGEL RIVEROS RESTREPO

DIRECTOR:
DOCTOR JAIRO ANDRÉS BECERRA ORTIZ

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ, D.C – COLOMBIA
2019

Resumen Ejecutivo

La sociedad ha venido siendo víctima de una serie de delitos que utilizan, en su mayoría, el ciberespacio, medio que sirve para afectar la información como bien tutelado en el código penal colombiano así como el medio para cometer delitos a otro tipo de bienes igualmente tipificados. En tal sentido, la Fiscalía General de la Nación realiza actividades desde el ámbito forense, aplicando las técnicas científicas para ello y cuidando de los elementos materiales probatorios y evidencias físicas vinculadas a cada caso, en donde la tecnología digital requiere de su intervención y desde al ámbito investigativo y de análisis, participando activamente en actuaciones de policía judicial que consoliden la información obtenida y en la presentación de informes que apoyen las decisiones que toma el fiscal y su grupo de apoyo en las investigaciones. En este sentido, se hace necesario estructurar un ente al interior de la Entidad que defina las políticas de actuación en el ciberespacio y que complemente las existentes para la temática de investigación y análisis criminal. Para ello, se debe conocer el estado del arte a nivel local, regional y mundial para entender el desarrollo que se ha tenido frente a la problemática de delitos en el ciberespacio, así como el desarrollo que se ha tenido por capacidades en el país, especialmente las fuerzas armadas mediante la implementación del modelo DOMPI (Doctrina, Organización, Material y equipo, Personal e Infraestructura). Además de ello, se debe conocer el desarrollo que han tenido las leyes frente a esta temática y poder descubrir, a partir de encuestas realizadas al personal adscrito a la Fiscalía General de la Nación en sus diferentes roles, las condiciones que se tienen para atacar este tipo de situaciones. Por último y teniendo en cuenta el avance exponencial que tiene la tecnología digital y su utilización de forma directa o indirecta en la comisión de delitos, es pertinente preguntar ¿Cuál es el impacto que causaría en la investigación de delitos penales, la creación de una Centro Cibernético de Investigación, que se encargue de adelantar oportunamente las investigaciones sobre actividades ilícitas que se realicen en el ciberespacio, de acuerdo con sus capacidades y recursos actuales?

Palabras clave

Cibercrimen, criminalidad informática, delito informático, seguridad de los datos

Abstract

Society has been victim of a series of crimes that are used most of the cyberspace medium that serves to affect the information as well protected in the colombian criminal code as well as the means to commit crimes to another type of goods similarly typed objects. In this sense, the office of the Prosecutor General of the Nation, performs activities from the field of forensics, applying scientific techniques to it and taking care of the material elements of proof and physical evidence related to each case, where the digital technology requires your intervention and from the field research and analysis, participating actively in the proceedings of the judicial police to consolidate the information obtained and in the presentation of reports to support the decisions that the prosecutor and his support group in the research. In this sense, it is necessary to structure an entity within the Entity that defines the policies of action in cyberspace and to complement the existing theme of research and criminal analysis. To do this, you must know the state of the art at the local level, regional and global levels to understand the development that has been had in regard to the problem of crime in cyberspace, as well as the development that has been building in the country, especially the armed forces through the implementation of the model DOMPI (Doctrine, Organization, Material and equipment, Personnel and Infrastructure). In addition, you must know the development that you have had the laws to address this subject and to be able to discover, from surveys made by personnel assigned to the office of the Prosecutor General of the Nation in their various roles, the conditions that have to attack this type of situations. Finally, and taking into account the exponential advance of technology, digital and their use directly or indirectly in the commission of crimes, it is pertinent to ask What is the impact that it would cause in the investigation of criminal offences, the creation of a Cyber Center of Research, in charge of the advance timely research on illegal activities that occur in cyberspace, in accordance with their current capabilities and resources?

Palabras clave

Cybercrime, computer crime, data security

Lista de Abreviaturas

FGN	Fiscalía General de la Nación
CTI	Cuerpo Técnico de Investigación
OSINT	Open Source Intelligence
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito
INTERPOL	Organización Internacional de Policía Criminal
TIC	Tecnologías de la Información y las Comunicaciones
CPC	Código Penal Colombiano
CP	Código Penal
NUNC	Número Único de Noticia Criminal
ICBF	Instituto Colombiano de Bienestar Familiar
SPOA	Sistema Penal Oral Acusatorio
INCIBE	Instituto Nacional de Ciberseguridad (España)

Fuente: Elaboración propia

Índice de Contenido

Objetivos

Evaluar el impacto de un Centro Cibernético de Investigación en la fiscalía general de la nación, que permita tanto apoyar las investigaciones judiciales que adelanta la entidad, como coadyuvar en la elaboración de políticas criminales enfocadas a la cibercriminalidad

Objetivos específicos

1. Identificar aspectos generales relacionados con investigación de delitos informáticos que sirvan como marco de referencia del Centro Cibernético propuesto
2. Establecer una metodología sobre la cual se pueda implementar el Centro Cibernético de Investigación, que permita el desarrollo de capacidades al interior de la Entidad
3. Realizar un análisis descriptivo de la situación propuesta relacionada con el Centro Cibernético, a partir de los datos que se puedan obtener de instrumentos de recolección de datos aplicados en la Entidad
4. Describir el impacto que pueda tener el Centro Cibernético de Investigación en la Entidad y en las investigaciones que esta orienta

Introducción

Los avances tecnológicos que vive el país actualmente, el alcance a los diferentes sectores de la economía y el fácil acceso y uso por parte de las personas del común, son aspectos que permiten visualizar la proyección de la tecnología digital en cualquiera de los aspectos de la sociedad. Es por ello, que la comunidad está viviendo una transición hacia aspectos cotidianos que hacen vulnerables a las personas por el mismo desconocimiento que tienen ante situaciones de riesgo, originadas por aquellas personas que ven en la tecnología una oportunidad para cometer actos delictivos, ya sea para lucrarse, para aprovechar el medio para delitos mayores, para adherirse a una causa o simplemente por satisfacción personal.

En los cuatro capítulos que se presentan a continuación, no sólo se pretende mostrar un panorama más detallado de los delitos que se cometen en el ciberespacio, sino ilustrar la temática de las investigaciones alrededor de los delitos cometidos utilizando medios informáticos como medio o como fin y describir los aspectos generales y mínimos con que debería contar el Centro Cibernético de Investigación y el impacto de su creación o no.

En este sentido, el primer capítulo recopila los antecedentes que enmarcan el planteamiento propuesto en este trabajo, relacionado con el modelo que actualmente direcciona los planes de acción de las fuerzas armadas en Colombia, a través de los componentes de capacidad llamado DOMPI. Este modelo está compuesto por 5 capacidades que desde su funcionalidad aportan a la construcción de su nombre: DOMPI. Estas capacidades son:

- Doctrina: Hace referencia al concepto de la capacidad adquirida y cómo se implementa a partir de la construcción del conocimiento de quienes se han encargado de realizar estos planteamientos.
- Organización: Refiere a las funciones de la entidad, la estructura funcional y los procedimientos desarrollados e implementados, en el marco del sistema de gestión de calidad.
- Material y equipo: Trata de los elementos físicos y lógicos que componen la entidad y que apoyan el desarrollo de su funcionalidad, además de su abastecimiento, mantenimiento y disponibilidad.

- Personal: Tiene en cuenta el talento humano y el fortalecimiento de sus capacidades, enfatizando en sus valores, liderazgo y entrenamiento.
- Infraestructura: Hace referencia a las instalaciones destinadas para la operación de las funciones de la entidad, ya sea una o varias propiedades.

El segundo capítulo, trata de los delitos informáticos y de aquellos que utilizan la tecnología como medio para lograr sus acciones. En este capítulo, se abordan las principales sentencias de la Corte Constitucional referente al uso de la tecnología y cómo la apropiación de las mismas puede ser perjudicial para una persona, su familia, la sociedad o traspasar barreras internacionales. Además, se muestra de manera general la fortaleza de tener un referente internacional como es el Convenio de Budapest y otros convenios europeos.

El capítulo tercero, describe los resultados obtenidos a partir de datos descriptivos obtenidos mediante la aplicación de una encuesta a los actores directos que intervienen en los procesos investigativos en la Fiscalía General de la Nación.

El cuarto capítulo, se describe la evaluación del impacto que tiene la creación de un Centro Cibernético de Investigación en la Fiscalía General de la Nación, en el marco de los elementos que se utilizaron para medirlo identificados como componentes de capacidades DOMPI.

Es así, como estos capítulos sintetizan el accionar que debería seguir este ente de investigación y abordar el ciberespacio como el escenario no complementario sino principal para realizar las investigaciones de su competencia y desde la luz del análisis criminal, orientar los planes de acción con miras a plantear no sólo procedimientos judiciales para fortalecer las investigaciones sino las políticas criminales que oriente el accionar judicial en nuestro país y así, establecer **¿cuál es el impacto que causaría en la investigación de delitos penales, la creación de una Centro Cibernético de Investigación, que se encargue de adelantar oportunamente las investigaciones sobre actividades ilícitas que se realicen en el ciberespacio, de acuerdo a sus capacidades y recursos actuales?**

Capítulo 1. Antecedentes

Este capítulo, pretende mostrar los elementos claves relacionados con el impacto de un centro cibernético con un enfoque investigativo criminal en la Fiscalía General de la Nación, que permita tanto apoyar las investigaciones judiciales que adelanta la Entidad, como coadyuvar en la elaboración de políticas criminales enfocadas a la cibercriminalidad.

Además, el centro cibernético propuesto debe orientar las capacidades de respuesta que la Entidad pueda apoyar respecto a las acciones de seguridad y defensa nacional, como participante activo del manejo de información criminal.

1.1.Marco teórico

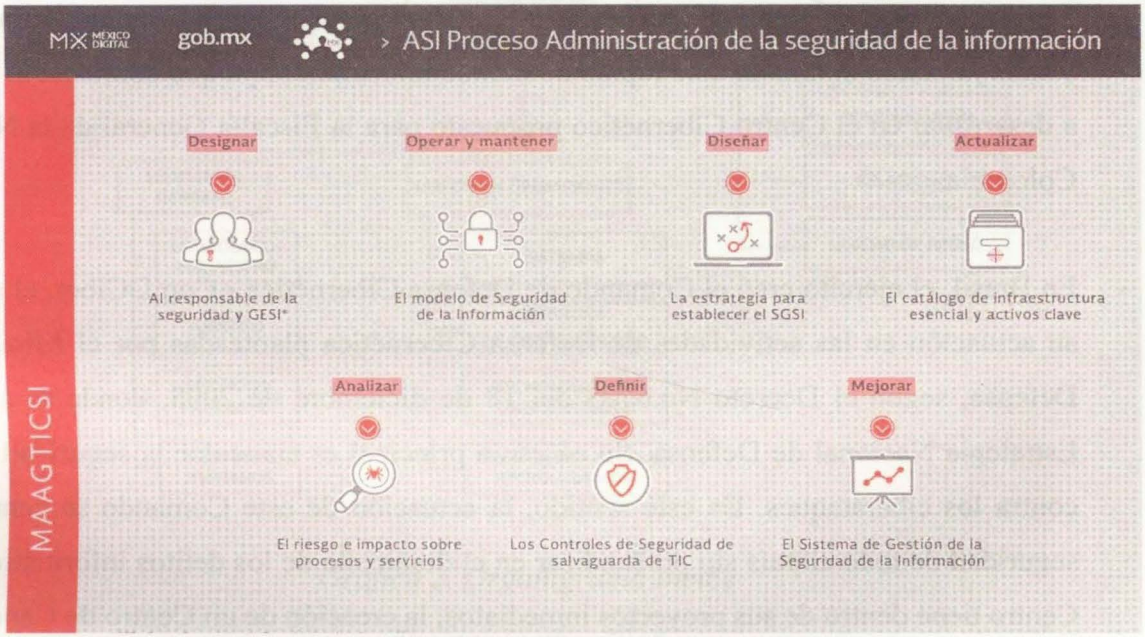
A continuación, se describen aspectos de lo que existe relacionado con el tema propuesto y que hace parte del estado del arte, donde algunos países cuentan con centros de investigación que de forma general muestran su actuar frente a la problemática de los delitos informáticos, pero no detallan la forma en que los mismos son abordados dentro de las investigaciones judiciales, así mismo, se complementa con el detalle de aspectos que muestran el desarrollo del planteamiento en el que se basa esta propuesta de creación de un centro de investigación cibernético.

Es importante, relacionar los organismos que de forma similar establecen acciones en contra del manejo ilícito de la información, ya sea como protección de datos o como seguridad estatal. Es así, como se pueden identificar los siguientes entes:

- En México el Centro de Investigación y Seguridad Nacional – CISEN, se define como el "órgano de inteligencia civil al servicio del Estado Mexicano cuyo propósito es generar inteligencia estratégica, táctica y operativa que permita preservar la integridad, estabilidad y permanencia del Estado Mexicano, dar sustento a la gobernabilidad y fortalecer al Estado de Derecho. Se encuentra alineado con el Plan Nacional de Desarrollo 2013-2018, donde se establece una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías de la información y comunicaciones (TIC), e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento". (CISEN, 2010)

Aquí, se puede apreciar que el enfoque está dado hacia la seguridad nacional pero con falencias hacia los delitos informáticos que afectan la información y que está contemplada en las políticas y disposiciones del gobierno mexicano, pero no están desarrolladas para su aplicación desde este tipo de centros de investigación.

Este Centro contempla en su gestión documental, el Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, donde describe los diferentes procedimientos que enmarcan la política de gobierno, pero no se visualiza de forma clara los aspectos hacia contrarrestar las acciones delictivas en el ciberespacio, aunque se tratan temas de seguridad de información de forma general. Una muestra de estos procedimientos se muestra en la Gráfica 1.



Gráfica 1. Proceso de Administración de la seguridad de la información

Fuente: Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información. CISEN(2010)

- En Perú, se encuentra la División de Investigación de Delitos de Alta Tecnología - DIVINDAT de la Dirección de Investigación Criminal – DIRINCRI, que mantiene un constante monitoreo de las acciones que se realizan en el ciberespacio, teniendo como hoja

de ruta la Ley No.30096 y su modificatoria en la Ley No.30171. En estas se detallan las faltas que tiene que ver con los bienes jurídicos, a saber:

- Delitos contra datos y sistemas informáticos
- Delitos informáticos contra la indemnidad y libertad sexuales
- Delitos informáticos contra la intimidad y el secreto de las comunicaciones
- Delitos informáticos contra el patrimonio
- Delitos informáticos contra la fe pública

El control que tiene este Centro sobre la actividad delictiva permite establecer la importancia que tienen los delitos en el ciberespacio y en especial aquellos que han sido identificados por quienes ejercen las funciones de investigación criminal.

Es de resaltar el esfuerzo que ha hecho el gobierno peruano por incluir una gran parte de bienes jurídicos dentro de este tópico de delitos informáticos ya que confirma la hipótesis a desarrollar en el Centro Cibernético propuesto para la Fiscalía General de la Nación en Colombia.

- En Brasil, el ejército creó el Comando de Defensa Cibernética - ComDCiber, el cual basa su actuación en las actividades de Defensa Cibernética planteadas por el Ministerio de Defensa, según el Decreto No.6703 del 18 de diciembre de 2008, donde se aprobó la Estrategia Nacional de Defensa. Su objetivo principal es aumentar la seguridad del país contra los ciberataques. En este sentido, la actuación de este Comando se centra en la seguridad de todo el país sin profundizar en el desarrollo de los delitos informáticos. Este Centro tiene dentro de sus proyectos inmediatos, la creación de un Centro de Capacitación para fortalecer las capacidades de reacción de civiles y militares frente a ataques cibernéticos, otro es, certificación de productos de Defensa Cibernética y la Creación del Observatorio de Defensa Cibernética para incentivar la investigación y desarrollo de tecnología. (Moury, 2017).

- En España, el Instituto Nacional de Ciberseguridad - INCIBE, "es una sociedad dependiente de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y consolidada como entidad de referencia para el desarrollo de la

ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos." (Incibe, 2108)

Este Instituto es un referente importante para todos los aspectos de ciberseguridad en España, no sólo por su componente académico que contempla una variedad de capacitaciones para dotar de conocimiento a los interesados en temas de ciber, sino en los servicios que ofrece en este mismo ámbito. En la Gráfica 2, se puede observar la estructura orgánica que permite entender la diversificación que tiene en temas de ciberseguridad. (Incibe, 2018)

Gráfica 2. Organigrama Incibe

Fuente: Incibe, 2018

Además, este instituto cuenta con varias capacidades de actuación que favorecen a quienes están interesados en temas de seguridad desde el ciberespacio:

- Respuesta a incidentes de seguridad
- Iniciativas para mejorar los niveles de ciberseguridad en España
- Estudio de riesgos emergentes para generar alertas tempranas
- Coordinación con otros entes a nivel nacional e internacional relacionados con ciberseguridad (Incibe, 2018)

- En Ecuador, se creó la Subdirección de Delitos Informáticos, "abarcará un espectro mucho más amplio que le permitirá tener una capacidad preventiva de inteligencia antidelincuencial en estos delitos." Esta Subdirección cuenta con un equipo de reacción para la investigación de las denuncias que los ciudadanos coloquen, además de un equipo de inteligencia preventiva para la búsqueda en redes y el ciberespacio. Así mismo, se cuenta con una estructura para desarrollar inteligencia antidelincuencial en las calles, así como inteligencia cibernética. (Serrano, 2016)

  Las actuaciones de esta subdirección están enmarcadas en el Código Orgánico Integral Penal (COIP), donde se especifican los delitos informáticos, algunos de los cuales se enuncian a continuación:

  - Pornografía infantil – 13 a 16 años de prisión.
  - Violación del derecho a la intimidad – de uno a tres años de prisión
  - Revelación ilegal de información de bases de datos – de uno a tres años de prisión
  - Interceptación de comunicaciones – de tres a cinco años de prisión
  - Pharming y Phishing – de tres a cinco años de prisión
  - Fraude informático – de tres a cinco años de prisión
  - Ataque a la integridad de sistemas informáticos – de tres a cinco años de prisión
  - Delitos contra la información pública reservada legalmente – de tres a cinco años de prisión
  - Acceso no consentido a un sistema informático, telemático o de telecomunicaciones – de tres a cinco años de prisión.

Es pertinente, para una mejor comprensión del estado actual de la Entidad y poder entender mejor el impacto del Centro Cibernético de Investigación a la luz de las competencias propuestas, conocer las funciones ordenadas en los diferentes actos administrativos de la Fiscalía General de la Nación, como es el Decreto 016 del 9 de enero de 2014, por el cual se modifica y define la estructura orgánica y funcional de la Fiscalía General de la Nación, relaciona las siguientes funciones para la Dirección Nacional del Cuerpo Técnico de Investigación, que se consideran útiles para el estudio del impacto de esta investigación (Ministerio de justicia y del derecho, 2017):

"3. Hacer análisis criminal para apoyar el cumplimiento de las funciones de la Fiscalía General de la Nación.

4. Apoyar, en el marco de sus competencias, las actuaciones que adelanten las dependencias de la Fiscalía General de la Nación en el ejercicio de sus funciones, cuando éstas lo requieran.

6. Adelantar, dentro del ámbito de su competencia, el intercambio de información entre los distintos organismos de investigación, de seguridad e inteligencia a nivel nacional e internacional, para la programación y el desarrollo de operaciones contra la delincuencia, bajo las directrices del Vicefiscal General de la Nación."

De igual forma, el Decreto 898 del 29 de mayo de 2017, "*por el cual se crea al interior de la Fiscalía General de la Nación la Unidad Especial de Investigación para el desmantelamiento de las organizaciones y conductas criminales responsables de homicidios y masacres, que atentan contra defensores/as de derechos humanos, movimientos sociales o movimientos políticos o que amenacen o atenten contra las personas que participen en la implementación de los acuerdos y la construcción de la paz, incluyendo las organizaciones criminales que hayan sido denominadas como sucesoras del paramilitarismo y sus redes de apoyo, en cumplimiento a lo dispuesto en el Punto 3.4.4 del Acuerdo Final para la terminación del conflicto y la construcción de una paz estable y duradera, se determinan lineamientos básicos para su conformación y, en consecuencia, se modifica parcialmente la estructura de la Fiscalía General de la Nación, la planta de cargos de la entidad y se dictan otras disposiciones*", establece la redefinición de la política criminal de la Entidad y *"define de manera más clara la capacidad de dirección estratégica y planeación de la Entidad, para adecuar su estructura a los cambios exigidos por el Acuerdo con el fin de hacer más eficiente la distribución de cargas de trabajo y enfocar los recursos de investigación y judicialización hacia las prioridades del Acuerdo de Paz y de la construcción de una paz estable y duradera"*. (Ministerio de justicia y del derecho, 2017)

1.1.1. Condiciones administrativas.

Así, con este marco legal de actuación definido en estos actos administrativos, se hace necesario contar con herramientas no sólo jurídicas, como el mismo Código Penal y el Código de Procedimiento Penal que contienen las normas jurídicas punitivas y sobre las cuales se trazan los

derroteros de la Entidad, sino técnicas y tecnológicas que garanticen el adecuado manejo de las acciones contra las organizaciones delincuenciales. Un ejemplo de esta situación son los modelos de investigación y metodologías de análisis criminal aplicadas al tratamiento de la información con miras a establecer patrones criminales de estas organizaciones, que son desarrolladas, revisadas e implementadas por las diferentes direcciones de investigación de la Fiscalía General de la Nación. (Fiscalía General de la Nación, 2016)

En este aspecto, es importante hacer referencia al Direccionamiento Estratégico propuesto por el señor Fiscal General de la Nación, donde se plantean prioridades en investigación y judicialización, que se consolida en el primer objetivo estratégico de este Plan: "Impactar de forma contundente el crimen organizado". Lo anterior, desde el enfoque institucional que busca fortalecer las capacidades en la lucha contra las actividades y organizaciones criminales y contrarrestar los resultados de impacto en el territorio nacional. (Fiscalía General de la Nación, 2016)

En este sentido, es importante establecer la infraestructura necesaria para cubrir las necesidades de ciberseguridad y ciberdefensa aunado a la gestión de riesgos que de forma obligada y juiciosa se debe desarrollar para cerrar brechas que continuamente aparecen en el mundo ciber. Estas consideraciones son obligatorias a la luz del Convenio de Budapest, el cual es el referente a nivel mundial sobre la protección de la sociedad frente al actuar de la delincuencia en el ciberespacio y que busca mediante cooperación entre las naciones combatir la ciberdelincuencia y establecer patrones de investigación conjunta. Es por esto, que el Ministerio de las Tecnologías de la Información y las Comunicaciones radicó un proyecto de ley para adherirse a este Convenio y fortalecer su lucha contra la ciberdelincuencia, buscando proteger tanto a las instituciones del Estado como las infraestructuras críticas del mismo. Esta adhesión, "le permitirá a Colombia no solo avanzar en temas de cooperación internacional contra delitos informáticos, sino también fortalecer las leyes y regulaciones nacionales contra el ciberdelito en todos los niveles." (Mintic, 2018)

Ahora bien, es necesario articular esta posición con la propuesta del gobierno nacional, sobre la Política Nacional de Seguridad Nacional, donde la diferencia principal entre el Documento CONPES 3701 y el documento CONPES 3854, es la gestión de riesgos propuesta en este último. Uno de sus objetivos de este documento es "fortalecer las capacidades de las múltiples partes

interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital." (DNP, 2016)

La política de ciberseguridad y ciberdefensa ha permitido fortalecer las instituciones. Esta afirmación es completamente visible si se hace una mirada detallada a los nuevos entes que fueron creados con ocasión de esta política, como son: el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL) y otras más que fortalecen varias instituciones del Estado y que coadyuvan en el compromiso primario de proteger la soberanía del país y mejorar las condiciones de la seguridad ciudadana.

Uno de los objetivos del Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) consiste en "Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones". (COLCERT, 2018)

Así pues, se puede denotar como desde el Gobierno Nacional está alineada la estrategia de apoyar las instituciones en las actividades de investigación sin hacer distinción o acotamientos especiales para estas. Por esto mismo, es importante hacer claridad que la investigación de delitos a la que se hace referencia en esta función específica y donde se indica la importancia de los elementos integradores de la Tecnologías de la Información y las Comunicaciones, se debe robustecer mediante la incorporación de recursos técnicos que apoyen esta labor especializada dentro del desarrollo de los procesos judiciales.

Según el Manual de Procedimientos de la Fiscalía en el Sistema Penal Acusatorio, la investigación es la fase en la que el fiscal delegado, con el apoyo de la policía judicial, busca fortalecer los elementos materiales probatorios o evidencia física o información legalmente obtenida que sirvieron de fundamento a la formulación de imputación, con el objetivo de poder acusar a los presuntos autores o partícipes de la conducta investigada, solicitar la preclusión, o dar aplicación al principio de oportunidad. Es así, que se debe advertir que las labores encaminadas a dar valor a estos elementos materiales probatorios y evidencia física deben estar soportadas por

recursos físicos, humanos y tecnológicos que integren los resultados y que apoyen las hipótesis propuestas por el respectivo fiscal y su equipo de policía judicial. Algunos de los actos de investigación del Manual de Procedimientos son la vigilancia, análisis, infiltración y búsqueda de información, los cuales permiten obtener información relevante para la investigación, no obstante, el tiempo, recursos y procesos utilizados en la consecución de los objetivos propuestos al inicio de la investigación. (Fiscalía General de la Nación, 2009)

En la Fiscalía General de la Nación se debe tener en cuenta la priorización de situaciones y casos para desvertebrar las organizaciones criminales, la evaluación de la gestión misional de la Policía Judicial, la racionalización del gasto, la eficiencia y un equilibrio racional de los recursos humanos, técnicos, financieros y logísticos para el mejoramiento de la gestión. (Fiscalía General de la Nación, 2014). En este sentido, los recursos a utilizar para este postulado deben contemplar los diferentes escenarios donde se desarrollan los crímenes, como lo es el estadio físico y el virtual o ciberespacio, como se ha venido describiendo en este documento.

1.1.2. Otras entidades.

Como se registra en el CONPES 3701 de 2011, el Centro Cibernético Policial – CCP, estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Y recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT. El CCP se encargará de la investigación y apoyará la judicialización de los casos que se materialicen y se tipifiquen como delitos informáticos.

Si se hace una lectura juiciosa de este párrafo, se puede entender que su prioridad y enfoque está en la información y datos que puedan resultar producto de actividades delictivas, enmarcadas en las acciones descritas mediante la Ley 1273 de 2009.

Más allá de este tipo de activos y bienes tutelados, no hay una línea funcional que proporcione elementos que apoyen las labores de investigación de otro tipo de delitos y/o que permitan hacer un seguimiento de personas, bienes e información relacionada con personas vinculadas a los procesos judiciales fuera del marco de los delitos informáticos.

Pero es internet el medio digital que proporciona espacio para todo tipo de actividades ya sean delictivas o no, más allá de afectar los datos y la información, protegida en nuestra legislación por la Ley 1273 de 2009. En este especial sentido, se hace un recorrido detallado de las acciones que se pueden encontrar en la web, especialmente en la conocida deep web, entre los cuales se destacan acciones delictivas distantes de los meros delitos informáticos, como: venta de drogas, asesinos a sueldo, compra de documentos de identidad, lavado de dinero y pornografía infantil. (Bolaños, 2015)

Trend Micro, después de dos años de consultar la deep web y analizar su información, el 85% de los usuarios de internet utilizan los servicios que en este espacio virtual se ofrecen, tan sólo un 15% utilizan los servicios de la web blanca o servicios como google y otros igualmente conocidos. Es por tanto, muy importante que se centre la atención de la deep web sin dejar de lado la web blanca, para establecer estrategias y mecanismos que ayuden o por lo menos se acerquen a la construcción de información y detalle de procesos, que permitan orientar las investigaciones judiciales de la Entidad. (Bolaños, 2015)

1.1.3. Condiciones criminales en el ciberespacio.

Según el estudio realizado por las empresas de inteligencia Intelliagg y Darksum , citadas por MOTOS (2016), hay un porcentaje en la deep web que no corresponde necesariamente a contenido ilegal, debido a que hay muchas personas que por su condición de rebeldía u otras motivaciones encuentran en este espacio su forma de expresión. Se utilizó un software de tipo spidering para monitorear la red TOR y poder establecer las relaciones que existen entre sus diferentes niveles de interconexión, a través de sus enlaces. El estudio arrojó que en las direcciones y servicios que están ocultas hay un 68% de contenido ilegal que está clasificado como ilegal en el Reino Unido y Estado Unidos. El método utilizado en este estudio se considera confiable ya que 9 de 10 veces en el que se aplicó, los algoritmos utilizados concluyeron lo mismo como si lo hubiera hecho un analista experto.

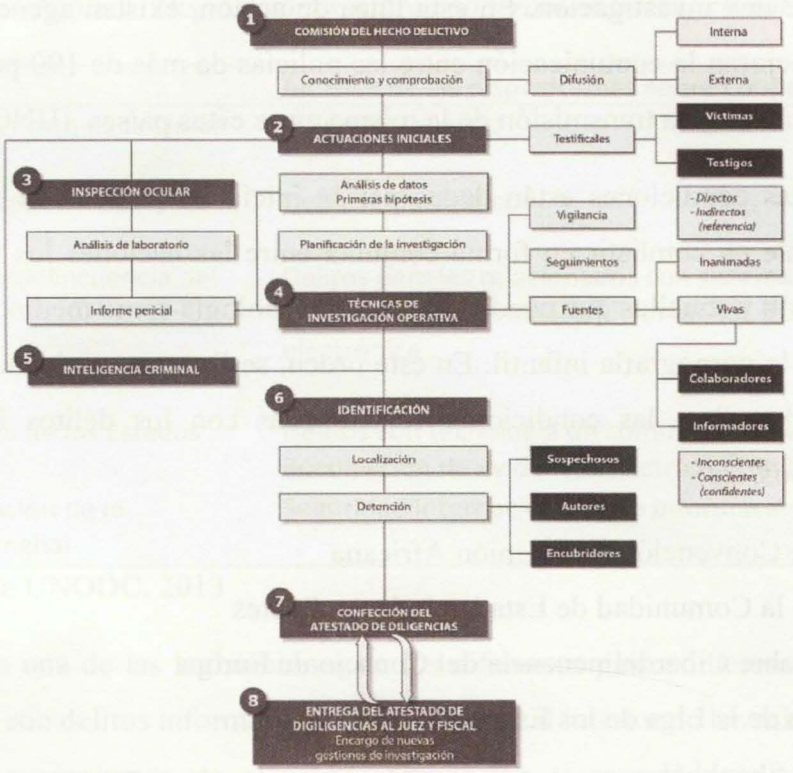
Debido a que no existen fronteras que permitan establecer la territorialidad de las acciones criminales, es difícil establecer el origen de donde se cometieron estas actividades para poder establecer las condiciones relacionadas con el ámbito judicial. (Teruelo, 2011)

Se reafirma lo que se ha venido destacando acerca del nuevo espacio creado para que la criminalidad encuentre una oportunidad para cometer sus acciones delictivas. Este espacio lo clasifica como una gran categoría en la cual se registran no sólo los delitos que tienen una funcionalidad intrínseca relacionada con la tecnología, sino aquellos que se valen del medio virtual para ser cometidos. (Miró, 2011)

Para el año 2015, tan sólo en el primer semestre se pudo constatar, que las denuncias por ciberdelincuencia aumentaron en un 25% y que la mayoría están relacionadas con el sector financiero y esto se consolida cuando se afirma que la mayoría de los usuarios de este sector tiene cada vez más facilidad para realizar transacciones en línea, debido al acercamiento con las tecnologías mediante el uso de teléfonos inteligentes, principalmente. (Hecsan, 2015). Este sector, uno de los más importantes para la delincuencia, invierte muchos recursos en seguridad informática y se considera el acompañamiento que debe tener el cliente mediante el monitoreo constante de la plataforma tecnológica, aunado a la supervisión y vigilancia que permita la protección del negocio. (Luicon, 2016).

Ahora bien, para cada uno de estos delitos y de las formas, medios y espacios en el que son cometidos, existen estructuras funcionales que desde el desarrollo de la investigación criminal se necesitan entender para articular las actividades que realiza la policía judicial con miras al esclarecimiento de los hechos y la identificación de los actores en estos hechos. De esta manera, se puede apreciar de forma gráfica (Gráfica 3) cómo se estructura el proceso de la investigación criminal y cómo esta propuesta adolece, en una visión rápida, de aquellas fases en las que intervienen el concepto de ciberespacio.

De igual forma, las redes sociales son el medio principal a través de las cuales se comunican los ciberdelincuentes, siendo Facebook y Twiter las más utilizadas. De la misma forma, tanto los mensajes instantáneos como los mensajes a través de Whatsapp son los preferidos según el estudio referenciado por la empresa Trend Micro. (Sempere, 2016)



Gráfica 3. Proceso y fases de la investigación criminal

Fuente: Giménez-Salinas y González (2016)

1.1.4. Referencias internacionales.

Cuando se habla de delitos informáticos, se debe tener en cuenta que no sólo se pueden cometer dentro del contexto nacional de un Estado sino que en la mayoría de los casos, hace referencia entre otras a la relación que existe entre los delitos informáticos y la participación de más de un país en la comisión de estos delitos, convirtiéndolos en delitos transnacionales, indicando la importancia de colaboración entre los Estados para el control y monitoreo de estos actos delictivos. En este sentido, se crean acuerdos internacionales que permite de forma colaborativa hacer que un Estado solicite información o genere mecanismos de asistencia que permitan reunir evidencia para ser tratada en el marco de investigación de los delitos informáticos reportados en su territorio. (UNODC, 2013)

Existen en este marco, tipos de cooperación internacional que en su concepción informal permiten solicitar información de policía a policía o de agencia a agencia, ésta referente a localización de personas, realización de interrogatorios o compartimentación de información

relevante dentro de una investigación. En esta línea de acción, existen agencias de ley como la INTERPOL que mejoran la comunicación entre las policías de más de 190 países, facilitando la solicitud de información y la transmisión de la misma entre estos países. (UNODC, 2013)

Ahora bien, estas condiciones están dadas por la iniciativa presentada en el Convenio de Budapest consistente en combatir en forma conjunta entre las naciones los delitos que atenten contra la información y aquellos que puedan utilizar la tecnología como medio para este cometido, como por ejemplo la pornografía infantil. En este orden, se listan a continuación algunos de los documentos que describen las condiciones relacionadas con los delitos informáticos desde acuerdos y convenios, así:

- Proyecto de Convención de la Unión Africana
- Acuerdo de la Comunidad de Estados Independientes
- Convenio sobre Ciberdelincuencia del Consejo de Europa
- Convención de la Liga de los Estados Árabes
- Acuerdo de Shanghai

Cada uno de estos acuerdos y convenios, presentan las pautas para establecer las líneas de acción sobre el actuar de las comunidades internacionales respecto a las diferentes formas de delitos informáticos, entre los que se destacan las interferencias de redes de comunicación, intrusiones a sistemas de información, fraudes, estafas, pornografía infantil, propiedad intelectual, entre otros. (*UNODC, 2013).* Es así como en la Gráfica 4, se muestran las disposiciones de cada uno de los instrumentos enunciados anteriormente.

Tabla 1. Disposiciones sobre cooperación internacional

Instrumento	Alcance de las disposiciones sobre cooperación internacional
Proyecto de la Convención de la Unión Africana	Delito cibernético
Acuerdo de la Comunidad de Estados independientes	Delitos informáticos
Convenio sobre Ciberdelincuencia del Consejo de Europa	Delitos penales relacionados con sistemas y delitos informáticos Recolección de evidencia de un delito penal en forma electrónica
Convención de la Liga de los Estados Árabes	Delitos con tecnología de comunicación e información Recolección de evidencia electrónica en los delitos
Acuerdo de Cooperación de la Organización de Shanghai	Seguridad internacional de la información

Nota: Tomado de UNODC, 2013

Adicional a cada una de las legislaciones de los diferentes países interesadas en combatir el crimen relacionado con delitos informáticos, se han creado al interior de los mismos, agencias que vienen generando mecanismos de atención, prevención y control de estas situaciones del ciberespacio.

Consultadas algunas de estas agencias internacionales que están interesadas en conformar espacios donde se orienten investigaciones criminales, se detalla que estas tienen su enfoque investigativo hacia los delitos informáticos.

Ahora bien, existen diferentes acciones adelantadas por agencias de investigación, como el FBI, donde se aplican entre otras vulnerabilidades de día Zero para poder recuperar evidencia que permita fortalecer las diferentes etapas judiciales en contra de indiciados, en delitos como pornografía infantil y terrorismo. (Romanosky y Weinbaum, 2017)

De la misma forma, se describe como buena práctica el conocimiento del enemigo, ya que se pueden hacer perfiles de las trazas que dejan los ataques o caminos que han recorrido los ciber delincuentes y así, poder diseñar y poner en ejecución herramientas que controlen este tipo de ataques. (Software Engineering Institute, 2013)

Es importante establecer algunos mecanismos que permitan tener reacción a las amenazas existentes y a los actos de cibercriminalidad que están en el ciberespacio, por eso es importante tener protocolos de conservación de evidencias que permitan posteriormente hacer los análisis

respectivos a las intrusiones a los sistemas o a la navegación no permitida por cierto tipo de información. (Prosecuting Computer Crimes, 2007).

Una vez explorado el ámbito en el que se movilizan los ciberdelincuentes y cómo los delitos tanto informáticos como los que usan las tecnologías para ser configurados, es necesario indagar los avances en materia de la legislación y cómo se ha concebido su incorporación en estos temas del ciberespacio. Por esta razón, es importante tener presente la forma en que la legislación española ha avanzado en este tema y cómo a través de su aprobada Ley Orgánica 13/2015 se incluyen diligencias de investigación como agentes encubiertos en internet, uso de drones y hasta virus espías. De esta manera, nos encontramos con progresos en el ámbito legal que se pueden considerar en nuestra legislación para ser incorporados y así, darle la fortaleza que necesitan las leyes colombianas en esta materia. (Bueno de Mata, 2016)

Una vez revisada la información, se puede concebir la idea de la falta tanto de legislación apropiada en el sistema penal actual que permita incluir acciones más detalladas respecto a la utilización de las tecnologías digitales en los ámbitos de investigación judicial, como la carencia de modelos técnicos que favorezcan los procesos de investigación criminal.

1.2. Componentes de capacidades DOMPI

El Ejército de Colombia en su proyección de fortalecer las capacidades tendientes a mejorar las estrategias y reacciones operativas en el campo de combate, ha diseñado la Doctrina DAMASCO como el eje que permite la articulación del plan de transformación institucional. (Rojas, 2017)

Esta Doctrina permite unificar criterios de capacidades mediante la implementación de los componentes de capacidades DOMPI, a saber, Doctrina, Organización, Material y equipo, Personal e Infraestructura, como se muestra y define en la Gráfica 4.

Gráfica 4. Definición de capacidad y componentes del sector defensa

Fuente: Plan Estratégico Sectorial de TIC 2018-2022

Ahora bien, para seguir entendiendo esta metodología, es necesario definir el concepto de capacidades, las cuales se refieren a "los recursos y aptitudes que tiene un individuo, entidad o institución, para desempeñar una determinada tarea o cometido" (Wikipedia, 2018), las cuales se adquieren para realizar una tarea y para ello, se deben tener en cuenta variables que permitan alinear estas capacidades con las acciones que se tiene proyectadas al interior de cada Entidad. Para que esto se pueda establecer de forma permanente y con un ciclo de mejoramiento continuo para lograr mejores resultados, existen actualmente componentes que fortalecen estas capacidades.

Estas capacidades están alineadas con la visión del Ejército que "busca enfocar sus procesos y procedimientos operacionales para anticipar y superar las amenazas y los desafíos del futuro". Esta visión está proyectada hacia el año 2030 y una de sus bases es el planeamiento por capacidades. (Rojas, 2017)

La implementación de esta metodología y por consiguiente el fortalecimiento de las capacidades del Ejército, parte de la necesidad de mejorar el ambiente operacional incierto sobre el cual actúa esta Fuerza, es decir, la falta de información, su procesamiento y respectivo análisis para lograr que los datos recolectados sean utilizados en las estrategias a implementar.

Es importante anotar que se debe "reconocer el tipo de enemigo que combatimos y por tener absoluta claridad sobre su naturaleza" (Rojas, 2017). Es así, como aún no se tiene claro el tipo de enemigo, especialmente en ambientes donde este no es claramente reconocido, tal vez por su falta de exploración, donde aspectos como tiempo y lugar son especialmente aprovechados por este actor.

Para lograr fortalecer las capacidades institucionales del Ejército y lograr la evolución de la cultura militar, se han planteado varias líneas de acción:

- Identificar e incorporar el talento humano que posea la mejor formación, de acuerdo con las competencias definidas por gestión humana.
- Establecer un lenguaje común respecto a la doctrina que oriente los principios, tácticas, técnicas y procedimientos de la Fuerza.
- Fortalecer los valores al interior de la Fuerza y lograr constituir la ética como única regla.
- Incentivar un modelo de liderazgo que permita la confianza entre quienes están en la línea de mando y subordinados.
- Garantizar a la Nación cobertura, control y protección tanto a nivel de territorio como a nivel de población.

Estas líneas de acción propuestas buscan responder a las amenazas futuras, sobre todo en campos poco explorados y las cuales buscan "tomar ventaja mediante la adquisición de nuevas tecnologías", es decir, la doctrina Damasco busca que el Ejército pueda "generar y adaptar su doctrina a las circunstancias que demandan las condiciones sociales, económicas, políticas y geoestratégicas actuales y futuras, con proyección al año 2030". (Rojas, 2017)

La implementación de esta Doctrina responde en parte al planteamiento de "Adquirir la superioridad militar en el ciberespacio a través de la integración de las capacidades de Ciberseguridad y Ciberdefensa de las FFMM" (Comando general, 2015)

De forma articulada con esta Doctrina, en el modelo de Planeación y desarrollo de capacidades, una capacidad se define como la habilidad de realizar una tarea, bajo ciertos estándares (como tiempo, ambiente y nivel de alistamiento específicos), a través de la combinación de los diferentes componentes. (MinDefensa, 2017)

De acuerdo con lo anterior, se debe revisar cada una de las capacidades a la luz de las Tecnologías de la Información y las Comunicaciones, que es el factor que incide en la respuesta oportuna frente a las amenazas modernas.

Las capacidades se pueden definir, como las habilidades que se adquieren para realizar una tarea y para ello, se deben tener en cuenta variables que permitan alinear estas capacidades con las acciones que se tiene proyectadas al interior de cada Entidad. Para que esto se pueda establecer de forma permanente y con un ciclo de mejoramiento continuo para lograr mejores resultados, existen actualmente componentes que fortalecen estas capacidades.

Estos componentes corresponden a un modelo que se viene implementando en las Fuerzas Militares de Colombia con la finalidad de hacer la proyección sobre la estructura de fuerza en el mediano y largo plazo (Pineda Fandiño, 2017) los cuales son llamados: Doctrina, Organización, Personal, Material y equipo e Infraestructura, conocido como componentes de capacidad DOMPI.

Es importante anotar que, para poder articular los componentes presentados con la propuesta sugerida, es necesario asociar estos a las capacidades de las Tecnologías de la Información y las Comunicaciones en la Fiscalía General de la Nación.

1.2.1. Doctrina.

Este término establece las concepciones teóricas de la Entidad, que permiten orientar su actuar en pro de la mejor estrategia de funcionamiento y del logro de sus objetivos misionales.

Es así, como se priorizan las capacidades enfocadas al uso y apropiación de las Tecnologías de la Información y las Comunicaciones, debido a que son estas las llamadas a trazar las pautas de actuación de los sistemas informáticos frente a las actividades del ciberespacio.

El sector defensa, representado por las fuerzas militares de Colombia, presenta una gran debilidad en este aspecto debido a la falta de protocolos para consolidar la planeación, estandarización y priorización de necesidades y acuerdos de servicio y así, ejecutar de manera efectiva las actividades que conduzcan al cumplimiento de los objetivos institucionales referentes a TIC. (Ministerio de Defensa, 2017)

En este sentido, el Ministerio de Defensa ha liderado la iniciativa de estandarizar algunos conceptos, entre ellos, el término TIC, el cual lo define como "conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento y transmisión de información (voz, datos, video e imagen) requeridas para el uso y fortalecimiento de las capacidades operacionales y de soporte, actuales y futuras, del Sector Defensa y Seguridad". (Ministerio de Defensa, 2017)

1.2.2. Organización.

En cuanto a organización, se deben tener en cuenta las áreas y procedimientos asociados a ellas, que desarrollan las competencias tanto misionales como en tecnologías de la información y las

comunicaciones. En este sentido, se ha planteado en el Plan de Desarrollo 2014-2018 de la Policía Nacional por parte de la entidad del Estado encargada de la Planeación Nacional la necesidad de que las instituciones del sector defensa y seguridad cuenten con oficinas de tecnología estructuradas y que se ubiquen estratégicamente para apoyar las decisiones. Ahora bien, de todas las instituciones del sector, la Policía Nacional es la única que cuenta con Oficina de Tecnología en el nivel estratégico, las demás, al no contar con una estructura similar desde el nivel estratégico hacen que las iniciativas que se presenten sobre centralizar y estandarizar las necesidades y procesos se afecten de forma negativa. (Ministerio de Defensa, 2017)

1.2.3. Material y equipo.

Este aspecto permite definir los componentes que debe tener la entidad para desarrollar su misionalidad, los cuales deben tener características homogéneas que permitan proyectar y organizar las necesidades de tecnología del sector. Los componentes son a nivel de hardware y software como se pueden apreciar en la Gráfica 6. (Ministerio de Defensa, 2017)

1.2.4. Personal.

Se definen los perfiles de cada una de las personas que pertenecen a las estrategias de la Entidad. Estas definiciones no están claras en las entidades del sector, en los temas relacionados con TIC. No existe una política para el manejo del personal que permita garantizar la permanencia en el desarrollo de las funciones que se asignan relacionadas con Tecnologías de la Información y las comunicaciones. (Ministerio de Defensa, 2017)

Tabla 2. Disposiciones sobre cooperación internacional

HARDWARE

CLASE	SUBCLASE
ORDENADORES	COMPUTADOR DE ESCRITORIO
	COMPUTADOR PORTÁTIL
	CLIENTE LIVIANO / DELGADO (Escritorio Virtualizado)
	TABLET / PDA
SERVIDORES	SERVIDORES FÍSICOS
	APPLIANCES PARA VIRTUALIZACIÓN
PERIFÉRICOS	EQUIPOS DE IMPRESIÓN / DIGITALIZACIÓN
	EQUIPOS DE VISUALIZACIÓN
	EQUIPOS DE ALMACENAMIENTO MASIVO
REDES DE DATOS	EQUIPOS DE TELEFONÍA
	EQUIPOS ACTIVOS
REDES DE COMUNICACIONES ESTRATEGICAS / OPERATIVAS / TACTICAS	EQUIPOS UHF
	EQUIPOS VHF
	EQUIPOS HF
	EQUIPOS SATELITALES
	RADIOENLACES
	RADIOAYUDAS
	EQUIPOS VCS (INTEGRADORES)
SEGURIDAD INFORMATICA	FIREWALL
	ANTISPAM
	CONTROL DE NAVEGACIÓN
	DLP
	CORRELACIONADOR
	IDS
	GESTIÓN DE IDENTIDADES
	EQUIPOS BIOMÉTRICOS / RECONOCIMIENTO

SOFTWARE

CLASE	SUBCLASE
DE BASE	SISTEMAS OPERATIVOS
	HERRAMIENTAS DE CORRECCIÓN Y OPTIMIZACIÓN
	HERRAMIENTAS DE DIAGNÓSTICO
	UTILITARIOS
DE PROGRAMACIÓN	COMPILADORES
	INTERPRETES
	DEPURADORES
	ENTORNOS DE DESARROLLO INTEGRADO (IDE)
DE APLICACIÓN	OFIMÁTICA
	SISTEMAS DE INFORMACIÓN EMPRESARIAL / SECTORIAL
	BASE DE DATOS
	COMUNICACIONES
	CARTOGRAFÍA
	SEGURIDAD
	CÁLCULO NUMÉRICO / ESTADÍSTICO
	DISEÑO ASISTIDO POR COMPUTADOR
	DESARROLLOS IN HOUSE / A LA MEDIDA
	COMUNICACIONES TÁCTICAS / OPERACIONALES

Nota: Plan Estratégico Sectorial de TIC 2018-2022

1.2.5. Infraestructura.

Se definen las fortalezas y deficiencias de la Entidad con respecto a las instalaciones y la ubicación física de los elementos necesarios como apoyo a los objetivos estratégicos.

Actualmente, existen deficiencias en la operación de los centros de datos de las fuerzas militares, las brechas que existen entre estos centros en las diferentes instituciones y la falta de soluciones y estándares para la operación y mantenimiento de las infraestructuras relacionadas con TIC. (Ministerio de Defensa, 2017)

Por lo anterior, es de resaltar las labores que vienen desempeñando las Fuerzas Militares respecto a su misión, la cual está enfocada en la Seguridad y Defensa Nacional, en concordancia con las líneas de acción de la Policía Nacional frente a las investigaciones en ciberdelitos. Es por esta situación, que el Centro propuesto debe servir como un elemento articulador de los datos (en especial los contenidos en los sistemas misionales) que requieran los diferentes entes estatales para establecer sus políticas y planes de acción frente a estas situaciones del ciberespacio.

Capítulo 2. Investigaciones judiciales en el ciberespacio

2.1. Delitos informáticos

Para llegar a comprender las normas legales alrededor de la protección de los datos y la información, como bien jurídico tutelado dentro del título VII bis del Código Penal Colombiano, se debe entender el avance que la información ha tenido a través del tiempo, en especial aquella que hace referencia a la informática como información automática, es decir, la información que se procesa a través de medios electrónicos automáticos, entre otras, usando el computador.

En esta gran evolución que se ha visto latente a nivel global, es necesario precisar que la tecnología ha llegado a todos los sectores productivos de la sociedad: económico, político, financiero, social, educativo, de salud, permitiendo mayor facilidad de uso de la información en su recolección, transporte y distribución. Así como la sociedad se ha visto beneficiada con la evolución de los medios a través de los cuales la información se obtiene, transforma y divulga, también es importante anotar que los modos de operar de los delincuentes han evolucionado y esto en relación con los sistemas donde se procesa y se transfiere de forma automática los datos, siendo esto una gran amenaza no sólo para el propio país sino para los demás países ya que se convierte este uso inadecuado de los recursos tecnológicos en un riesgo a nivel transnacional. (Suarez, 2016)

2.2. La ley 1273 del 5 de enero de 2009

En el entendido que el ciberespacio es un ambiente virtual donde se construye y se comparte información, además de encontrar diferentes perfiles de personas que desarrollan actividades variadas, es significativo anotar que también es el ambiente propicio para desarrollar acciones que, por su condición de anonimato, se prestan para estar al margen de la ley. De forma analógica con el ambiente físico en el cual vivimos todos, también existen algunas personas que buscan sacar provecho tanto de sus cualidades negativas como de la excesiva confianza de las demás personas.

Este ambiente virtual es el ideal para servir como medio para el soporte de muchos de los delitos que se cometen en el mundo real o físico, pero se ha hecho especial énfasis en los delitos informáticos representados en la Ley 1273 del 5 de enero de 2009, la cual establece la protección

de la información y de los datos como un bien tutelado. Esta ley, está contenida en dos capítulos, en donde el primero hace referencia a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, donde se encuentran tipificados los siguientes delitos:

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación
- Artículo 269C: Interceptación de datos informáticos
- Artículo 269D: Daño informático
- Artículo 269E: Uso de software malicioso
- Artículo 269F: Violación de datos personales
- Artículo 269G: Suplantación de sitios web para capturar datos personales
- Artículo 269H: Circunstancias de agravación punitiva

En el segundo capítulo, se hace referencia a los delitos relacionados de los atentados informáticos y otras infracciones, así:

- Artículo 269I: Hurto por medios informáticos y semejantes
- Artículo 269J: Transferencia no consentida de activos

A continuación, se ilustra cada uno de los artículos incluidos en esta ley no sin antes advertir que se hace una mirada a la luz del derecho no siendo este el objeto principal del trabajo pero si considerando importante identificar estos elementos por cada uno de los delitos presentados en la ley 1273/2009:

- Artículo 269A. Acceso abusivo a un sistema informático

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo". (Congreso de Colombia, 2009)

Tabla 3. Elementos del delito 269A de la ley 1273 de 2009

Artículo	269A
Delito	Acceso abusivo a un sistema informático
Aspectos vulnerables	Confidencialidad, integridad, disponibilidad de datos y sistemas informáticos
Verbos rectores	Acceder Mantener(se)
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio Tipo penal Mono subjetivo
Sujeto pasivo	Sociedad Usuario del sistema informático afectado
Objeto material	Bien jurídico fenomenológico: Software del sistema informático
Elementos normativos	sin autorización por fuera de lo acordado medida de seguridad contra la voluntad de quien tenga el legítimo derecho
Concurso efectivo	Con los delitos de: - Daño informático - Uso de software malicioso - Violación de datos personales Obstaculización ilegítima de sistema informático o red de telecomunicaciones
Concurso aparente	Con los delitos de: - Hurto por medios informáticos y semejantes - Transferencia no consentida de activos
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación

"El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones". (Congreso de Colombia, 2009)

Tabla 4. Elementos del delito 269B de la ley 1273 de 2009

Artículo	269B
Delito	Obstaculización ilegítima de sistema informático o red de telecomunicación
Aspectos vulnerables	Sistemas informáticos Redes de telecomunicaciones
Verbos rectores	Impedir, obstaculizar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio Mono subjetivo
Sujeto pasivo	Sociedad Usuario del sistema informático afectado
Objeto material	Bien jurídico real: Todos los elementos físicos del sistema informático Bien jurídico fenomenológico: los elementos intangibles del sistema informático y de las redes de telecomunicaciones
Elementos normativos	sin estar facultado normal
Concurso efectivo	Con los delitos de: - Acceso abusivo a un sistema informático - Daño informático - Uso de software malicioso - Terrorismo (art.343 CP)
Concurso aparente	Con los delitos de: - Daño en bien ajeno
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269C. Interceptación de datos informáticos

  "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte". (Congreso de Colombia, 2009)

Tabla 5 Elementos del delito 269C de la ley 1273 de 2009

Artículo	269C
Delito	Interceptación de datos informáticos
Aspectos vulnerables	- Datos informáticos en el origen - Datos informáticos en el destino - Datos informáticos en el interior de un sistema informático - Datos informáticos en las emisiones electromagnéticas que se transporten
Verbos rectores	Interceptar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio Mono subjetivo
Sujeto pasivo	Sociedad: protege la integridad, confidencialidad y disponibilidad de la información y los datos Individuo: vela por la integridad de los derechos de la libertad informática y la intimidad
Objeto material	Bien jurídico fenomenológico: Software del sistema informático
Elementos normativos	sin orden judicial previa sistema informático emisiones electromagnéticas
Concurso efectivo	Con los delitos de: - Acceso abusivo a un sistema informático - Daño informático - Uso de software malicioso
Concurso aparente	Con los delitos de: - Violación ilícita de comunicaciones - Violación de datos personales
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269D. Daño informático

"El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos". (Congreso de Colombia, 2009)

Tabla 6. Elementos del delito 269D de la ley 1273 de 2009

Artículo	269D
Delito	Daño informático
Aspectos vulnerables	- Entrada de datos - Programación - Procesamiento de datos - Salida de datos - Comunicación electrónica
Verbos rectores	Destruir, dañar, borrar, deteriorar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad Titular del sistema informático
Objeto material	Bien jurídico fenomenológico: Datos informáticos, sistema de tratamiento informático, partes del sistema informático
Elementos normativos	sin estar facultado datos informáticos sistema de tratamiento de información partes o componentes lógicos
Concurso efectivo	Con los delitos de: - Acceso abusivo a un sistema informático - Obstaculización ilegítima de sistema informático o red de telecomunicaciones - Interceptación de datos - Uso de software malicioso - Daño en bien ajeno
Concurso aparente	Con los delitos de: - Transferencia no consentida de activos - Violación de datos personales - Falsedad documental - Sabotaje
Tipo subjetivo	Dolo directo o eventual

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269E. Uso de software malicioso

"El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos". (Congreso de Colombia, 2009)

Tabla 7. Elementos del delito 269E de la ley 1273 de 2009

Artículo	269E
Delito	Uso de software malicioso
Aspectos vulnerables	Confidencialidad, integridad, disponibilidad de la información y los datos
Verbos rectores	Producir, traficar, adquirir, distribuir, vender, enviar, introducir, extraer
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad
Objeto material	Bien jurídico fenomenológico: Software malicioso, otros programas de computación de efectos dañinos
Elementos normativos	sin estar facultado para ello software malicioso programa de computación efectos dañinos territorio nacional
Concurso efectivo	Con los delitos de: - Acceso abusivo a un sistema informático - Obstaculización ilegítima de sistema informático o red de telecomunicaciones - Interceptación de datos - Daño informático - Violación de datos personales - Suplantación de sitios web para capturar datos personales
Concurso aparente	Con el delito de: - Transferencia no consentida de activos
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269F. Violación de datos personales

"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes". (Congreso de Colombia, 2009)

Tabla 8. Elementos del delito 269F de la ley 1273 de 2009

Artículo	269F
Delito	Violación de datos personales
Aspectos vulnerables	Intimidad de las personas titulares de los datos Información y datos
Verbos rectores	Obtener, intercambiar, interceptar, emplear, sustraer, modificar, compilar, ofrecer, vender, enviar, divulgar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad Titular de los datos
Objeto material	Bien jurídico fenomenológico: Código personal, dato personal
Elementos normativos	sin estar facultado provecho propio o de un tercero códigos personales datos personales ficheros archivos base de datos medios semejantes
Concurso efectivo	Con los delitos de: - Acceso abusivo a un sistema informático - Uso de software malicioso - Suplantación de sitios web para capturar datos personales - Hurto por medios informáticos y semejantes
Concurso aparente	Con los delitos de: - Interceptación de datos informáticos - Daño informático
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269G. Suplantación de sitios web para capturar datos personales

"El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes… el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza". (Congreso de Colombia, 2009)

Tabla 9. Elementos del delito 269G de la ley 1273 de 2009

Artículo	269G
Delito	Suplantación de sitios web para capturar datos personales
Aspectos vulnerables	Información y datos
Verbos rectores	Diseñar, desarrollar, programar, traficar, vender, ejecutar, enviar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad Titular de los datos
Objeto material	Bien jurídico fenomenológico: páginas electrónicas, enlaces, ventanas emergentes, sistema de resolución de nombres de dominio, ip
Elementos normativos	sin estar facultado para ello páginas electrónicas enlaces ventanas emergentes sistema de resolución de nombres de dominio ip, usuario, banco, sitio personal o de confianza
Concurso efectivo	Con los delitos de: - Violación de datos personales - Hurto por medios informáticos y semejantes - Transferencia no consentida de activos - Estafa
Concurso aparente	Sin información
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269I. Hurto por medios informáticos y semejantes

"El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos". (Congreso de Colombia, 2009)

Tabla 10. Elementos del delito 269I de la ley 1273 de 2009

Artículo	269I
Delito	Hurto por medios informáticos y semejantes
Aspectos vulnerables	Información y datos
Verbos rectores	Apoderar(se)
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad Titular de los datos
Objeto material	Bien jurídico real: cosa mueble (dinero circulante)
Elementos normativos	ajenidad mueble usuario medidas de seguridad informática sistema informático red de sistema electrónico y telemática sistemas de autenticación y autorización
Concurso efectivo	Con los delitos de: - Violación de datos personales - Suplantación de sitios web para capturar datos personales - Falsedad en documento
Concurso aparente	Con los delitos de: - Acceso abusivo a un sistema informático - Secuestro extorsivo
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

- Artículo 269J. Transferencia no consentida de activos

"El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave" (Congreso de Colombia, 2009)

Tabla 11. Elementos del delito 269J de la ley 1273 de 2009

Artículo	269J
Delito	Transferencia no consentida de activos
Aspectos vulnerables	Información y datos
Verbos rectores	**Primera parte:** Transferir **Segunda parte:** Fabricar, introducir, poseer, facilitar
Sujeto activo	Indeterminado (no cualificado) Delito común o de dominio
Sujeto pasivo	Sociedad Titular de los datos
Objeto material	Bien jurídico fenomenológico: cualquier activo
Elementos normativos	manipulación informática artificio semejante transferencia no consentida activo perjuicio programa de computador
Concurso efectivo	Con los delitos de: - Violación de datos personales - Suplantación de sitios web para capturar datos personales
Concurso aparente	Con los delitos de: - Acceso abusivo a un sistema informático - Daño informático - Uso de software malicioso
Tipo subjetivo	Doloso

Nota: Elaboración propia basada en Posada (2017) y Suárez (2016)

Esta ley tiene una especial relación con las normas internacionales, las cuales se describen en la Tabla 12.

Tabla 12. Referencias normativas internacionales

Ley 1273/2009 - Colombia		Normas internacionales			
Artículo	Delito informático	Convenio de Budapest de 2001	Consejo de la Unión Europea, Decisión Marco 2005/222/JAI del 24/02/2005	Directiva 2013/40/UE	Ley Modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática del 2002
269A	Acceso abusivo a un sistema informático	Artículo 2 Acceso ilícito	Artículo 2 Acceso ilegal a los sistemas de información	Artículo 3 Acceso ilegal a los sistemas de información	Sección 5
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Artículo 4 Interferencia de datos Artículo 5 Interferencia de sistemas	Artículo 3 Intromisión ilegal en los sistemas de información Artículo 4 Intromisión ilegal en los	Artículo 4 Interferencia ilegal en los sistemas de información	Sección 6 Daño informático Sección 7 Obstaculización
269C	Interceptación de datos informáticos	Artículo 3 Interceptación ilícita	No hay referencia	Artículo 6 Interceptación ilegal	Sección 8
269D	Daño informático	No hay referencia	No hay referencia	No hay referencia	No hay referencia
269E	Uso de software malicioso	Artículo 6 Abuso de los dispositivos	No hay referencia	Artículo 7 Instrumentos utilizados para cometer las infracciones	Sección 9
269F	Violación de datos personales	No hay referencia	No hay referencia	No hay referencia	No hay referencia
269G	Suplantación de sitios web para capturar datos personales	No hay referencia	No hay referencia	No hay referencia	No hay referencia
269H	Circunstancias de agravación punitiva	No hay referencia	No hay referencia	No hay referencia	No hay referencia
269I	Hurto por medios informáticos y semejantes	Artículo 8. Fraude informático	No hay referencia	No hay referencia	No hay referencia
269J	Transferencia no consentida de activos	Artículo 8. Fraude informático	No hay referencia	No hay referencia	No hay referencia

Nota: Elaboración propia basada en Posada (2017)

Vale la pena decir que esta Ley desarrolla en sus artículos y de forma exclusiva, aquellas situaciones en las cuales la información en su plena expresión es violentada y cómo su afectación puede involucrar personas e instituciones. De esta forma, encontramos una primera aproximación en el ciberespacio de cómo son tratados desde la visión de la ley, este tipo de delitos, incluyendo o representando situaciones que igualmente no son ajenas a lo referenciado como, denegación de servicio, troyanos y phishing, entre otras.

2.3. La investigación de delitos informáticos

La Fiscalía General de la Nación, basado en el Manual de Policía Judicial aplica actuaciones que desarrollan los investigadores con miras a aportar elementos de juicio que les permita a los fiscales estructurar sus casos, mediante el planteamiento de hipótesis y así poder concluir sobre

los hechos jurídicamente relevantes objeto de investigación. Es así, como estos investigadores se valen de procedimientos de obtención de información tanto de fuentes internas como externas, ya sea de sistemas de información formales como de fuentes abiertas tanto en el mundo real como en el virtual.

Por lo que se refiere a la evaluación del impacto de un Centro Cibernético de Investigación en la Fiscalía General de la Nación, es relevante conocer de forma progresiva la evolución que la criminalidad ha tenido y cómo su actuar ha llegado y se ha enquistado en los mecanismos comunicativos del ciberespacio. Debido a esto, es importante descifrar el comportamiento criminal al interior de este mundo virtual y de esta manera entender la importancia del proceso investigativo a favor de la verdad y de la resolución de casos criminales.

En este sentido, se hace referencia a un caso particular relacionado con el uso de la banca virtual sobre los hechos sucedidos entre el 1 de enero de 2016 y el 31 de diciembre de 2017.

Las generalidades se relacionan a continuación:

- 55 casos identificados en las denuncias registradas con diferente NUNC (Número Único de Noticia Criminal)
- Un solo banco afectado con las transacciones efectuadas
- Entidades del Estado afectadas con las transacciones realizadas
- Estos casos se sucedieron en 16 departamentos de Colombia
- Alrededor de $9.000.0000.0000 afectaron las arcas de varios municipios

Lo anterior con el ánimo de comprender de manera general el procedimiento, que al interior de la Entidad no se ha estandarizado, para realizar investigaciones de este tipo. No se sabe si es por falta de información de los procedimientos de policía judicial, por desconocimiento de cómo funciona internet y sus variantes (Deep web, dark web, etc), por las actividades investigativas rutinarias que evitan que los mismos investigadores vayan más allá dentro de este tipo de investigaciones o simplemente, por la falta de herramientas técnicas, investigativas y jurídicas para realizar estas actividades. Estos resultados se podrán observar en el siguiente capítulo de este trabajo, buscando orientar a quienes realizan investigaciones de este tipo de delitos.

Ahora bien, en el caso en mención, se coordinaron actividades tanto de gestión como de policía judicial para tratar de recopilar la mayor cantidad de información relevante para el caso y así, llegar

a conclusiones más asertivas sobre el mismo. Es así, como se inicia con un informe descriptivo de las actividades registradas mediante las denuncias recibidas relacionadas con la banca virtual. Este análisis surge de la utilización de un aplicativo informático adquirido por la Entidad que, combinado con inteligencia artificial, minería de datos e inteligencia de negocios arrojó una clasificación de los procesos judiciales objeto de estudio, a partir del campo "delito" de la base de datos del sistema misional de la entidad SPOA (Sistema Penal Oral Acusatorio) y del campo de información no estructurada correspondiente al campo "descripción de los hechos" del mismo sistema. El proceso en este sentido permitió observar que algunas denuncias fueron registradas fuera de la clasificación que ofrece el título VII bis del CPP, es decir, delitos como peculado, estafa y hurto fueron concebidos dentro del proceso investigativo de delitos informáticos en el marco de actuación de la banca virtual mencionada.

A partir de allí, se realizan inspecciones a los procesos para identificar elementos que permitan hacer relaciones entre la data obtenida de cada uno. Con las inspecciones realizadas, se elabora una matriz que permite visualizar los aspectos de todos y cada uno de los procesos generando un escenario adecuado para el analista de información. Con la información organizada, estructurada y con una calidad mínima de la información obtenida, se procede a realiza un informe de contexto para lograr la asociación de los casos y establecer estrategias que lleven al seguimiento, identificación y judicialización de los diferentes actores en este proceso judicial.

Luego, se elaboran órdenes a la policía judicial para confirmar la información obtenida y obtener nuevos elementos dentro de la investigación, basado en los actos de indagación e investigación los cuales son ordenados de forma previa por el fiscal del caso y con control posterior del Juez de Garantías. A continuación, se relacionan todos los actos relacionados de indagación e investigación destacando aquellos que son utilizados dentro del proceso de investigación de los delitos informáticos:

Tabla 13. Actos de policía judicial utilizados en investigación criminal

Acto de policía judicial	Utilizado en investigaciones de policía judicial
Registros y allanamientos	
Retención, examen y devolución de correspondencia	
Interceptación de comunicaciones telefónicas y similares	
Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes	X
Vigilancia y seguimiento de personas	
Vigilancia de cosas	
Análisis e infiltración de organización criminal	
Actuación de agentes encubiertos	
Entrega vigilada	
Búsqueda selectiva en base de datos que involucran al indiciado e imputado	X
Exámenes de ADN que involucren al indiciado o al imputado	

Nota: Elaboración propia

Como resultado se presenta el respectivo informe de policía judicial y se hace el análisis para establecer números de cuentas, titulares de las cuentas de destino que han sido utilizadas en el proceso de transferencia no consentida de activos, direcciones ip que han sido utilizadas en este proceso y a partir de allí continuar con las labores de investigación, destinadas a ubicar, individualizar e identificar a los actores de esta cadena delincuencial.

Los actores a que se hace referencia corresponden a los identificados en este caso en particular y cuya estructura piramidal se muestra en la Gráfica 5.

Gráfica 5. Estructura de una organización cibercriminal

Fuente: Elaboración propia

A pesar de tener una posible estructura delincuencial, que permita a través de las investigaciones realizadas poder desmantelarla, las investigaciones se están quedando en el primer escalón de la pirámide. Esto debido a que los actores de este escaño son los más visibles por su participación mediante el uso de cuentas bancarias.

¿Pero, hasta dónde esta actuación del ente acusador es el adecuado para la intervención en las estructuras criminales que aprovechan el uso de los medios electrónicos para cometer estos ilícitos? Es en este punto, donde el impacto de un Centro Cibernético de Investigación puede llegar a fortalecer no sólo los procedimientos, sino el uso y apropiación de herramientas tecnológicas que ahonden en las investigaciones que realizan los grupos de policía judicial de la Fiscalía General de la Nación.

Para este caso, se ha identificado como delito el tipificado en la norma como 269I: Hurto por medios informáticos y semejantes y cuyas actuaciones aún siguen en curso para establecer elementos materiales probatorios suficientes y así lograr la individualización e identificación de los presuntos responsables ya sea a nivel individual o dentro del marco de organizaciones criminales. No obstante, este delito puede estar en concurso con el 269A: Acceso abusivo a un sistema informático y con el 269J: Transferencia no consentida de activos. Lo anterior, toda vez

que para sustraer el dinero se realizan transferencias de dinero las cuales no son autorizadas por quien es dueño del bien jurídico, además de ser accesado el sistema sin la previa autorización para hacerlo.

A partir de lo anterior, se hace necesario que se generen cambios en los planteamientos tradicionales, en especial cuando se hace estudio de los crímenes y se realiza el seguimiento respectivo. En este sentido, una persona puede realizar un sinnúmero de tareas que pueden o no ser anónimas y que debido a la conexión en la red o ciberespacio trascienden las situaciones del mundo real al mundo virtual, creando el medio ideal para el delincuente (Giménez-Salinas y González, 2016).

Ahora, el anonimato es uno de los factores que favorece el actuar en el ciberespacio y por eso, centra especial atención su intervención, sobre todo, cuando este factor dificulta las acciones de seguimiento, vigilancia e individualización que tradicionalmente se vienen realizando en el contexto físico de investigación criminal. Este anonimato, los actos y comunicaciones generados en la red son inherentemente rastreables, además de contar con que el emisor no aporta datos personales, pero sus comunicaciones se registran y pueden ser rastreables. De igual forma, supone un mayor reto para la investigación criminal y ejemplifica este actuar con el uso de recursos en la red como la red TOR, en donde se anonimiza las acciones de los usuarios de forma casi total, a tal punto que es de las situaciones más complicadas para establecer algún parámetro que permitir hacer seguimiento de algún tipo de comunicación. Ahora bien, se vuelve un reto el hecho de identificar una escena de cibercrimen cuando se desvía la comunicación hacia la víctima, debido a la técnica minuciosa que utiliza el victimario en la búsqueda de no dejar rastro alguno de sus cometidos. Podemos apreciar en estas líneas, la descripción de actividades que necesariamente deben tener el conocimiento y experticia tecnológica de quien comete actos delictivos, esto al margen de la utilización adecuada de los medios tecnológicos para el acercamiento a las víctimas. (Chawki, 2006 citado por Giménez-Salinas y González, 2016)

Las personas que utilizan el ciberespacio como un medio para hacer sus actos delictivos, aprovechan el anonimato para facilitar su modus operandi haciendo uso de identidades falsas o utilización de perfiles que distan de los que en la realidad tienen. Por este motivo, se hace necesario incluir capacidades de ciber inteligencia para la adquisición y análisis de información que permitan identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los

atacantes que permitan tomar decisiones y así, lograr la organización de la información vital acerca de las investigaciones judiciales que se adelanten. (Polanco, 2016)

Es de anotar que quienes ejecutan estas acciones delictivas están considerados como ciberdelincuentes, pero su reseña está orientada a cometer delitos informáticos aprovechando la vulnerabilidad que tiene las personas en el uso de los dispositivos que tienen, como celulares y portátiles y en donde la información, por lo general sensible, no tiene las condiciones de seguridad adecuadas. (Jesús, N. D, 2010).

Así mismo, se genera una percepción que está a cargo de la persona que comete los delitos y que consiste en minimizar la condición de ser detectado, identificado y posteriormente, detenido. (García, 2016)

2.4. Otros delitos que utilizan el ciberespacio

Es de anotar que en el ciberespacio no sólo se desarrollan las acciones que afectan los datos y la información propuestas en la Ley 1273 de 2009, sino que se ejecutan acciones que pueden llegar a ser tipificadas dentro de la normativa colombiana, por su interacción con las redes informáticas, en especial, la utilizada como internet y que utilizan los medios tecnológicos como medio o como fin. Al respecto, se hace una referencia de estas situaciones:

Trata de personas:

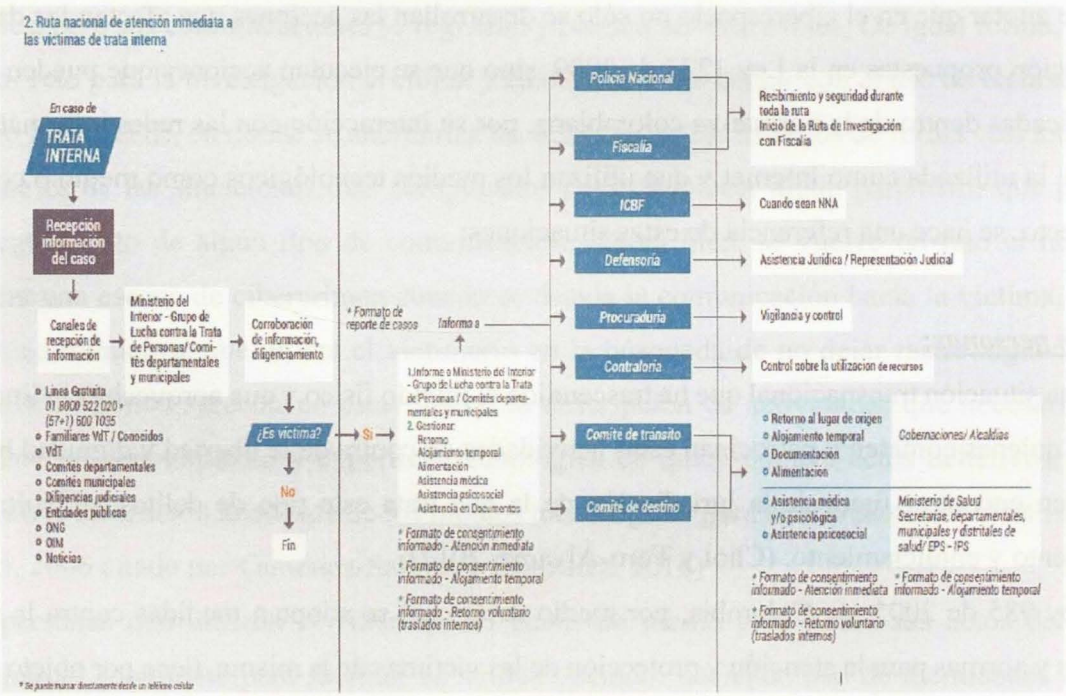
Es una situación transnacional que ha trascendido el mundo físico y que aprovecha el virtual, toda vez que quienes cometen y patrocinan estas actividades en contra de la libertad y dignidad humana, se pueden encontrar fuera de la jurisdicción de la que trata este tipo de delitos, dificultando su seguimiento y enjuiciamiento. (Choi y Toro-Álvarez, 2017)

La ley 985 de 2005, en Colombia, por medio de la cual se adoptan medidas contra la trata de personas y normas para la atención y protección de las víctimas de la misma, tiene por objeto adoptar medidas de prevención, protección y asistencia para garantizar el respeto de los derechos humanos de las víctimas. (Congreso, 2005) En este sentido, existen redes criminales identificadas desde las investigaciones que lleva la Fiscalía General de la Nación, las cuales han extendido su accionar al ámbito del ciberespacio al diversificar su modus operandi.

El tráfico de personas ha impactado las víctimas y hoy día, aún más, al utilizar el ciberespacio para captar estas víctimas y a sabiendas que los controles por parte de las autoridades es limitado, en su mayoría por falta de conocimiento y de herramientas adecuadas para esta tarea. Prueba de ello, es el plan de acción propuesto por el Ministerio de las Tecnologías de la Información y las Comunicaciones, al proponer estudios para funcionarios del Estado, relacionado con seguridad y defensa en el ciberespacio.

El estado colombiano ha venido, de forma colaborativa entre las entidades que tienen injerencia en estas actividades, construyendo la ruta para asistir a las víctimas de la trata de personas, como se muestra en la Gráfica 6.

Para este tipo de delitos es necesario identificar las normas sobre las cuales se establece el marco jurídico, así como se muestra en la Tabla 14. En este sentido, se potencia la condición de captación cuando se utilizan los medios tecnológicos, ya que se da un mayor aprovechamiento de las redes sociales, como medio principal para llegar a las víctimas.



Gráfica 6. Ruta Nacional de Asistencia Inmediata a las víctimas de trata interna

Fuente: UNODC, 2013

Tabla 14. Normativa sobre trata de personas

NORMA	OBJETO	GENERALIDAD
Protocolo de Palermo	Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional	Los fines del presente Protocolo son: a) Prevenir y combatir la trata de personas, prestando especial atención a las mujeres y los niños; b) Proteger y ayudar a las víctimas de dicha trata, respetando plenamente sus derechos humanos; y c) Promover la cooperación entre los Estados Parte para lograr esos fines.
Ley 985 de 2005	Por medio de la cual se adoptan medidas contra la trata de personas y normas para la atención y protección de las víctimas de la misma.	La interpretación y aplicación de la presente ley se orientará por los siguientes principios: 1. El Estado tiene la obligación de actuar con la diligencia debida para prevenir la trata de personas, investigar y procesar a quienes la cometen, y ayudar y proteger a las víctimas de la misma. 2. La acción estatal en este campo tiene como propósito impedir la vulneración de los derechos humanos por razón de la trata de personas.
Decreto 1069 de 2014	Por el cual se reglamenta parcialmente la Ley 985 de 2005	El presente decreto tiene por objeto reglamentar las competencias, beneficios, procedimientos y trámites que deben adelantar las entidades responsables en la adopción de las medidas de protección y asistencia a las personas víctimas del delito de la trata de personas.
Artículo 188-A. CP	Trata de pesonas. El que capte, traslade, acoja o reciba a una persona, dentro del territorio nacional o hacia el exterior, con fines de explotación, incurrirá en prisión de trece (13) a veintitrés (23) años y una multa de ochocientos (800) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes.	se entenderá por explotación el obtener provecho económico o cualquier otro beneficio para sí o para otra persona, mediante la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre, la explotación de la mendicidad ajena, el matrimonio servil, la extracción de órganos, el turismo sexual u otras formas de explotación.

Nota: Elaboración propia, basado en UNODC (https://www.unodc.org/documents/colombia/2016/marzo/cartilla_trata.pdf)

Violencia sexual:

Si bien es cierto que las víctimas pueden ser personas mayores, los datos que informa Unicef indican que el 80% de los jóvenes sienten un nivel de peligro cuando navegan por internet y sienten miedo de ser acosados sexualmente.

El Convenio del Consejo de Europa, en el artículo 23, hace referencia a la captación de niños y niñas con fines sexuales y la correspondiente protección que se debe tener para evitar ser explotados y abusados. La dinámica de los depredadores sexuales en internet inicia con la seducción a través de redes sociales, correos electrónicos y aplicaciones de chat y después de tener la paciencia suficiente y crear una buena relación de confianza, puede terminar con encuentros físicos para culminar con actos de carácter sexual. Este tipo de conductas no están tipificadas como delitos informáticos, pues no afectan el bien jurídico tutelado en el capítulo VII bis del CP, pero si utilizan los elementos tecnológicos que permiten a través de comunicaciones acercar a la víctima y el victimario. Además, que pueden llegar a configurar se dentro de la temática de pornografía infantil, al margen que pueda ser tratado como un delito independiente o en concurso con este. (Consejo de Europa, 2011)

Tabla 15. Normativa de delitos sexuales en Colombia

No	Norma	Fecha de Expedición	Tema que regula
1	Ley 765	31 de Julio de 2002	"Por medio de la cual se aprueba el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, adoptado en Nueva York, el veinticinco (25) de mayo de dos mil (2000)."
2	Ley 906	31 de Agosto de 2004	"Por la cual se expide el Código de Procedimiento Penal". Artículos 205, 206, 207, 208, 209, 210, 210, 213, 231, 214, 217, 217, 218, 219, 219, 219, 188 y 188.
3	Ley 679	3 de Agosto de 2001	"Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución".
4	Ley 1236	23 de Julio de 2008	"Por medio de la cual se modifican algunos artículos del Código Penal relativos a delitos de abuso sexual"
5	Ley 1146	10 de Julio de 2007	"Por medio de la cual se expiden normas para la prevención de la violencia sexual y atención integral de los niños, niñas y adolescentes abusados sexualmente".
6	Ley 1154	4 de Septiembre de 2007	"Por la cual se modifica el artículo 83 de la Ley 599 de 2000, Código Penal".
7	Ley 1236	23 de Julio de 2008	"Por medio de la cual se modifican algunos artículos del Código Penal relativos a delitos de abuso sexual".
8	Ley 1257	4 de Diciembre de 2008	"Por la cual se dictan normas de sensibilización, prevención y sanción de formas de violencia y discriminación contra las mujeres, se reforman los Códigos Penal, de Procedimiento Penal, la Ley 294 de 1996 y se dictan otras disposiciones".
9	Ley 1329	17 de Julio de 2009	"Por medio del cual se modifica el Título IV de la Ley 599 de 2000 y se dictan otras disposiciones para contrarrestar la explotación sexual comercial de niños, niñas y adolescentes".
10	Ley 1336	21 de Julio de 2009	"Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes".
11	Ley 1453	24 de Junio de 2011	"Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad".

Nota: ICBF (*https://www.icbf.gov.co/programas-y-estrategias/proteccion/violencia-sexual*)

Acoso cibernético y matoneo digital:

Aunque parecieran dos actividades sinónimas por la similitud en sus nombres, es de anotar que el acoso cibernético es conocido como cibertalking y es aplicado cuando un adulto acosa a otro adulto, ya sea a través de los medios conocidos de comunicación utilizados en internet o ya sea obteniendo información en internet para luego, ubicar a la víctima en el mundo real. Dentro de las tácticas más utilizadas están: vandalizar un motor de búsqueda y amenazar el empleo, la reputación o seguridad de la víctima. (Choi y Toro-Álvarez, 2017)

A su vez, el matoneo digital es conocido como ciberbullying y aplica cuando el acoso es dado hacia un niño, niña o adolescente ya sea por parte de uno de sus pares o por cualquier otra persona. En las actividades que más son utilizadas por quienes promueven este tipo de prácticas están: el acoso, las amenazas, difamación, rechazo, publicación o envío de imágenes personales. (Choi y Toro-Álvarez, 2017)

En el CP no hay una normativa que permita establecer las condiciones en que se puede configurar un delito con las características antes mencionadas, creando un vacío jurídico y abriendo la brecha para la comisión de otras actividades en contra de la persona acosada como, por ejemplo, llevar a la víctima al suicidio. (Posada, 2017)

Algunas de las situaciones que se presentan bajo esta modalidad se describen a continuación:

- Grooming: Acoso sexual extorsivo por internet

- Sexting: Acoso mediante el uso de mensajería instantánea, cuando se realiza el envío de fotografías con contenido sexual

Tráfico de drogas:

En este tema, el mercadeo de cualquier tipo de estupefaciente debe garantizar el anonimato y las condiciones adecuadas de quien comercializa y de quien adquiere estos productos. Es aquí, donde se hace referencia a la deep web, como aquella parte de la red que contiene información, herramientas y páginas web que no pueden ser indexadas por ningún navegador de los que tradicionalmente se utilizan, como google, yahoo, etc.

La mayoría de las drogas disponibles en internet, pueden ser compradas fácilmente con una simple y rápida búsqueda. Al igual que otro tipo de compras, quien desea obtener el producto recibe información de este con las calificaciones recibidas por otros clientes, ubicados a través del mundo y utilizando medios de pago como Paypal o tarjetas de crédito. Las dificultades se presentan en temas de jurisdicción, a pesar de haber sido identificado el tráfico de estas sustancias, así como a los compradores y distribuidores. (Guardian, 2014 citado por Choi y Toro-Álvarez, 2017)

Uno de los principales sitios reconocidos en internet por ser un sitio dedicado al tráfico de estupefacientes se llamó "silk road", el cual era un mercado clandestino para las drogas ilegales, principalmente la cocaína y heroína, además ofrecía servicios de homicidio por encargo. Este sitio era un servicio que de forma oculta operaba bajo la funcionalidad de Tor, el navegador utilizado en la Deep web para anonimizar la navegación y evitar el control de tráfico en la red.

Una vez revisados las anteriores situaciones y habiendo hecho referencia a la Deep web, como el medio adecuado para evitar dejar rastros que permitan identificar a quienes operan bajo operaciones ilícitas, a continuación, se detallan algunas de las actuaciones que están al margen de la ley y que aprovechan estos recursos tecnológicos para potenciar estos hechos:

1. Comercialización de drogas
2. Comunicación terrorista
3. Pornografía tanto legal como ilegal, con adultos e infantil
4. Venta de información clasificada
5. Servicios de sicariato
6. Fabricación y comercialización de armas
7. Foros de información en busca de víctimas

8. Piratería de libros, música, películas
9. Fabricación y comercialización de software (malware)
10. Páginas para comprar o fabricar armas

2.5. Sistema de información misional SPOA

La Fiscalía General de la Nación, a partir de la expedición de la Ley 906 del 31 de agosto de 2004, por la cual se expide el Código de Procedimiento Penal tenía un gran reto a nivel tecnológico y era la implementación y puesta en funcionamiento de un sistema de información que permitiera la funcionalidad extensa del manejo de información propuesta en la ley mencionada. Este sistema fue denominado SPOA, por sus siglas del Sistema Penal Oral Acusatorio y cuenta con la infraestructura tecnológica necesaria para el registro, almacenamiento, consulta y generación de informes necesarios dentro de las actuaciones judiciales dentro del proceso misional de la Entidad. Este sistema cuenta con siete módulos, como lo muestra la Gráfica 12, así:

- Cinco (5) para el registro de información
- Uno (1) relacionado con la administración del sistema (cuentas de usuario y opciones de seguridad)
- Uno (1) relacionado con la ayuda del sistema, obteniendo información en línea

Gráfica 7. Pantalla principal del SPOA

Fuente: Fiscalía General de la Nación, 2016

La descripción de cada uno de los módulos se relaciona a continuación:

- Gestión policía judicial: Permite registrar las noticias criminales que recibe la policía judicial, relacionar bienes e intervinientes con esas noticias y asignarles los funcionarios que estarán a cargo de las mismas. La noticia criminal es registrada e identificada con un número de 21 dígitos llamado NUNC (Número Único de Noticia Criminal).

- Registro de actuaciones: Aquí se encuentran las actuaciones procesales realizadas por fiscales, jueces y policía judicial en las diferentes etapas del proceso penal (indagación, investigación, imputación, juicio). Estas actuaciones están asociadas con los indiciados y los delitos relacionados con estos.

- Reparto: En este módulo se asignan los casos a los funcionarios de policía judicial y fiscales a cargo de estos casos. Existe el reparto manual, automático y reasignación. (Fiscalía General de la Nación, 2016)

- Administración del almacén: Permite tener el control de los elementos ingresados al almacén de evidencias, previo registro en los formatos de policía judicial y con los requerimientos y exigencias de la cadena de custodia.

- Consultas e informes: Se realizan las consultas de acuerdo con los diferentes criterios, como consulta del reparto de los casos, búsquedas por personas, ya sean funcionarios de la fiscalía (investigadores o fiscales) o indiciados.

2.6. Algunos datos de interés

La Fiscalía General de la Nación propone un proyecto de ley para liberar a los niños de las drogas, castigar con rigor a los reincidentes y sancionar los ciberdelitos, estos últimos como nueva forma de criminalidad. Una de las medidas presentadas en esta propuesta que fue socializada con los mandatarios locales, regionales y nacionales, describiendo la mutación de los fenómenos conocidos de criminalidad, hace relación con las medidas para controlar la cibercriminalidad y garantizar la seguridad ciudadana. El Censo Delictivo de la Fiscalía General de la Nación, es un instrumento de comunicación relacionado con el número de actividades delictivas registradas en el sistema de información de la Entidad y sus elementos complementarios como regiones, modus operandi, indiciados, todo esto para dar luces sobre cómo actuar sobre estos fenómenos. Uno de los informes de 2018, indica que, en el primer semestre del año, las denuncias por delitos informáticos crecieron en un 69.92% frente al mismo periodo del año anterior. (Fiscalía, 2018)

La iniciativa presentada propone la penalización de algunas formas de sexting con prisión de 6 a 10 años, para quien con la intención de causar daño y sin la autorización del titular del contenido, publique, divulgue o revele a través de cualquier medio, imágenes o grabaciones audiovisuales de la actividad sexual de una persona. La Fiscalía propone que en estas circunstancias de sexting, la extorsión sea una causal de agravación. (Fiscalía, 2018)

Ahora bien, es necesario conocer cómo en los últimos años se han comportado los delitos informáticos que han sido denunciados en la Fiscalía General de la Nación para conocer si han crecido o decrecido. La temporalidad está dada desde el 1 de enero de 2015 al 30 de junio de 2018

con un reporte total de 28.960 delitos, bajo el título "De la protección de la información y los datos". A continuación, se muestran diferentes clasificaciones de esta información, de tal manera que se puedan ilustrar las situaciones respecto a estos delitos. En la Gráfica 8, se muestran el incremento de los delitos en los últimos 5 años. (Fiscalía, 2016)

Gráfica 84. Total de delitos informáticos por año

Fuente: Elaboración propia

Como se puede observar, desde los últimos cinco años se han venido incrementando los delitos que se tipifican en la Ley 1273 de 2009. Tan sólo en el primer semestre de 2018 ya se han superado los valores de los dos primeros años de la muestra, su incremento ha sido del 180% aproximadamente.

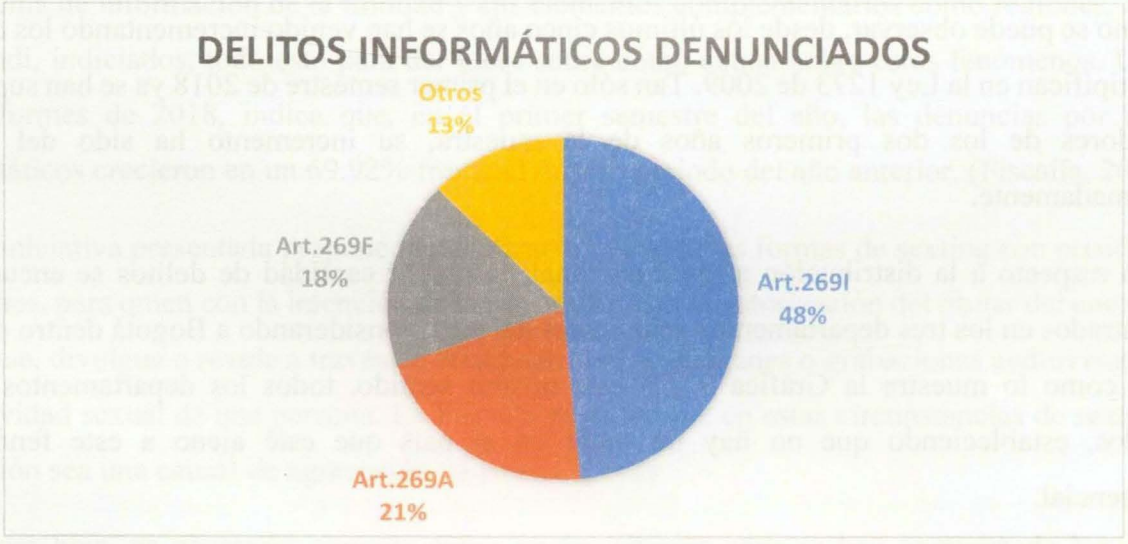
Con respecto a la distribución a nivel nacional, la mayor cantidad de delitos se encuentran concentrados en los tres departamentos principales del país, considerando a Bogotá dentro de este grupo, como lo muestra la Gráfica 9. En este mismo sentido, todos los departamentos están incluidos, estableciendo que no hay un lugar en el país que esté ajeno a este fenómeno delincuencial.

Gráfica 9. Total de delitos informáticos por departamento

Fuente: Elaboración propia

Para tener un mejor entendimiento de los delitos que han sido reportados a través de las denuncias realizadas en la Fiscalía General de la Nación, se muestra en la Gráfica 15 el porcentaje de los delitos en los últimos años.

Es importante conocer cuáles son los delitos más denunciados, para así, aplicar políticas de control respecto a los mismos, las cuales deben ser prioridad de la Entidad toda vez que los delitos informáticos vienen en aumento como se ha visualizado anteriormente.



Gráfica 5. Delitos informáticos denunciados

Fuente: Elaboración propia

2.7. Sectores administrativos del Estado Colombiano

Existe una clasificación de los sectores administrativos con los que cuenta el Estado colombiano y los cuales están articulados con los aspectos operativos y misionales de la Fiscalía General de la Nación, por ser este un órgano transversal a todos los anteriores. Estos sectores son:

- Sector del interior
- Sector relaciones exteriores
- Sector Hacienda y Crédito Público
- Sector Justicia y del Derecho
- Sector de la Defensa Nacional
- Sector Agropecuario, pesquero y de desarrollo rural
- Sector salud y de la protección social
- Sector del trabajo
- Sector Minas y Energía
- Sector de Comercio, Industria y turismo
- Sector Educación Nacional
- Sector Ambiente y desarrollo sostenible
- Sector vivienda, ciudad y territorio
- Sector de las Tecnologías de la Información y las Comunicaciones
- Sector transporte
- Sector cultura
- Sector Presidencia de la República
- Sector de Planeación
- Sector Función Pública
- Sector Inclusión Social y reconciliación
- Sector Inteligencia estratégica y contrainteligencia
- Sector Información estadística
- Sector Administrativo del Deporte
- Sector Ciencia y Tecnología (Función Pública, 2019)

Se destacan los sectores de Justicia y del Derecho, de la Defensa Nacional, de las Tecnologías de la Información y las Comunicaciones y de Inteligencia estratégica y contrainteligencia, los cuales tiene un aspecto en común relacionado con la seguridad y defensa del país, en especial, la protección que se merece la ciudadanía y las infraestructuras críticas del país.

Por eso, la importancia que la Entidad cuente con un Centro Cibernético de Investigación, que provea a cada uno de esto sectores, la información pertinente respecto al estado de ciberdelincuencia, a través de los registros de información en los sistemas misionales internos y que permita la interacción colaborativa entre las entidades que tiene en su misionalidad la defensa y seguridad del Estado colombiano.

Capítulo 3. Datos descriptivos de la situación actual

El Centro Cibernético de Investigación propuesto, debe proveer las estrategias necesarias para desarrollar las actividades que materialicen las actuaciones ordenadas no sólo contra delitos que tengan afectación en el activo conocido como información sino contra delitos que en su configuración incluyan procedimientos tecnológicos, involucrando medios digitales actuales, como redes sociales y sitios de publicación pública de información. Además, debe proveer los procedimientos necesarios para adquirir, retener y fortalecer las competencias que le permitan a la Fiscalía General de la Nación ser un actor activo en los eventos decisivos en la lucha contra la cibercriminalidad en Colombia. (Fiscalía General de la Nación, 2016)

En este sentido, este Centro debe contar con los aspectos relevantes que permitan impulsar y evaluar las variables necesarias para un correcto funcionamiento y generación de procesos, procedimientos y protocolos para que sirva como eje fundamental en la toma de decisiones respecto a los ciberdelitos en Colombia, siendo importante que estos aspectos estén enmarcados en las competencias seleccionadas dentro de los componentes de capacidad DOMPI. (Fiscalía General de la Nación, 2006)

Ahora bien, el impacto que debe causar en el ecosistema judicial debe fortalecer las acciones que se vienen ejecutando en materia de investigación y para ello, se deben definir las capacidades que apalanquen la integración de las instituciones del Estado encargadas de la seguridad ciudadana y la defensa nacional.

Es así, como las necesidades del Centro deben estar alineadas con el suministro de información procesada, a partir del análisis desde la acción criminal y así poder proveer a las demás instituciones los insumos precisos para la toma de decisiones a nivel estratégico, táctico y operativo. Lo anterior, en concurso con las capacidades de las demás entidades tanto públicas como privadas que tengan corresponsabilidad en la seguridad del país.

3.1. Diagnóstico de necesidades del Centro Cibernético de Investigación

Este diagnóstico es un proceso donde es indispensable analizar y sintetizar aquellas condiciones identificadas sobre las necesidades del Centro. Estas necesidades están planteadas desde las capacidades señaladas en el DOMPI y sobre las cuales el Centro debería operar, buscando optimizar sus recursos, tener mayor cobertura a nivel administrativo y operativo, contemplar aspectos de infraestructura e implementar herramientas de investigación.

En este sentido, se diseña una encuesta como instrumento de recolección de datos que permite concentrar las opiniones, conocimientos y experiencias de quienes son encuestados y poder visibilizar y viabilizar soluciones que lleven a la Fiscalía General de la Nación a ser partícipe activo de las investigaciones judiciales en el ciberespacio. (Fiscalía General de la Nación, 2016)

Debido a que este diseño es de carácter general, los resultados obtenidos serán necesarios para definir las capacidades con que se debe preparar la Entidad para brindar herramientas a quienes desarrollan las investigaciones relacionadas con delitos que utilizan la tecnología como medio o como fin y que requieren del ciberespacio para realizar estas actividades. Así mismo, se puede llegar a un acercamiento sobre las condiciones sobre las cuales va a operar el Centro de Investigación y poder plantear hipótesis explicativas que avalen la pertinencia del mismo.

Se tiene proyectado para obtener esta información, elaborar un diagnóstico primario que permita concebir los recursos y capacidades actuales de la Entidad con respecto a las investigaciones que tienen pertinencia en el ciberespacio y para ello, se apoyará en un cuestionario que llegue a dimensionar estas capacidades.

De igual forma, se debe recopilar la información a nivel documental que soporte los procesos, procedimientos, protocolos y demás, que apoyen las actuaciones que, desde la parte operativa a nivel de investigación, se adelanta respecto a los delitos en el ciberespacio, ya seas informáticos o que tengan relación con otro tipo de delitos que utilicen el ciberespacio como medio para su cometido.

La evaluación, realizada mediante un cuestionario de 20 preguntas, está dirigido especialmente a los investigadores, analistas, fiscales y peritos que en el diario quehacer, conocen de

investigaciones que tienen como línea base la tecnología ya sea como medio o como fin. El universo de esta selección es de 120 personas que a nivel nacional conforman en cada una de las 35 seccionales de la Entidad, este grupo de expertos en el tema de delitos informáticos.

Una vez aplicado el cuestionario en mención, se obtuvo respuesta de 85 personas que participaron de acuerdo con lo que han vivenciado desde cada uno de sus grupos.

A continuación, se presenta el resultado cuantitativo por cada una de las preguntas formuladas, a fin de destacar los aspectos sobre los cuales se basaron las preguntas y cómo podrían servir de apalancamiento en las actuaciones judiciales dentro de las investigaciones ordenadas por los fiscales.

El cuestionario se estructuró de la siguiente forma, teniendo en cuenta que su clasificación está de acuerdo con las competencias definidas en el modelo de componentes de capacidad DOMPI, así.

1. DOCTRINA
    a. Preguntas 1, 2, 3
2. ORGANIZACIÓN
    a. Preguntas 4, 5, 6 y 7
3. MATERIAL Y EQUIPO
    a. Preguntas 8, 9, 10, 11 y 12
4. PERSONAL
    a. Preguntas 13, 14, 15 y 16
5. INFRAESTRUCTURA
    a. Preguntas 17, 18, 19 y 20

De igual forma se describe a continuación la estructura del cuestionario aplicado, así:

Metodología

El cuestionario aplicado en el desarrollo de este trabajo, se basa en el método analítico-descriptivo, donde se identificarán aspectos relevantes de la situación relacionada con las temáticas ciber en la Entidad y se analizará su pertinencia y resultado. Respecto al criterio descriptivo, se relacionarán

los resultados generados por cada pregunta en el contexto de investigación y análisis criminal de la Entidad.

Esta encuesta pretende identificar los aspectos principales que la Entidad debe enfrentar en las investigaciones sobre delitos que afecten la información y los datos, consignados en la Ley 1273 de 2009 y así, establecer las capacidades con que debería contar, al implementar un Centro Cibernético de Investigación.

La encuesta está dividida en 5 partes, cada una de las cuales corresponde a las capacidades relacionadas en el modelo DOMPI y una parte adicional que señala aspectos generales de quien realiza la encuesta.

Población:

La población a quién está dirigida la encuesta corresponde a los investigadores y fiscales que desde la variable de delitos informáticos manejan este tipo de situaciones a nivel nacional.

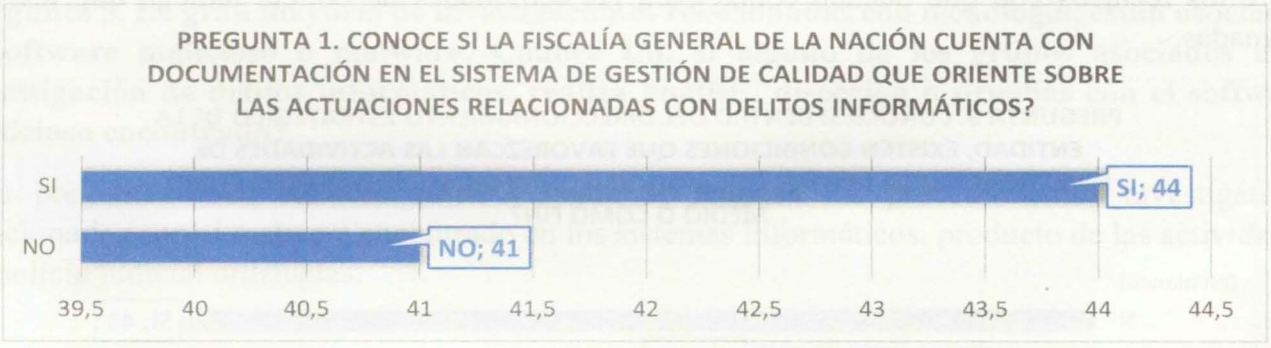
Resultados:

A continuación, se presentan los resultados obtenidos de cada una de las preguntas realizadas:

CUESTIONARIO APLICADO

Pregunta 1. Conoce si la Fiscalía General de la Nación cuenta con documentación en el sistema de gestión de calidad que oriente sobre las actuaciones relacionadas con delitos informáticos?

Esta pregunta pretende establecer el conocimiento que tiene los funcionarios tanto fiscales como de policía judicial acerca de la documentación que avala sus actuaciones, ya sea desde el Manual de procedimientos de la Fiscalía u otros similares.



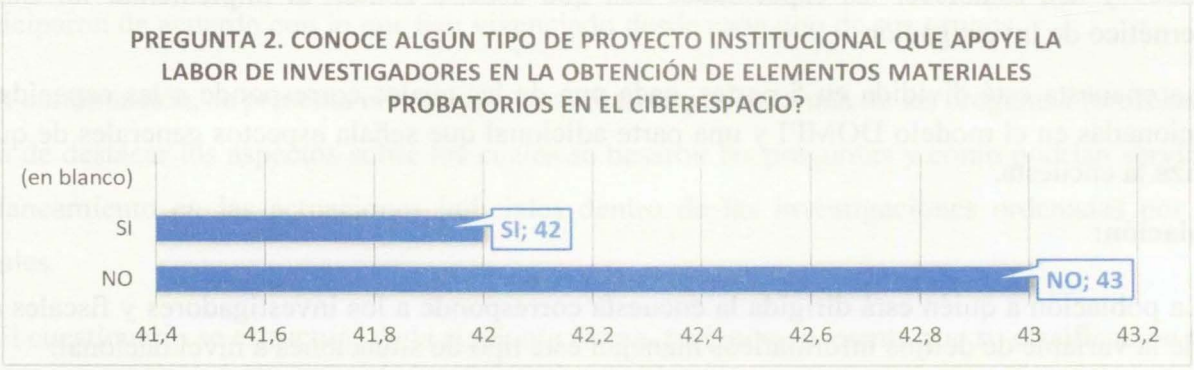
Gráfica 11. Pregunta 1 Encuesta Ciber

Fuente: Elaboración propia

Se puede apreciar que no existe una tendencia hacia el conocimiento de esta documentación, ya que 1 de cada 2 entrevistados dicen conocer este tipo de documentos.

Pregunta 2. Conoce algún tipo de proyecto institucional que apoye la labor de investigadores en la obtención de elementos materiales probatorios en el ciberespacio?

Con esta pregunta se pretende establecer los recursos que conocen los investigadores acerca de los procedimientos en el ciberespacio, relacionados con el manejo de los elementos materiales probatorios.



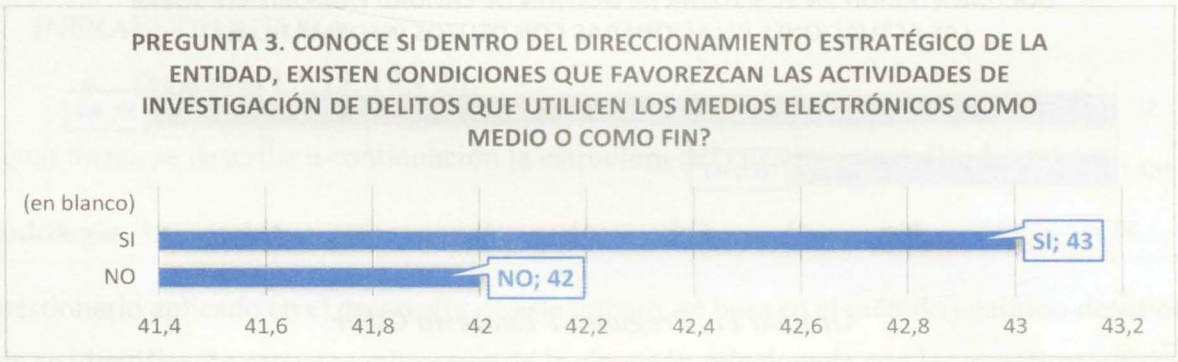
Gráfica 126. Pregunta 2 Encuesta Ciber

Fuente: Elaboración propia

Se observa como uno de cada dos investigadores dice conocer acerca de los procedimientos de recolección de los elementos materiales probatorios en el ciberespacio.

Pregunta 3. Conoce si dentro del Direccionamiento Estratégico de la Entidad, existen condiciones que favorezcan las actividades de investigación de delitos que utilicen los medios electrónicos como medio o como fin?

Esta pregunta está encaminada a establecer sobre el conocimiento que tienen los investigadores sobre los recursos con que pueden contar para las actividades de policía judicial que les son asignadas.



Gráfica 137. Pregunta 3 Encuesta Ciber

Fuente: Elaboración propia

No todos los investigadores conocen los recursos que ofrece la Entidad para apoyar sus actividades, interpretando esto como un desinterés por las líneas de acción que son trazadas desde la planeación misma de la Entidad, ya que es desde allí que son trazados los objetivos estratégicos.

Pregunta 4. Conoce los perfiles criminales de los ciberdelincuentes?

Esta pregunta, ya se especializa en la temática de la cibercriminalidad y busca establecer si los funcionarios que conocen de estos aspectos tienen claro los perfiles de los ciberdelincuentes, para así poder establecer similitudes, diferencias y comportamientos.

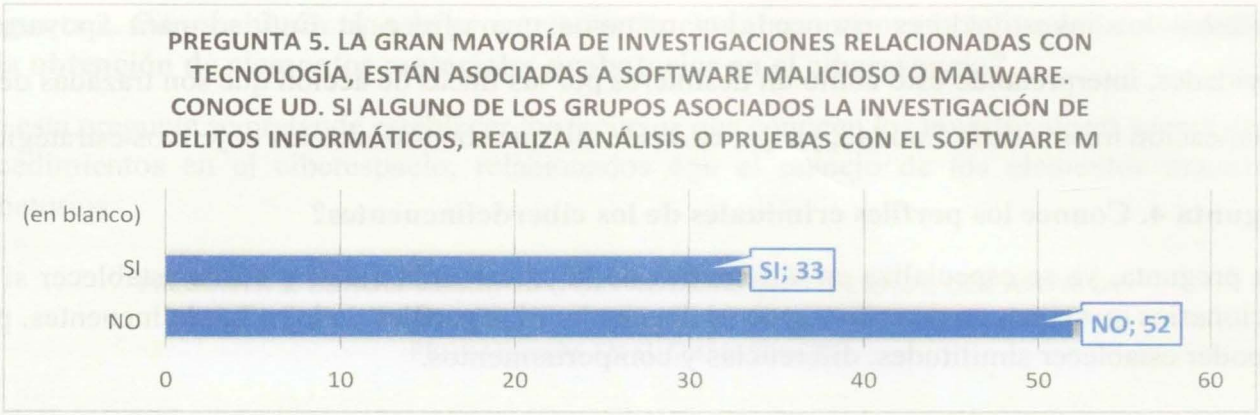
Gráfica 14. Pregunta 4 Encuesta Ciber

Fuente: Elaboración propia

La mayoría de los funcionarios contactados, dicen tener conocimiento sobre cuáles son los perfiles de los cibercriminales, observando que sólo un porcentaje mínimo carece de esta información.

Pregunta 5. La gran mayoría de investigaciones relacionadas con tecnología, están asociadas a software malicioso o malware. Conoce Ud. si alguno de los grupos asociados a la investigación de delitos informáticos, realiza análisis, disección o pruebas con el software malicioso encontrado?

Esta pregunta busca conocer quién y cómo se realizan los procedimientos investigativos relacionados con el malware encontrado en los sistemas informáticos, producto de las actividades de policía judicial ordenadas.



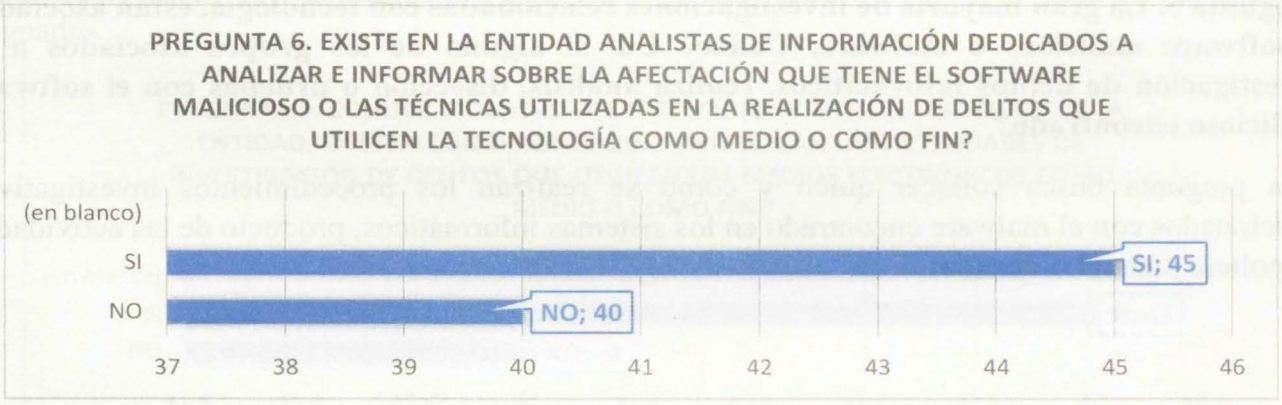
Gráfica 15. Pregunta 5 Encuesta Ciber

Fuente: Elaboración propia

Una gran parte de la población consultada, dice desconocer los procedimientos que realizan los grupos de informática forense y delitos informáticos. Esta situación es preocupante, toda vez que se debería tener claro qué y en dónde se pueden realizar las labores de apoyo en las actuaciones judiciales.

Pregunta 6. Existe en la entidad analistas de información dedicados a analizar e informar sobre la afectación que tiene el software malicioso o las técnicas utilizadas en la realización de delitos que utilicen la tecnología como medio o como fin?

Con esta pregunta se busca identificar las capacidades con que cuenta la Entidad, relacionada con el personal idóneo para realizar las actividades de análisis de los programas maliciosos encontrados en los elementos materiales probatorios, producto de la recolección de información dentro de los casos de investigación judicial.



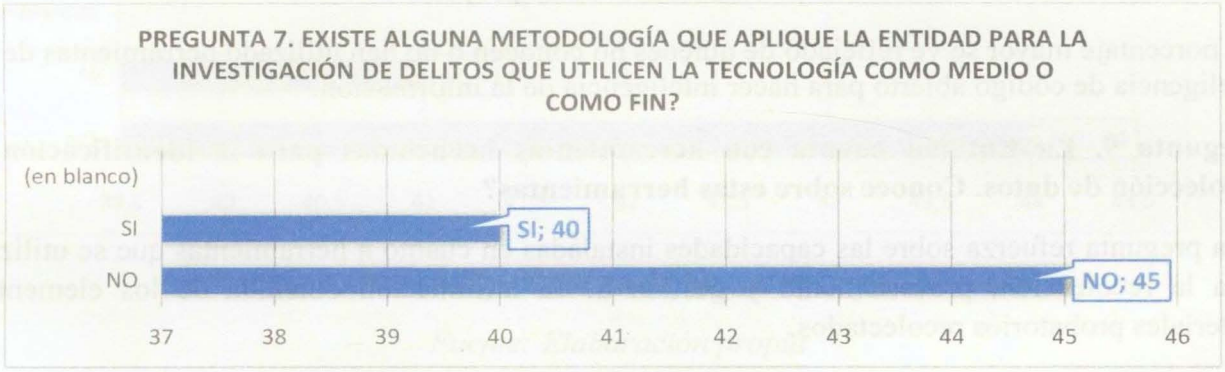
Gráfica16. Pregunta 6 Encuesta Ciber

Fuente: Elaboración propia

Una de cada dos personas entrevistadas indicaron que si conocen sobre este tipo de funcionarios especializados, los demás indicaron que no. De igual forma, existen grupos que recolectan información y hacen análisis de la misma. Lo que no es claro, es si estos grupos realizan análisis al "malware" encontrado.

Pregunta 7. Existe alguna metodología que aplique la Entidad para la investigación de delitos que utilicen la tecnología como medio o como fin?

Esta pregunta se diseñó pensando en identificar la documentación que oriente las actuaciones de los investigadores y analistas frente a los resultados requeridos en materia de ciberdelitos.



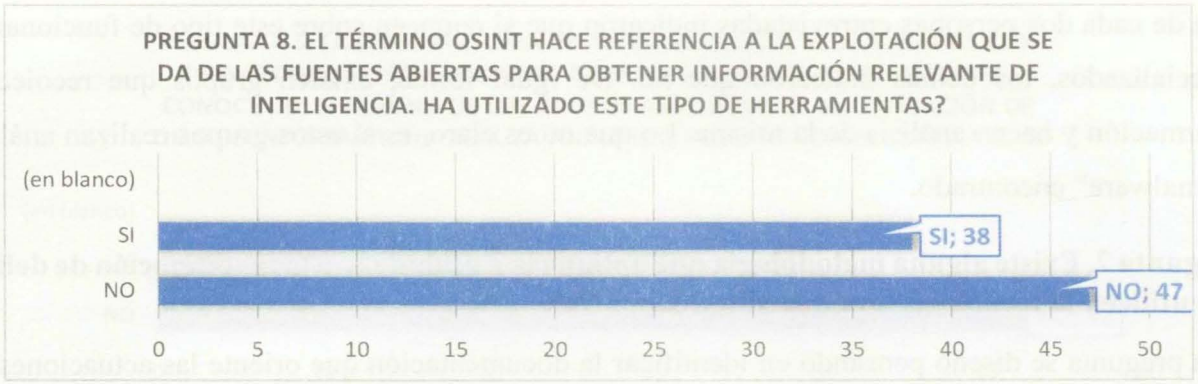
Gráfica 17. Pregunta 7 Encuesta Ciber

Fuente: Elaboración propia

No es claro para todos los investigadores, reconocer la documentación con la que cuneta la Entidad para aplicarla en los procedimientos de investigación de ciberdelitos.

Pregunta 8. El término OSINT hace referencia a la explotación que se da de las fuentes abiertas para obtener información relevante de inteligencia. Ha utilizado este tipo de herramientas?

Esta pregunta hace referencia a las herramientas que de código abierto se encuentran disponibles para obtener información relevante que ayude a orientar las investigaciones realizadas en torno a los delitos cometidos por medios electrónicos



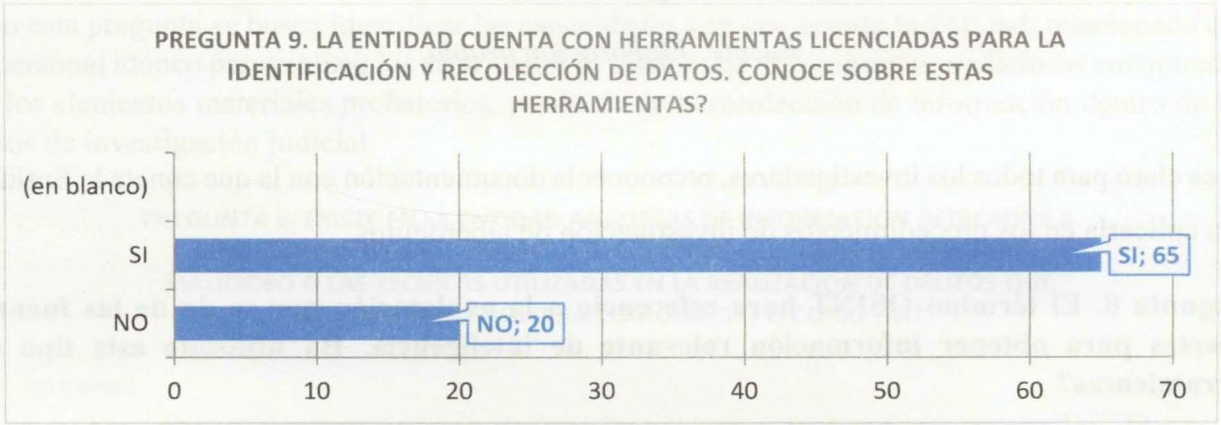
Gráfica18. Pregunta 8 Encuesta Ciber

Fuente: Elaboración propia

Un porcentaje mayor se ve reflejado de quienes no conocen o no han utilizado herramientas de inteligencia de código abierto para hacer inteligencia de la información.

Pregunta 9. La Entidad cuenta con herramientas licenciadas para la identificación y recolección de datos. Conoce sobre estas herramientas?

Esta pregunta refuerza sobre las capacidades instaladas en cuanto a herramientas que se utilizan para la recolección, procesamiento y gestión de la información obtenida de los elementos materiales probatorios recolectados.



Gráfica19. Pregunta 9 Encuesta Ciber

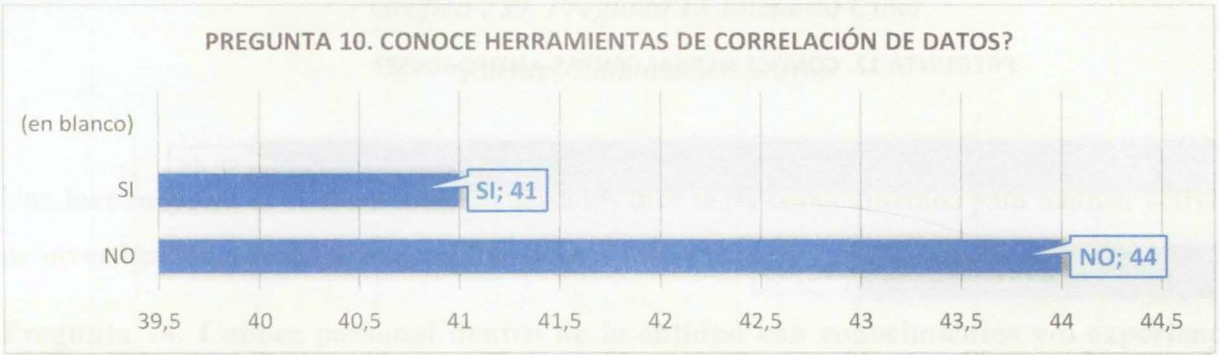
Fuente: Elaboración propia

La mayoría de los encuestados, un gran porcentaje técnico, conocen y utilizan este tipo de herramientas en las que la Entidad ha invertido en licencias y en capacitación. El porcentaje que

dice no conocer corresponde a funcionarios del área de fiscales que por sus roles dentro de las investigaciones no utilizan este tipo de herramientas.

Pregunta 10. Conoce herramientas de correlación de datos?

Esta pregunta pretende establecer que tanto conocimiento tienen los funcionarios de policía judicial sobre las herramientas de correlación de datos con las que cuenta la Fiscalía General de la Nación.



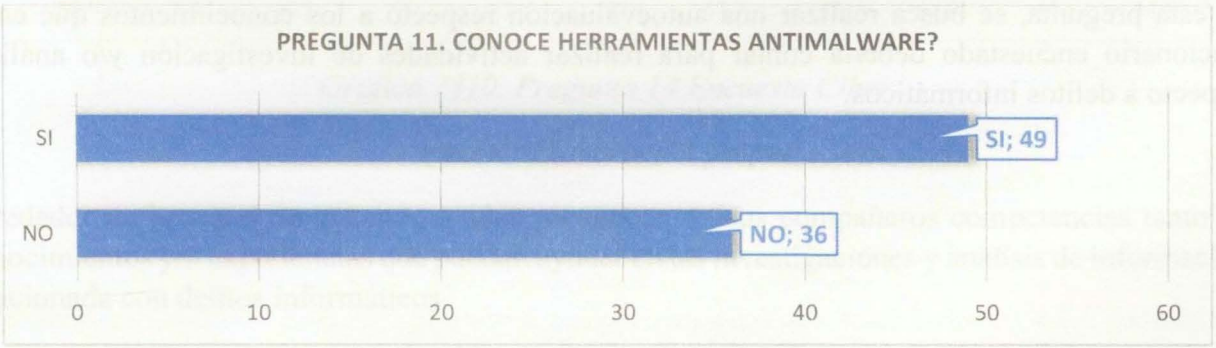
Gráfica 20. Pregunta 10 Encuesta Ciber

Fuente: Elaboración propia

Un leve porcentaje de funcionarios encuestados, manifiestan no conocer sobre herramientas de correlación de datos, aunque muchos de ellos posiblemente las utilicen.

Pregunta 11. Conoce herramientas antimalware?

La pregunta realizada proyecta el conocimiento con que deben contar los expertos en delitos informáticos e informática forense para realizar sus actividades de investigación y análisis.



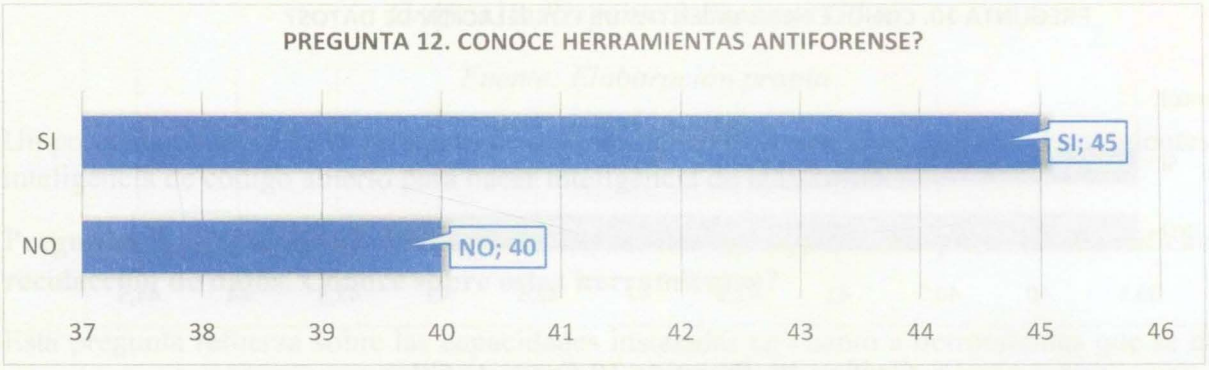
Gráfica 21. Pregunta 11 Encuesta Ciber

Fuente: Elaboración propia

La mayoría de los encuestados dicen conocer sobre herramientas que permiten analizar y procesar información que está relacionada con software malicioso.

Pregunta 12. Conoce herramientas antiforense?

Se intenta establecer el conocimiento que se tiene sobre herramientas antiforense y que puedan servir en los procedimientos que se aplican en la Entidad.



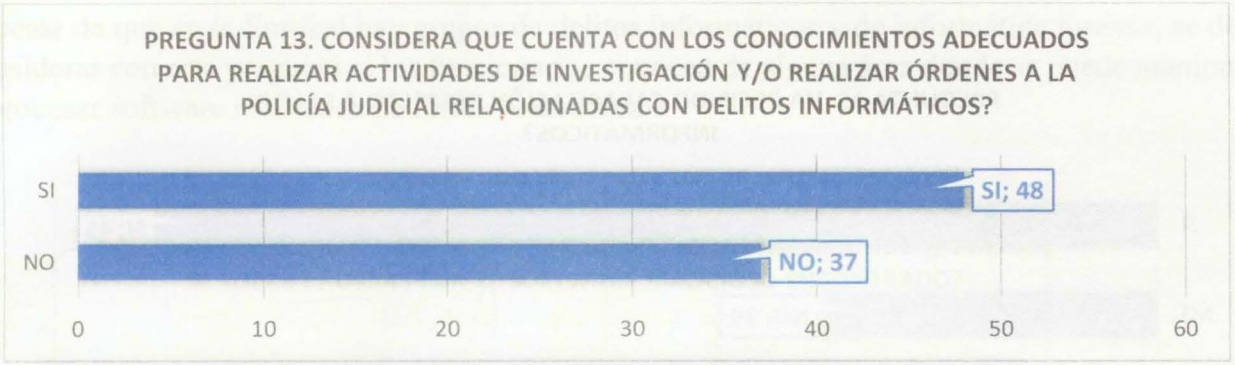
Gráfica 228. Pregunta 12 Encuesta Ciber

Fuente: Elaboración propia

Una mayoría leve de funcionarios encuestados, dicen conocer sobre herramientas antiforenses, ya sea por uso en la Entidad o por fuera de ella.

Pregunta 13. Considera que cuenta con los conocimientos adecuados para realizar actividades de investigación y/o realizar órdenes a la policía judicial relacionadas con delitos informáticos?

En esta pregunta, se busca realizar una autoevaluación respecto a los conocimientos que cada funcionario encuestado debería contar para realizar actividades de investigación y/o análisis respecto a delitos informáticos.



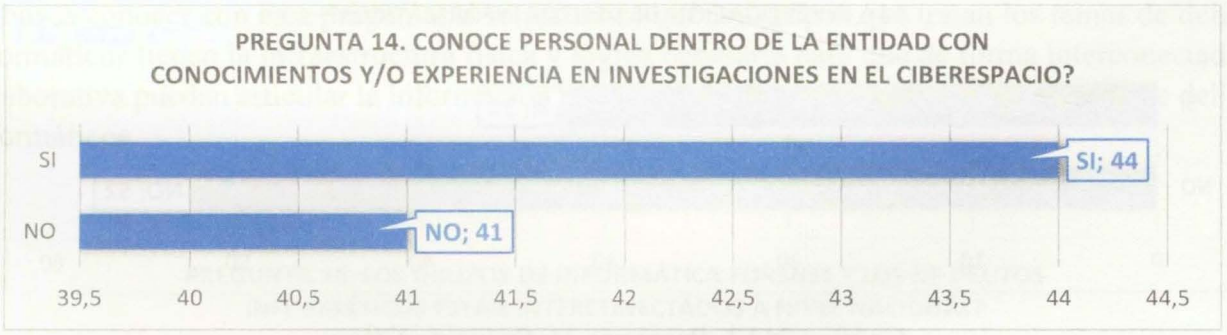
Gráfica 239. Pregunta 13 Encuesta Ciber

Fuente: Elaboración propia

Una leve mayoría de funcionarios encuestados dice tener conocimientos para realizar actividades de investigación y/o análisis respecto a delitos informáticos.

Pregunta 14. Conoce personal dentro de la entidad con conocimientos y/o experiencia en investigaciones en el ciberespacio?

La pregunta aspira conocer que tanto personal identifican los funcionarios con los conocimientos y experiencias en delitos informáticos.



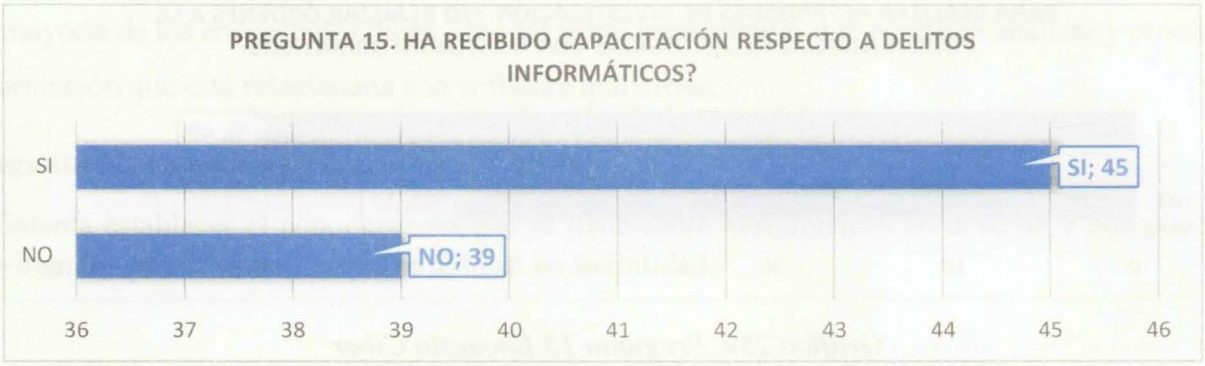
Gráfica 2410. Pregunta 14 Encuesta Ciber

Fuente: Elaboración propia

Alrededor de la mitad de los encuestados reconocen en sus compañeros competencias tanto de conocimientos y/o experiencias que puedan ayudar en las investigaciones y análisis de información relacionada con delitos informáticos.

Pregunta 15. Ha recibido capacitación respecto a delitos informáticos?

Se busca con esta pregunta, conocer el estado de las competencias relacionadas con conocimientos en delitos informáticos y el porcentaje de personas que cuentan con este aspecto.



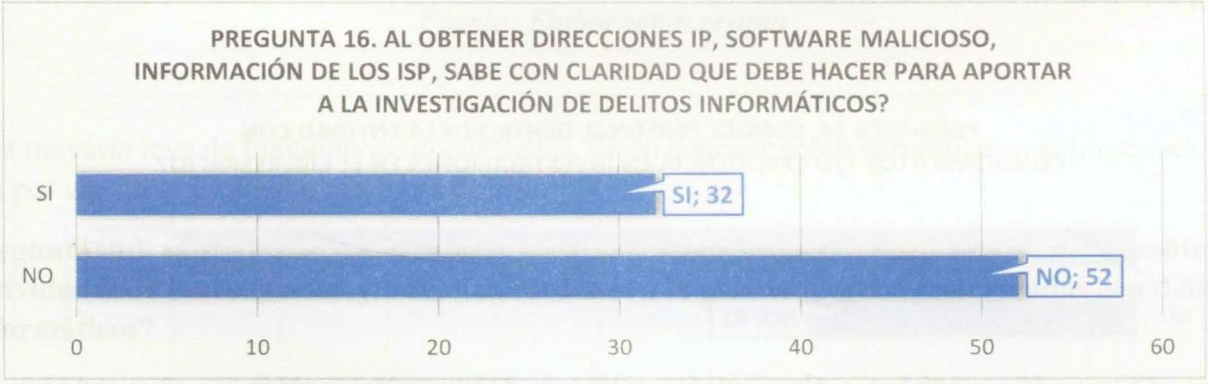
Gráfica 2511. Pregunta 15 Encuesta Ciber

Fuente: Elaboración propia

Ligeramente hay un mayor número de personas que han tenido la posibilidad de capacitarse en delitos informáticos, ya sea en la Entidad o por fuera de ella.

Pregunta 16. Al obtener direcciones IP, software malicioso, información de los ISP, sabe con claridad que debe hacer para aportar a la investigación de delitos informáticos?

En esta pregunta, se pretende establecer las líneas de acción de los investigadores y analistas con relación a la información obtenida en el proceso de investigación judicial.



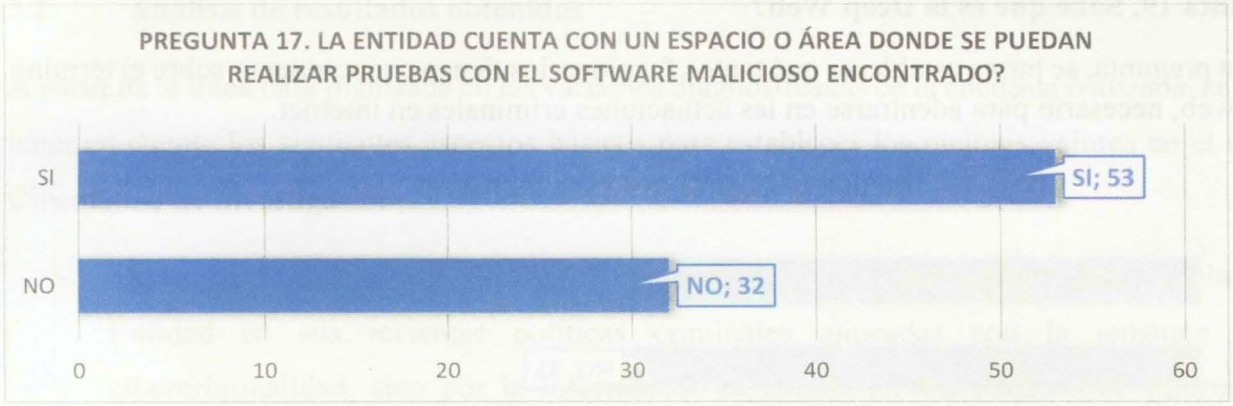
Gráfica 2612. Pregunta 16 Encuesta Ciber

Fuente: Elaboración propia

Un gran porcentaje de personas encuestadas no tiene claro que hacer con la información que pueden obtener para enriquecer las investigaciones y lograr los objetivos de identificación de información como modus operandi, personas que participan, etc.

Pregunta 17. La Entidad cuenta con un espacio o área donde se puedan realizar pruebas con el software malicioso encontrado?

A pesar de que en la Entidad hay grupos de delitos informáticos y de informática forense, se debe considerar con esta pregunta si los funcionarios conocen de alguna área donde se puede manipular y procesar software malicioso de forma controlada.



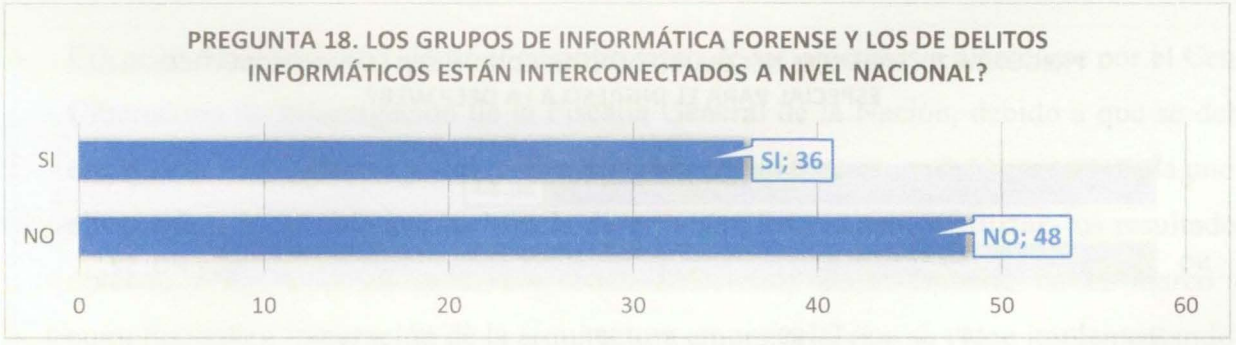
Gráfica 27. Pregunta 17 Encuesta Ciber

Fuente: Elaboración propia

La mayoría de encuestados reconocen un sitio o área donde según lo contestado, consideran que se puede manipular el software malicioso.

Pregunta 18. Los grupos de informática forense y los de delitos informáticos están interconectados a nivel nacional?

Se busca conocer con esta pregunta, si se reconoce que los grupos que tratan los temas de delitos informáticos tienen la infraestructura física y lógica necesaria para que de forma interconectada y colaborativa puedan articular la información pre y post de las investigaciones en materia de delitos informáticos.



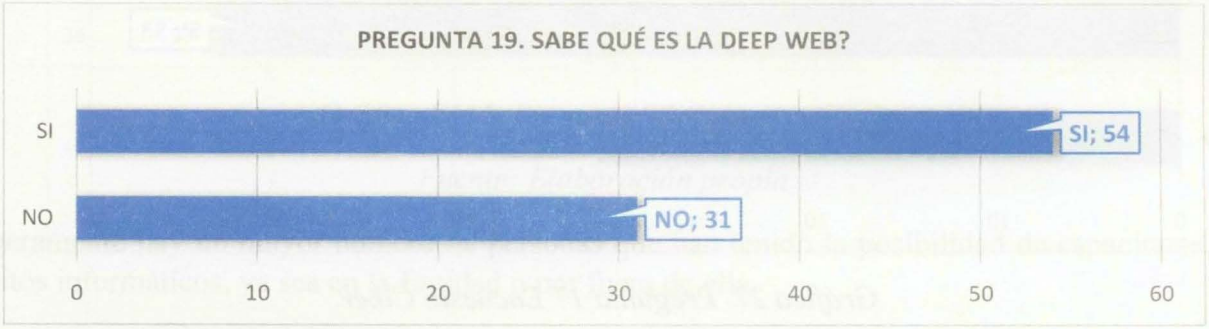
Gráfica 2813. Pregunta 18 Encuesta Ciber

Fuente: Elaboración propia

Un mayor porcentaje de funcionarios reconocen que los grupos relacionados con delitos informáticos no están interconectados entre sí, tan sólo un porcentaje menor considera que sí están unidos pero no es claro sobre los aspectos que lo confirman.

Pregunta 19. Sabe qué es la Deep Web?

En esta pregunta, se busca establecer qué tantos funcionarios tienen conocimiento sobre el término Deep web, necesario para adentrarse en las actuaciones criminales en internet.



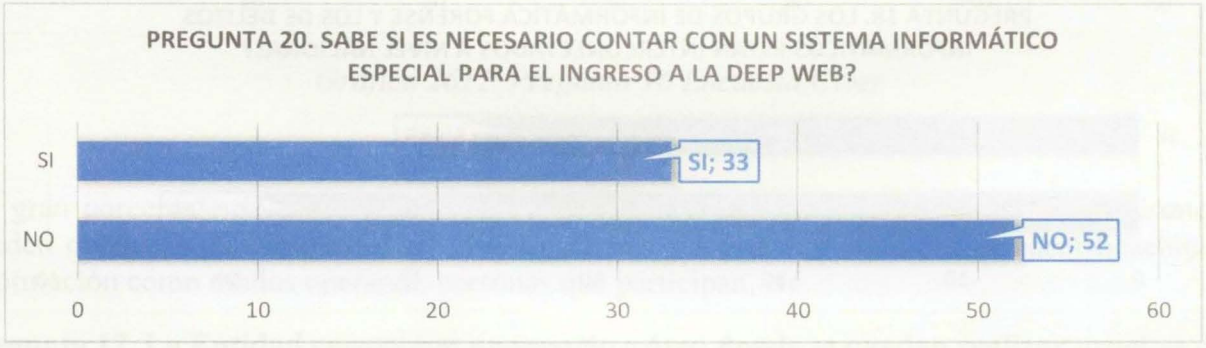
Gráfica 2914. Pregunta 19 Encuesta Ciber

Fuente: Elaboración propia

La mayoría de encuestados dicen conocer sobre la expresión Deep web, tan sólo una pequeña porción de ellos dice no conocerla.

Pregunta 20. Sabe si es necesario contar con un sistema informático especial para el ingreso a la Deep Web?

Se busca con esta pregunta, establecer si los encuestados conocen aspectos técnicos de los recursos necesarios para acceder a la Deep web.



Gráfica 3015. Pregunta 20 Encuesta Ciber

Fuente: Elaboración propia

La mayoría de encuestados asegura que no es necesario contar con sistemas especiales para el ingreso a la Deep web.

3.2. Análisis de resultados obtenidos

A partir de la línea base planteada en las variables diagnosticadas de la encuesta realizada, se deben tener en cuenta los siguientes aspectos básicos para establecer los mejores valores en el Centro Cibernético de Investigación:

- Pertinencia: Este aspecto va en concordancia con las prioridades planteadas no sólo por la Entidad en sus recientes políticas criminales alineadas con la temática de la cibercriminalidad, sino por la información registrada en los sistemas de información, respecto a los delitos que tienen que ver con la información y que se encuentran tipificados en el capítulo VII bis de la Ley 906, esta corresponde a la Ley 1273 de 2009.
  Actualmente, debido a la globalización y al acceso que se tiene de las tecnologías de la información y las comunicaciones se han generado nuevas tipologías que han sido contempladas en el código penal, en un intento contundente para frenar la desmedida utilización de los medios digitales en acciones al margen de la ley.
  Por lo anterior, es conveniente considerar que la Entidad incorpore en sus procesos técnicos investigativos y de análisis, un centro que cuente con la infraestructura tanto funcional como física y lógica para tratar los temas de delitos que tengan como medio o como fin los medios digitales.

- Eficacia: Aquí se debe valorar el cumplimiento de los objetivos a plantearse por el Centro Cibernético de Investigación de la Fiscalía General de la Nación, debido a que se deben estructurar los productos y servicios que se ofrecerán. Esto es, poder hacer por cada uno de ellos, una hoja de vida que incluya la descripción, los recursos a utilizar, los resultados a obtener y como se articulan con otras soluciones de la Entidad en el marco del cumplimiento e integración de la arquitectura empresarial que se viene implementando.

- Eficiencia: Se revisa la utilización de los recursos respecto al cumplimiento de los objetivos. Esto es, poder utilizar los recursos tanto técnicos como operativos y funcionales

en pro de obtener los mejores resultados, siempre buscando que las investigaciones y los análisis que se realicen aporten para la toma de las decisiones respecto a los procesos judiciales en materia de delitos informáticos.

- Sostenibilidad: Este aspecto debe permitir conocer las situaciones tanto económicas, contextuales, de funcionalidad y de personal que son necesarias para que el Centro Cibernético de Investigación funcione y se adecue a las condiciones cambiantes del medio y permite integrar nuevas tecnologías y funcionalidades que le den al centro un nivel bajo de obsolescencia.

Ahora bien, los resultados que se obtuvieron en cada una de las respuestas del cuestionario anteriormente aplicado en la Entidad contienen los aspectos relacionados con las capacidades del modelo DOMPI que se deben considerar para crear el Plan de Acción del Centro Cibernético de Investigación propuesto y articular con los valores sugeridos para el mismo. En tal sentido, se crean postulados basados en estas respuestas, las cuales han sido agrupadas de acuerdo con las capacidades planteadas y sobre las cuales se basa la evaluación de impacto.

Capacidad DOCTRINA

Esta capacidad debe permitir recolectar, mantener, ajustar y difundir todo el conjunto de concepciones que alrededor del tema de investigación criminal y en especial, el de cibercriminalidad, debe tener la Fiscalía General de la Nación, con el ánimo de contar con un soporte documental que sea la línea base del actuar de la Entidad. En este sentido, se revisó el conocimiento de algunos de los actores del proceso judicial que deberían tener el conocimiento adecuado para el correcto tratamiento de las investigaciones en el ciberespacio, siendo visiblemente notorio la utilización de herramientas que provee la misma Entidad como el Manuel de Procedimientos. Es así, como cobra fuerza la utilización de recursos del Sistema Penal actual, como es la recolección de elementos materiales probatorias y evidencia física y su cuidado mediante la utilización de la Cadena de custodia.

Esta capacidad debe estar orientada a dos frentes principales:

Prevención: Recursos destinados a disminuir la ocurrencia de eventos relacionados no sólo con delitos informáticos sino con aquellos delitos que pueden utilizar la tecnología como medio para cometer otro tipo de delitos.

Investigación criminal: Conjunto de tareas dispuestas a permitir de forma adecuada la recolección de elementos materiales probatorios y evidencia física, logrando actividades óptimas de investigación y análisis criminal.

Capacidad ORGANIZACIÓN

Esta capacidad permite entender la estructura tanto orgánica del Centro propuesto como de las estructuras que se deben investigar, no sólo como componentes de organizaciones criminales sino como apéndices del actuar de otro tipo de delitos diferentes a los informáticos. Es así, como se debe conocer todo el universo de características con que cuentan los ciberdelincuentes, para poder perfilar, investigar y analizar su comportamiento tanto en el ciberespacio como en el mundo físico.

En este sentido, es apropiado que se revisen, ajusten y adopten los protocolos necesarios para desarrollar las actividades de policía judicial relacionadas con investigación y análisis en el ámbito de las actuaciones judiciales en el ciberespacio.

Así mismo, es conveniente establecer la cadena de mando y control que permita articular la documentación existente y la proyectada para interactuar con los procedimientos al interior del Centro Cibernético y para ello, es importante establecer la estructura organizacional y funcional del mismo para conocer por parte de cada uno de quienes integren el Centro, así como de los usuarios que hagan uso de este, el alcance y objetivos y su participación en los procesos judiciales relacionados con el uso inapropiado de tecnologías.

Capacidad MATERIAL Y EQUIPO

Esta capacidad debe proveer los lineamientos relacionados con recursos físicos necesarios para la operación del Centro, en especial las herramientas tanto de código abierto como comerciales que permitan dotar de elementos tecnológicos al Centro Cibernético de Investigación y que sean el soporte técnico en las investigaciones judiciales. Así mismo, se debe contar con los equipos de

tecnología que por su robustez y funcionalidad permitan de manera ágil brindar resultados en la información solicitada, ya sea a nivel investigativo o de análisis criminal.

Esta capacidad debe proyectar la adquisición, sostenimiento y articulación de herramientas tecnológicas propias de investigación y análisis criminal y así, establecer el presupuesto requerido para los planes de financiamiento tato interno como de ayudas de agencias internacionales.

Capacidad PERSONAL

Esta capacidad debe permitir el reclutamiento al interior de la Entidad, de aquellos funcionarios que cuentan no sólo con la formación sino con la experiencia y los deseos de aprender más sobre el desarrollo de las investigaciones en el marco de los delitos informáticos y de aquellos que se valen de los medios informáticos para cometer otro tipo de delitos.

Aquí es donde se deben articular los procedimientos definidos por la Entidad con aquellos que, con la participación de los funcionarios reclutados, se construyan para fortalecer las actividades de policía judicial en el espacio.

Todo el personal identificado, debe estar incorporado en un plan de capacitación permanente que se desarrolle desde el Centro Cibernético de Investigación, en concurso con la Dirección de altos Estudios, encargados de los procesos de capacitación para los servidores de la Entidad.

Capacidad INFRAESTRUCTURA

Esta capacidad debe permitir que la Entidad cuente con los espacios físicos adecuados para la ubicación del personal experto que investigue y analice la información que se allegue. Estos espacios deben contar con los elementos básicos de conexión y comunicación para permitir la interacción entre estos servidores.

Estos elementos de conexión y comunicación deben estar enfocados no sólo en obtener información de los sistemas misionales de la Entidad, sino que deben permitir la navegación en sitios que actualmente son de difícil acceso, como lo es la Deep Web.

De igual forma, es importante que estén articulados los grupos que actualmente desarrollan actividades de investigación de delitos informáticos, como son "Delitos Informáticos" e "Informática forense".

3.3. Consideraciones para la creación del Centro Cibernético de Investigación

Si bien es cierto que se requiere de un ente que permita centralizar las actividades de investigación en el ciberespacio, en especial las que tienen que ver con la comisión de delitos informáticos, sin desconocer otro tipo de conductas delictivas, es importante también establecer algunos criterios que permitan que el centro propuesto sea exitoso desde la óptica de los componentes DOMPI.

Es por ello, que es importante conocer las directrices que surgen con ocasión de la creación de los Centros de Respuesta a Incidentes en Seguridad Informática, conocidos globalmente como CSIRT.

A continuación, se describe de forma general los aspectos a destacar para ser incorporados en el Centro Cibernético de Investigación de la Fiscalía General de la Nación, siempre bajo el marco de los componentes DOMPI mencionados, así:

DOCUMENTACIÓN:

Para la constitución del Centro Cibernético de Investigación, se hace necesario que se elabore un documento de constitución donde se indique de forma clara y específica aspectos como:

- Misión (Qué actividades realizará el Centro)
- Visión (Cuál es la proyección del Centro en la Fiscalía y en el sector justicia)
- Objetivos (Cuáles serán sus parámetros de acción)
- Alcance (Hasta dónde tiene su aplicación el Centro, identificando los servicios que prestará)
- Partes interesadas (Quienes participarán activa y pasivamente en la misionalidad del Centro)
- Beneficiarios (Cuál será la población objetivo de los resultados del Centro)
- Políticas de transversalidad respecto a las investigaciones ya sea de delitos informáticos o la utilización de medios tecnológicos con ocasión de otro tipo de delitos

Lo anterior correspondería al marco institucional que permita que el Centro tenga las políticas adecuadas de funcionamiento y pueda tener claro su accionar frente a las investigaciones que se puedan dar en el ciberespacio. Así mismo, se debe elaborar un cronograma que permita establecer el tiempo suficiente para la puesta en funcionamiento del Centro Propuesto y realizar el

seguimiento adecuado a su implementación. Las actividades por considerar en este cronograma son:

- Aprobación de las directivas de la Entidad
- Conseguir instalaciones físicas adecuadas
- Ubicación de los funcionarios que estarán en el Centro Cibernético de Investigación
- Elaborar plan de capacitación y entrenamiento
- Adquisición de infraestructura de hardware y software
- Inicio de operaciones
- Divulgación de las actividades del Centro
- Revisión de procesos y procedimientos del Centro (OEA, 2016)

RECURSO HUMANO:

Para establecer el mejor accionar del Centro Cibernético de Investigación, se hace necesario contar con el recurso humano adecuado tanto en conocimiento como en habilidades tecnológicas. Por ello, se deben definir funciones y responsabilidades del personal que formará parte de este Centro sin desconocer la importancia de elaborar un organigrama que muestre la estructura al interior del mismo.

Dentro de los roles sugeridos para el Centro están:

- Coordinador
- Asistente
- Analistas / investigadores
- Administrador de red (personal técnico)
- Gestor de incidentes

Dentro de los conocimientos que este personal debería tener, están los siguientes aspectos:

- Seguridad informática y respuesta a incidentes
- Seguridad de la información
- Políticas públicas en tecnología y telecomunicaciones
- Seguridad y defensa nacional
- Ley pública

- Marco legal
- Actuaciones de policía judicial

Aunque este es el personal propuesto, se debe tener presente que varios de estos roles pueden cumplir una o más funciones, siempre encaminadas a trabajar en equipo y dar soluciones ágiles y efectivas frente a las investigaciones de tipo penal que se puedan presentar. Por tanto, se debe elaborar una política y práctica de la separación de funciones. (OEA, 2016)

INFRAESTRUCTURA

El Centro Cibernético de Investigación de la Fiscalía General de la Nación debe contar con unos servicios básicos de operación que permitan el desarrollo óptimo de las actividades a ejecutar por parte de los funcionarios que estén adscritos al mismo.

Por tanto, se hace necesario incluir temas de infraestructura de tecnologías, arquitectura de red y diagramas de configuración del centro, así, se pueden identificar elementos necesarios como:

- Equipamiento de espacio físico, como aires acondicionados, sistema de detección de incendios, sistemas redundantes
- Controles de acceso al centro
- Circuito cerrado de televisión
- Sistema de comunicaciones de red, como servidores, computadores, switches
- Sistemas de almacenamiento

Capítulo 4. Evaluación del impacto

Este capítulo describe de manera general por cada una de las capacidades que se han venido proponiendo, la proyección que se tiene del Centro Cibernético de Investigación y su pertinencia para la Fiscalía General de la Nación y cómo este modelo es el seleccionado como base para la operación del Centro en mención:

La planeación por capacidades se empezó a desarrollar en Colombia a partir del año 2004 y hasta el 2006, cuando una comisión de Estados Unidos inició sus actividades sin llegar a profundizarla y mucho menos implementarla, pero no es hasta el año 2011 cuando a través del Comité de Revisión Estratégica e Innovación – CREI activado por la Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional se hicieron planteamientos estratégicos frente al objetivo presidencial de terminar el conflicto armado en Colombia.

En este sentido, en el año 2012 el "Comité Estratégico de Transformación e Innovación" (CETI) plantea la teoría de la planeación por capacidades y se crea un modelo conocido como DOMPI, (Doctrina, organización, material, personal e infraestructura). (Acore, 2016)

Lo interesante del modelo es que permite fortalecer las capacidades del sector al cual es aplicado, es decir, si es a nivel de tecnologías de la información y las comunicaciones, su robustez permite un mayor alcance a nivel de comunicaciones y seguridad de la información. En el caso de las fuerzas militares, no sólo se fortaleció el plan de acción para el cumplimiento de los objetivos del país sino que institucionalmente se crearon estrategias que impulsaron a las fuerzas militares a tener una mejor estructura en su funcionalidad, a la cual llamaron "Fuerza Multimisión" (Acore, 2017)

La Fiscalía General de la Nación, no puede ser ajena a estos cambios productivos que fortalecen las instituciones del Estado y es por ello, que el modelo propuesto cubre las variables que permiten un actuar más preciso y efectivo. En tal sentido, se describe por cada capacidad el estado sugerido de la Institución desde la creación del Centro Cibernético de Investigación:

Capacidad DOCTRINA

Con la incorporación de una estructura documental que permita el registro de información relacionada con investigaciones y análisis criminales, además de permitir ser fuente de consulta, así como repositorio de buenas prácticas y acopio de lecciones aprendidas, se logra dar cobertura de la información relacionada con ciberdelitos, siendo el primer proceso formal en el ámbito misional de la Gestión de Conocimiento que se incorpore en la Fiscalía General de la Nación.

Al crear procedimientos y protocolos, se garantiza que las actividades que se realicen al interior del centro cumplan con la rigurosidad que demanda las investigaciones y los análisis criminales en el ámbito del ciberespacio, tema que hoy en día, la Entidad no cubre como debería ser por falta precisamente de las capacidades que se están exponiendo.

Este proceso se incorpora al Sistema de documentación de la entidad, conocido como BIT, donde está toda la estructura documental al servicio de todos y cada uno de los servidores a nivel nacional y de uso en cada una de las 35 seccionales a nivel nacional.

Dentro de los procedimientos y protocolos sugeridos a incorporar en el Centro, están:

- Recolección de datos en el ciberespacio
- Recolección, organización y construcción de grafos con información obtenida por medio de fuentes abiertas
- Generación de perfiles alternos como medio para el uso de la figura de Agente virtual encubierto

Capacidad ORGANIZACIÓN

Al impulsar la capacidad de Organización, se logra que el Centro Cibernético de Investigación, tenga una estructura funcional, enmarcado en una jerarquía que permite facilitar las actividades de mando y control ejerciendo la autoridad y dirección por parte de quienes lideren los procesos en el Centro. Esta estructura debe estar en consonancia con la arquitectura institucional que se viene implementando en la Entidad, logrando acoplarse a los mecanismos organizacionales de la Fiscalía evitando retrasos en su operación.

Al contar con esta capacidad, la incorporación de personal, procedimientos y recursos técnicos, físicos y lógicos al Centro se hace de forma transparente porque cada servidor incorporado tendría definidas sus funciones, tendría claro el uso de los recursos asignados y la interacción con el personal del Centro sería más natural.

El organigrama sugerido para el Centro se muestra en la Gráfica 31. Estructura funcional del Centro Cibernético de Investigación.

Gráfica 16. Estructura funcional del Centro Cibernético de Investigación

Fuente: Elaboración propia

Es a partir de la Resolución número 01165 de 2018, por medio de la cual se define el esquema de gobierno de la Arquitectura Institucional de la Fiscalía General de la Nación y se dictan otras disposiciones, que el Centro Cibernético de Investigación se vincula a este gobierno propuesto y se adhiere de forma tal que permite incorporar nuevos procesos y recursos a la Entidad, proyectándola como una institución moderna y de un enfoque transversal en los procesos misionales en su interior.

Con este Centro, se está fortaleciendo a nivel tecnológico la Entidad, llevándola a ser más eficiente en los resultados que le puede presentar a la ciudadanía en general, con el fin no sólo de esclarecer las investigaciones sino lograr esos resultados en mejores tiempos, afianzando así, la visión institucional actual.

Es un proyecto que vincula a todas las áreas de la Entidad, ya sea de investigación, análisis o forense, además de permitir a fiscales, asistentes y a los mismos jueces, participar de las

investigaciones y análisis criminales de los procesos judiciales que se adelanten en el ciberespacio, mejorando su entendimiento, percepción y toma de decisiones.

Capacidad MATERIAL Y EQUIPO

Con esta capacidad el Centro estaría liderando los equipos de tecnología al servicio de la Investigación, ya que se requiere de equipos de última tecnología con gran capacidad de almacenamiento, procesamiento de video, uso de memoria RAM, garantizando un nivel de obsolescencia bajo durante su vida de uso en el Centro. Así mismo, se contaría con el software tanto de uso libre como de uso comercial que permita obtener la información requerida en las investigaciones y análisis criminal en el ámbito del ciberespacio.

Entre algunos de los elementos que pueden fortalecer esta capacidad están:

Recurso tecnológico

- Hardware

  Componentes físicos requeridos como:

  - Estaciones de trabajo portátiles
  - Impresoras
  - Escaner
  - Ploter

- Software

  Herramientas necesarias para obtener, procesar, difundir la información dentro de investigaciones a realizar en el ciberespacio, a saber:

  - ANONIMACIÓN (Permite navegar por la Deep web, sin poder ser detectada la dirección ip de quien está realizando la navegación)
    - Navegador TOR, el más conocido y utilizado de los navegadores

  - IDENTIDAD (Permite hacer seguimiento de las actuaciones de las personas y su círculo social, respecto a publicaciones de elementos multimediales, que sirven como indicios dentro de una investigación)
    - Facebook, red social para publicar elementos multimediales
    - Twiter, red social de opinión
    - Instagram, red social con enfoque en imágenes (fotografías)

  - BUSCADORES (Permite ubicar elementos específicos dentro de la red internet)
    - Shodan, especial para ubicar dispositivos conectados en internet

- OTROS
  - Maltego

- Comunicaciones

Los elementos y protocolos necesarios para garantizar la comunicación entre el Centro y la red institucional, así como los elementos para crear una red que permita el acceso anonimizado a la Deep Web, sin llegar a afectar las conexiones al interior de la entidad.

Actualmente, la FGN tiene todas las seccionales interconectadas, el proveedor de servicio de comunicaciones es Telefónica.

La proyección de la solución debe estar dada para garantizar el almacenamiento de los datos, teniendo en cuenta que la FGN cuenta con la infraestructura para hacerlo.

Es necesario, ampliar la capacidad de acuerdo a esta proyección, a partir de infraestructura de desarrollo (PCs, Redes, Internet, etc.) y fortalecer los sistemas de almacenamiento y seguridad de datos

Recurso operativo

Se garantiza capacitación, en el manejo del hardware y software, para ir profesionalizando a quienes vayan a estar manejando el Centro, así como entrenamiento en estos recursos y formación respecto al uso y apropiación de los mismos.

Se debe contar con el acompañamiento necesario para la construcción de bibliotecas, catalogación de elementos y automatización de procedimientos.

Capacidad PERSONAL

Con esta capacidad se asegura la administración de los recursos humanos asignados al Centro, estableciendo perfiles profesionales para el ingreso y garantizando la idoneidad de quienes estén a cargo de este. Para ello se requiere contar con el siguiente equipo de trabajo para su puesta en funcionamiento y sostenibilidad operativa:

- Coordinador del Centro
- Programadores de sistemas
- Técnicos de sistemas
- Ingenieros de sistemas
- Investigadores criminales
- Analistas criminales

Más allá de la conformación de la planta con la que contará el Centro, es importante establecer la población objeto al interior de la Entidad que se verá beneficiada con este, así como se muestra en la Tabla 16:

Tabla 16. Población objeto interna beneficiaria

Actor	Ubicación	Interés-expectativa	Posición o rol	Influencia
Investigador	CTI, Direcciones adscritas a las delegadas	Existe interés en mejorar los resultados de investigación	Beneficiario	Alta
Analista	SAC, CEAC, CEVAP, Direcciones adscritas a las delegadas	Existe interés en mejorar los resultados de análisis	Beneficiario	Alta
Perito	Criminalística	Existe interés en mejorar los resultados forenses	Beneficiario	Alta
Asistente de fiscal	Despachos a nivel nacional	Existe expectativa sobre la incorporación de estos productos a sus procesos	Beneficiario	Alta
Fiscal	Despachos a nivel nacional	Existe expectativa sobre la incorporación de estos productos a sus procesos	Beneficiario	Alta
Coordinadores de capacitación	Dirección de Altos Estudios	Existe expectativa sobre cómo utilizar estos recursos en los programas de capacitación	Beneficiario	Baja
Comunicadores	Dirección de Comunicaciones	Existe expectativa sobre la utilización de este nuevo medio de comunicación	Beneficiario	Baja

Nota: Elaboración propia

De la misma forma, la población objeto externa se beneficiaría con el Centro y sus resultados, siendo estos relacionados en la Tabla 17:

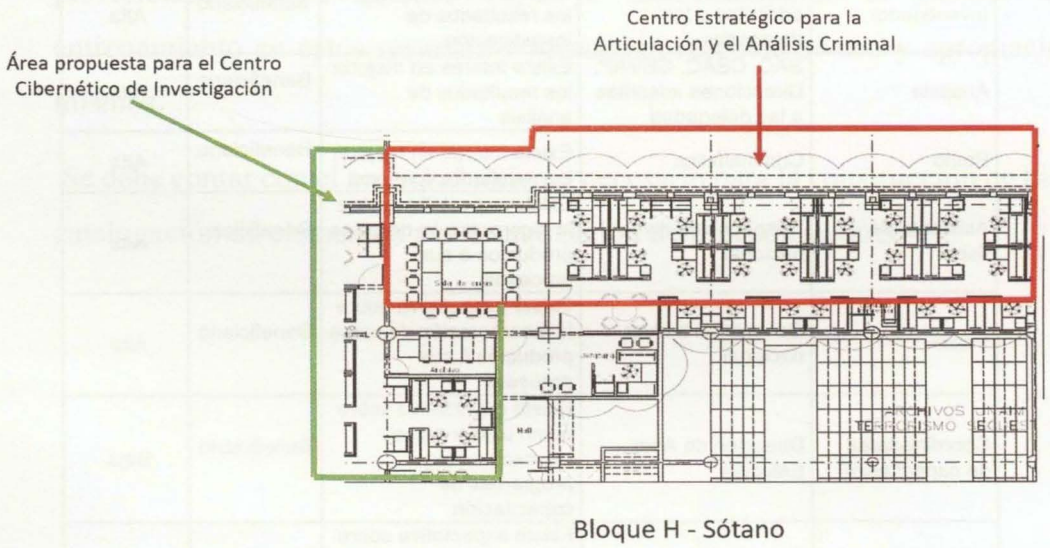
Tabla 17. Población objeto externa beneficiaria

Actor	Interés-expectativa	Posición o rol	Influencia
Juez	Existe expectativa en la aplicación de esta tecnología	Beneficiario	Media
Policía Nacional	Existe interés en mejorar los resultados de investigación y análisis	Beneficiario	Alta
Medicina Legal	Existe interés en mejorar los resultados forenses	Beneficiario	Media

Nota: Elaboración propia

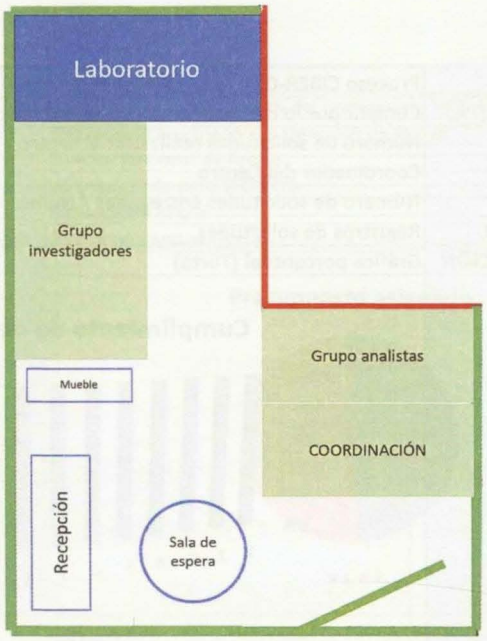
Capacidad INFRAESTRUCTURA

Esta capacidad ofrece la posibilidad de contar con espacios físicos adecuados para el uso de las herramientas adquiridas, además de la distribución del personal y la atención adecuada a quienes requieran de los servicios del Centro. Para esta capacidad, se plantea el esquema de distribución en su vista general como se aprecia en la Gráfica 32 y en vista detallada como se puede ver en la Gráfica 33:



Gráfica 3217. Distribución física del Centro Cibernético de Investigación (General)

Fuente: Elaboración propia



Gráfica 33. Distribución física del Centro Cibernético de Investigación (Detalle)

Fuente: Elaboración propia

Ahora bien, la evaluación del impacto debe contener por lo menos los siguientes indicadores que permitan sugerir la continuación o no del Centro Cibernético de Investigación en la Fiscalía General de la Nación, estos indicadores son:

- Pertinencia

FICHA DE INDICADOR	Proceso CIBER-01
RESULTADO PLANIFICADO	Disminuir en por lo menos 5% los problemas identificados con las investigaciones en el ciberespacio
INDICADOR	Porcentaje de disminución de problemas identificados
RESPONSABLE	Coordinador del Centro
FORMA DE CÁLCULO	Porcentaje de problemas identificados con relación a las investigaciones en el ciberespacio
FUENTES DE INFORMACIÓN	Plan de mejoramiento del Centro
SEGUIMIENTO Y PRESENTACIÓN	Gráfica manual de avance mensual
GRÁFICO	

Gráfica 34. Indicador de pertinencia

Fuente: Elaboración propia

- Eficacia

FICHA DE INDICADOR	Proceso CIBER-02
RESULTADO PLANIFICADO	Cumplir por lo menos con el 95% de las solicitudes realizadas al Centro
INDICADOR	Número de solicitudes realizadas al centro
RESPONSABLE	Coordinador del Centro
FORMA DE CÁLCULO	Número de solicitudes entregadas / Número de solicitudes resueltas
FUENTES DE INFORMACIÓN	Registros de solicitudes
SEGUIMIENTO Y PRESENTACIÓN	Gráfica porcentual (Torta)
GRÁFICO	

Gráfica 35. Indicador de eficacia

Fuente: Elaboración propia

- Eficiencia

FICHA DE INDICADOR	Proceso CIBER-03
RESULTADO PLANIFICADO	Establecer tiempos de servicio por debajo de lo ofrecido
INDICADOR	Tiempo límite de entrega de resultados
RESPONSABLE	Coordinador del Centro
FORMA DE CÁLCULO	Tiempo dentro del límite ofrecido
FUENTES DE INFORMACIÓN	Registro de hora de la solicitud
SEGUIMIENTO Y PRESENTACIÓN	Gráfica porcentual de registro de tiempos de servicio
GRÁFICO	

Gráfica 36. Indicador de eficiencia

Fuente: Elaboración propia

- Sostenibilidad

FICHA DE INDICADOR	Proceso CIBER-04
RESULTADO PLANIFICADO	Utilizar por lo menos el 30% del presupuesto asignado para fortalecer el Centro
INDICADOR	Presupuesto asiganado a la Dirección de Apoyo
RESPONSABLE	Director Nacional de Apoyo
FORMA DE CÁLCULO	Valor asignado para el Centro
FUENTES DE INFORMACIÓN	Presupuesto oficial
SEGUIMIENTO Y PRESENTACIÓN	Gráfica porcentual (Torta)
GRÁFICO	

Gráfica 37. Indicador de sostenibilidad

Fuente: Elaboración propia

Ahora bien, para poder que los anteriores aspectos se puedan fortalecer para el funcionamiento óptimo del Centro planteado, es necesario destacar los lineamientos para el Centro dentro de su funcionalidad y operatividad, así:

- Se debe realizar una campaña sobre dar a conocer mejor el sistema de gestión integral de la Entidad, programa que puede ser tratado con la Dirección de Comunicaciones y/o la Dirección de Altos Estudios de la Entidad.
- Se debe profundizar en la estrategia de que todos los investigadores tengan el mismo estándar en cuanto a saber qué hacer en el momento de hacer intervención en una investigación o actuación especial.
- Se debe integrar a los programas de capacitación, un espacio de sensibilización sobre los aspectos institucionales que permitan a los funcionarios, en especial los de policía judicial, entender la importancia de conocer las políticas institucionales.
- Establecer equipos de trabajo para elaborar fichas técnicas que permitan identificar las características de cada uno de los perfiles identificados, para así, hacer partícipes de quienes carecen de este conocimiento y se les facilite su aprendizaje.

- Actualizar los procedimientos de cada una de las áreas informáticas, donde se indiquen los pasos a seguir en los casos de análisis y acciones reactivas frente al malware encontrado.
- Se debe potenciar las capacidades de los funcionarios de los grupos de informática forense y similar, para que tengan la posibilidad de hacer análisis del software malicioso encontrado. Además, se pueden realizar convenios interinstitucionales, por ejemplo, con la Policía Nacional para compartir conocimientos y experiencias.
- Se debe socializar la documentación que exista relacionada con ciberdelitos y de no existir, se deben crear mesas de trabajo para elaborar esta documentación.
- Implementar herramientas de monitoreo de fuentes abiertas en un grupo centralizado que sirva de proveedor de información tanto a investigadores como analistas y que los ayude a alinear sus investigaciones o a orientar sus análisis y que estos resultados optimicen las acciones que ordenan los fiscales en las investigaciones judiciales.
- Vincular a fiscales y a asistentes de fiscal, a las posibilidades que ofrecen este tipo de herramientas, para que ellos, quienes son los que ordenan las actuaciones a la policía judicial, conozcan qué y cómo se deben hacer estas órdenes sin tener que exagerar en sus peticiones o quedarse limitados en las mismas.
- Vincular en las investigaciones e informes de análisis de los funcionarios de policía judicial, las herramientas de correlación de datos con que cuenta la Entidad ya sean de uso ofimático o de uso avanzado relacionado con minería de datos, analítica e inteligencia de negocios.
- Adquirir herramientas antimalware, que no solamente permita la detección de software malicioso sino que permita analizar y elaborar informes de su funcionalidad y elaboración.
- Adquirir herramientas anti forenses que permitan apoyar las labores de investigación y análisis de los funcionarios de policía judicial y potencien las decisiones a tomar por parte de los fiscales y su equipo de apoyo.
- Se deben nivelar las competencias que tienen investigadores y analistas respecto a delitos informáticos, realizando barras académicas que permitan intercambiar conceptos y experiencias.
- Crear comités y mesas de trabajo que permitan vincular a los funcionarios con los conocimientos suficientes sobre delitos informáticos. Además, publicar en los medios de

comunicación institucionales este tipo de eventos para ir creando reconocimiento en la comunidad judicial.

- Se debe elaborar un diagnóstico que permita establecer el número de personas que han tenido la posibilidad de recibir capacitación en temas relacionados con delitos informáticos y vincularlos a programas especializados, mientras se vincula a aquellos que no se han capacitado, en programas básicos en la misma temática.
- Elaborar una cartilla básica que oriente a los investigadores y analistas sobre qué hacer con cada uno de los elementos aportados en las investigaciones y que sirvan en las decisiones que pueden tomar los fiscales.
- Se debe proponer un área donde de forma controlada se pueda manipular el software malicioso detectado en las diferentes actuaciones de inspección por parte de la policía judicial. Esta área puede ser dentro del espacio físico de alguna de las áreas de delitos informáticos o informática forense, pero lo ideal sería que existiera de forma independiente.
- Establecer un plan de acción con la Subdirección de Tecnologías de la Información y las Comunicaciones, para que todos los grupos de delitos informáticos cuenten con canales seguros a través de los cuales puedan intercambiar información de las investigaciones y puedan hacer pruebas y compartir resultados de los elementos obtenidos en las actuaciones judiciales.
- Crear una red informática independiente dentro de la Entidad, para que se puedan tener acceso a la Deep web y así, poder navegar en este medio y obtener mejores resultados al momento de establecer contextos de las situaciones a investigar.
- Establecer protocolos de acceso a la Deep web, dando a conocer las vulnerabilidades, amenazas y riesgos que se dan al ingresar a la Deep web.

Conclusiones

- Todas las anteriores situaciones enunciadas, son susceptibles de ser investigadas en el ciberespacio y en mundo real, en donde están los victimarios. Ahora bien, es necesario poder navegar no sólo en la web superficial utilizando los sitios más comunes, desde buscadores hasta páginas especializadas, sino llegar a lo más sensible que esconde la web profunda, porque es allí donde se mantiene información que sería importante vincular a las investigaciones judiciales.

- A partir de las necesidades que requiere la Fiscalía General de la Nación, en cuanto a las investigaciones judiciales relacionadas con el uso de la tecnología como medio o como fin y a partir de la propuesta del Centro Cibernético de Investigación para la Entidad a través de este trabajo de grado, se han venido incorporando elementos definidos en las capacidades planteadas en las diferentes mesas de trabajo que se han realizado en torno al tema de investigaciones relacionadas con la ciberdelincuencia. Es así, como se ha revisado, entre otros el espacio físico adecuado para el funcionamiento del Centro y las fuentes de financiación para su implementación. Además, la Entidad ya adquirió un software que permite el monitoreo de fuentes abiertas, elemento considerado esencial para el investigador como obtención de datos que permitan su correlación.

- El Centro Cibernético de Investigación propuesto, debe ser un referente en la región respecto a la investigación y análisis de los delitos informáticos, en especial por las condiciones tecnológicas y procedimentales que se incorporen.

- A partir del diagnóstico establecido a través de las encuestas realizadas, se deben ir construyendo las condiciones ideales a nivel de área física, profesionales especializados, procedimientos y protocolos estandarizados para la creación del Centro Cibernético de Investigación de la Fiscalía General de la Nación.

- Es necesaria la definición de procesos funcionales y operativos, que soporten las estrategias que requiere la Fiscalía para apoyar las investigaciones criminales en el ciberespacio y que sirvan de referente para la creación de otros centros cibernéticos en el país.

- Tanto los centros de investigación relacionados que se encuentran en la región, así como la documentación que existe en torno a la ciberdelincuencia, están direccionados a la seguridad de la información y a la protección de la misma como bien jurídico, sin tener un componente base relacionado con el uso de las tecnologías como medio para cometer cualquier tipo de delito.

- Respecto a la participación de la Fiscalía frente al tema de las investigaciones y análisis criminal de los ciberdelitos y el apoyo que esta le pueda brindar a otras entidades como Policía Nacional, que es un referente en el tema, se están adelantando mesas de trabajo para lograr unificar criterios frente a la información que tiene la entidad a través de sus sistemas misionales y poder compartirla en pro de la justicia del país.

- La Entidad debe ser un actor activo en la definición de las condiciones que frente a los ciberdelitos se establezcan y ser una voz desde el sector justicia que indique las actuaciones sobre las cuales se den regir documentos como el nuevo CONPES en ciberseguridad propuesto por el gobierno.
- Se deben articular las diferentes áreas que al interior de la Fiscalía, tienen competencias con la temática de delitos informáticos, como son: el área de informática forense, el área de delitos informáticos y las áreas de cibercriminalidad de las Delegadas de Seguridad ciudadana y de crimen organizado, esto con el fin de establecer un único plan de acción que oriente las actuaciones de los investigadores y analistas respecto a la temática de ciberdelitos.

Glosario de términos de Ciberseguridad

A continuación, se describen algunos de los términos más utilizados en el ambiente informático relacionados con la seguridad de la información y por ende con la seguridad y defensa en el ciberespacio. La descripción de cada uno de ellos se encuentra incluido en la guía de aproximación para el empresario que emite el Instituto Nacional de Ciberseguridad de España (2017). Glosario de términos de ciberseguridad. INCIBE. Recuperado el 5 de febrero de 2019, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Activo de información

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Adware

Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores.

Aunque se asocia al *malware,* no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de *software* que lo implementan en sus programas, generalmente en las versiones *shareware*, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en *malware* en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad

Antivirus

Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware*.

La forma de actuar del antivirus parte de una base de datos que contiene parte de los códigos utilizados en la creación de virus conocidos. El programa antivirus compara el código binario de cada archivo ejecutable con esta base de datos. Además de esta técnica, se valen también de procesos de monitorización de los programas para detectar si éstos se comportan como programas maliciosos.

Autenticación

Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

Bomba Lógica

Trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que se ejecuta una acción maliciosa.

La característica general de una bomba lógica y que lo diferencia de un virus es que este código insertado se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador.

Botnet

Una *botnet* es un conjunto de ordenadores (denominados *bots*) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de *spam*, ataques de *DDoS*, etc.

Las *botnets* se caracterizan por tener un servidor central (*C&C*, de sus siglas en inglés *Command & Control*) al que se conectan los *bots* para enviar información y recibir comandos.

Existen también las llamadas *botnets P2P* que se caracterizan por carecer de un servidor *C&C*

Cartas nigerianas

Se trata de una comunicación inesperada mediante correo electrónico carta o mensajería instantánea en las que el remitente promete negocios muy rentables.

La expectativa de poder ganar mucho dinero mediante unas sencillas gestiones es el gancho utilizado por los estafadores para involucrar a las potenciales víctimas en cualquier otra situación engañosa, procurando que finalmente transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

Denegación de servicio

Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.

El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

Dirección IP

Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separado por puntos. Por ejemplo: 192.168.121.40

En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

DNS

El término DNS, del inglés *Domain Name Service*, se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio.

El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.

Exploit

Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de *exploit* se suele perseguir:

- el acceso a un sistema de forma ilegítima
- obtención de permisos de administración en un sistema ya accedido
- un ataque de denegación de servicio a un sistema

Incidente de seguridad

Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Malware

Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*.

Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Puerta trasera

Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante.
Por lo tanto aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat. Chat.

Sniffer

Un *sniffer* es un programa que monitoriza la información que circula por la red con el objeto de capturar información.
Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema.
Si no es así, la rechaza. Un *sniffer* lo que hace es colocar a la placa de red en un modo el cual desactiva el filtro de verificación de direcciones (promiscuo) y por lo tanto acepta todos los paquetes que llegan a la tarjeta de red del ordenador donde está instalado estén dirigidos o no a ese dispositivo.
El tráfico que no viaje cifrado podrá por tanto ser «escuchado» por el usuario del *sniffer*.
El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto).

Spyware

Es un *malware* que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.
El término *spyware* también se utiliza más ampliamente para referirse a otros productos como *adware*, falsos antivirus o troyanos.

Zero-day

Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

Por esta razón son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

Referencias Bibliográficas

- Acore. (2016, Sept 16) La doctrina militar "Damasco". Recuperado de https://www.acore.org.co/boletin-acore/la-doctrina-militar-damasco/
- Ballesteros, M. C. R., & Hernández, J., Antonio G. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento/Cybercrime: Particularities in investigation and prosecution. Anuario Jurídico y Económico Escurialense, (47), 209-233. Recuperado de: https://search.proquest.com/docview/1528550562?accountid=143348
- Bolaños, D., G. (2015, Jun 29). ¿Qué se compra, qué idioma se habla y qué esconde la deep web? Cinco Dias Recuperado de https://search.proquest.com/docview/1691877140?accountid=143348
- Bueno de Mata, F. (2016). Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [BOE n. ° 239, 6-X-2015]. Ars Iuris Salmanticensis, vol. 4, junio 2016, 326-328 eISSN: 2340-5155 © Ediciones Universidad de Salamanca - cc by-nc-nd. Pgs. 326-328 https://gredos.usal.es/jspui/bitstream/10366/130070/1/Ley_Organica_13_2015,_de_5_de_octubre,_d.pdf
- Camacho Garcia, J. D. (2016). Evolución de la ciberdefensa y la seguridad de la información en Colombia (Bachelor's thesis, Universidad Militar Nueva Granada). http://hdl.handle.net/10654/14382
- Cano Martínez, Jeimy José. El peritaje informático y la evidencia digital en Colombia: Conceptos, retos y propuestas. 2010. Ediciones Uniandes

- Cárdenas Lesmes, R. M. (2011). Política de ciberseguridad y ciberdefensa. Portafolio, Recuperado de https://search.proquest.com/docview/885568347?accountid=143348
- Centro de Investigación y Seguridad Nacional - CISEN (2010) http://www.cisen.gob.mx/
- Centro de Investigación y Seguridad Nacional - CISEN (2010). Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/58680/ASI_Proceso_Administraci_n_de_la_Seguridad_de_la_Informaci_n.pdf
- CESGIR. (2017). Ciberseguridad, asunto de todos. Portafolio, Recuperado de https://search.proquest.com/docview/1860887745?accountid=143348
- Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital. Kyung Shick Choi y Marlon Mike Toro-Alvarez. Bogotá: Universidad Antonio Nariño. Vicerectoría de Tecnología, Ciencia e Innovación. Fondo Editorial, 2017.
- COLCERT (http://www.colcert.gov.co/?q=acerca-de, consultada el día 28 de marzo de 2018)
- Congreso de Colombia, 2005. Ley 985 de 2005. Recuperado de: https://www.icbf.gov.co/cargues/avance/docs/ley_0985_2005.htm
- Congreso de Colombia, 2009. Ley 1273 de 5 de enero de 2009. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
- Congreso de la República del Perú. Ley 30096. Recuperado de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/
- Congreso de la República del Perú (). Ley 30171. Recuperado de https://www.deperu.com/legislacion/ley-30171-pdf.html
- Consejo de Europa. Convenio de Budapest. 2011. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

- DNP. (2016) CONPES 3854. Política Nacional de Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- DNP. (2011) CONPES 3701. Política Nacional de Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
- Fiscalía General de la Nación (2006). Manual de procedimientos de Fiscalía en el Sistema Penal Acusatorio
- Fiscalía General de la Nación (2016). Plan Estratégico
- Fiscalía General de la Nación (2018). Proyecto de ley para liberar a los niños de las drogas, castigar con rigor a los reincidentes y sancionar los ciberdelitos. Tomado de: https://www.fiscalia.gov.co/colombia/fiscal-general-de-la-nacion/proyecto-de-ley-para-liberar-a-los-ninos-de-las-drogas-castigar-con-rigor-a-los-reincidentes-y-sancionar-los-ciberdelitos/
- Función pública. Manual de Estructura del Estado Colombiano. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/ejecutiva-orden-nacional.php
- García G, Javier. (Barcelona 2015). Oportunidad criminal, internet y redes sociales. INDRET Universidad de Navarra. http://www.indret.com
- García, A. Marta (2016, Jul 01). ASÍ SERÁN LOS DELITOS DEL FUTURO. Actualidad Económica, 51. Recuperado de https://search.proquest.com/docview/1798557948?accountid=143348
- Grupo de delitos telemáticos de la Guardia Civil. (2015). Combatiendo el cibercrimen. http://www.astic.es/sites/default/files/articulosboletic/monografico4oscardelacruz.pdf
- Guía de términos de ciberseguridad (2017) Instituto Nacional de Ciberseguridad INCIBE. Recuperado de

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

- Hecsan. (2015). Denuncias de ciberdelitos crecen al 25% en Colombia. Portafolio, Recuperado de https://search.proquest.com/docview/1728209279?accountid=143348
- Instituto Nacional de Ciberseguridad – INCIBE. Recuperado de: https://www.incibe.es/
- Law Enforcement Cyber Center. About the Cyber Center. Recuperado de http://www.iacpcybercenter.org/about-the-cyber-center/
- LUICON. (2016). La ciberdelincuencia no segmenta: Todos somos vulnerables. Portafolio, Recuperado de https://search.proquest.com/docview/1765294635?accountid=143348
- Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82
- Ministerio de Defensa. Plan Estratégico Sectorial de Tecnologías de la Información y las Comunicaciones 2018 – 2022 (Borrador). 2017.
- Ministerio de Defensa. Guía Metodológica para la Proyección de Financiación de Capacidades. 2018
- Ministerio de Defensa. Guía Metodológica de Planeamiento por Capacidades. 2018
- Ministerio de justicia y del derecho (2014). Decreto 016 de 2014
- Ministerio de justicia y del derecho (2017). Decreto 898 de 2017
- Ministerio del Interior (2016). https://www.mininter.gob.pe/content/ciberpolic%C3%AD-contra-delitos-inform%C3%A1ticos
- Mintic. Gobierno radicó Proyecto de Ley para adherirse al Convenio de Budapest contra la ciberdelincuencia. 10 de junio de 2018. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-56315.html
- Miró L, F. (Madrid 2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Edit. Marcial Pons http://www.marcialpons.es/static/pdf/9788415664185.pdf

- Miró Llinares, Fernando. La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología (en línea). 2011, núm. 13-07, p. 07:1-07:55. Disponible en internet: http://criminet.ugr.es/recpc/13/recpc13-07.pdf
- Montoliú, P. (2014, Feb 23). 'Ciberdelincuencia', el nuevo reto. Cinco DiasRecuperado de https://search.proquest.com/docview/1522497399?accountid=143348
- Moscardó, I. (2014, Nov 16). La web profunda pone en jaque su seguridad. Cinco Dias Recuperado de https://search.proquest.com/docview/1625266395?accountid=143348
- N. D. Jesus, (2010). Ciberdelincuentes, tras control de firmas. Portafolio, Recuperado de https://search.proquest.com/docview/816525944?accountid=143348
- Moury, Taciana. Ejército de Brasil invierte en defensa cibernética. 12 de mayo de 2017. Recuperado de: https://dialogo-americas.com/es/articles/brazilian-army-invests-cyber-defense
- Nova Alarcón, Michael Alejandro (2016). Ciberestrategia Colombia. Ed. Universidad Militar Nueva Granada http://hdl.handle.net/10654/14171
- Office of Legal Education Executive Office for United States Attorneys (2007). Prosecuting Computer Crimes.
- Oficina de las Naciones Unidas para la Droga y el delito – UNODC. Estudio exhaustivo sobre el delito cibernético. 2013
- Organización de los Estados Americanos – OEA. Buenas prácticas para establecer un CSIRT nacional. Recuperado de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
- P Sempere, /. M. G. P. (2016, Jul 23). Así operan los ciberdelincuentes. Cinco Dias Recuperado de https://search.proquest.com/docview/1806255355?accountid=143348

- Peralta Rodríguez, O. H. (2016). Ciberseguridad: nuevo enfoque de las Fuerzas Militares en Colombia (Bachelor's thesis, Universidad Militar Nueva Granada). http://unimilitar-dspace.metabiblioteca.org/bitstream/10654/7884/1/ensayo%20final%20EAS-2015%20UMNG%20OSCAR%20PERALTA.pdf
- Pérez, Carla. Policía Nacional del Ecuador. Delitos informáticos establecidos en el COIP y cómo prevenirlos. 27 de diciembre de 2017. Recuperado de: http://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/
- Pineda Fandiño, Miguel Heráclito (2017). Planeación basada en capacidades, herramienta de gestión para la transformación y futuro de la Fuerza Pública en Colombia. Universidad Militar
- Polanco, Marcos. (2016). La ciberinteligencia como habilitador de la ciberseguridad. Tomado de la revista electrónica MAGAZCITUM http://www.magazcitum.com.mx/?p=3205#.WNvEcc81_IU
- Presidencia de la República del Brasil. Decreto 6703 del 18 de diciembre de 2008. Recuperado de: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm
- Posada Maya, Ricardo. Los cibercrímenes: un nuevo paradigma de criminalidad. 2017. Grupo Editorial Ibañez.
- Riva, R. C. (2016). El nuevo entorno digital de la actividad criminal/a new digital environment for criminal activity. Boletín De Estudios Económicos, 71(219), 591-612. Recuperado de https://search.proquest.com/docview/1864119518?accountid=143348
- Rivera Vazquez, J. C. (2012). Percepción del crimen cibernético y la confianza en la asignación de recursos para combatirlo: Un estudio multisectorial en puerto rico (Order

No. 3511539). Available from Psychology Database. (1023109092). Recuperado de https://search.proquest.com/docview/1023109092?accountid=143348

- Rojas, P.J. (2017, enero-julio). Doctrina Damasco: eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Rev. Cient. Gen. José María Córdova* 15(19), 95-119. DOI: http://dx.doi.org/10.21830/19006586.78

- ROPERO, Javier García. (2016, Jun 24). El ciberespacio, el nuevo campo de batalla. Cinco Días Recuperado de https://search.proquest.com/docview/1799302921?accountid=143348

- Serrano, José. Ministerio del Interior. Ciberdelitos serán enfrentados e investigados por una nueva estructura policial. 3 de febrero de 2016. Recuperado de: https://www.ministeriointerior.gob.ec/ciberdelitos-seran-enfrentados-e-investigados-por-una-nueva-estructura-policial/

- S, M., & M, J. (2009, Jul 01). EE UU y europa avanzan hacia la ciber policía global. Cinco Dias Recuperado de https://search.proquest.com/docview/431451202?accountid=143348

- Software Engineering Institute. (2013) SEI Innovation Center Report: Cyber Intelligence Tradecraft Project. Recuperado de http://www.dtic.mil/get-tr-doc/pdf?AD=ADA585939

- Suarez Sánchez, Alberto. Manual de delito informático en Colombia: análisis dogmático de la Ley 1273 de 2009. 2016. Editorial Universidad Externado de Colombia

- Temperini, A. M., Borghello, C., & Macedo, A. M. La cifra negra de los delitos informáticos: Proyecto ODILA. https://www.ekoparty.org/archivo/2014/eko10-La_cifra_negra_de_los_delitos_informaticos.pdf

- TERUELO, Javier Fernández. Derecho Penal e Internet (e-book). Lex Nova, 2011. https://books.google.com.co/books?id=91h0U1ji_pQC&printsec=frontcover#v=onepage&q&f=false
- Umaña Ramírez, G., & Mosquera Navarrete, I. C. (2014). Diseño e implementación de un centro de informática forense en la Universidad Autónoma de Occidente (Bachelor's thesis, Universidad Autónoma de Occidente). https://red.uao.edu.co/bitstream/10614/6473/1/T04529.pdf
- UNODC (2013). Compilación normativa sobre la trata de personas en Colombia Convenio M – 221 de 2013 entre UNODC y el Ministerio del Interior Acuerdo de contribución DCI – MIGR / 2013 / 282 – 731 Unión Europea
- Valdivielso Villanueva, L. (2016). Las diligencias de investigación tecnológica y su aplicación práctica en el orden jurisdiccional penal. Escuela de práctica jurídica Salamanca http://hdl.handle.net/10366/132618

Índice de gráficas

Índice de tablas

Anexos

Encuesta de diagnóstico de necesidades

CIBERDELITOS: UN RETO PARA LA FISCALÍA GENERAL DE LA NACIÓN

Encuesta de diagnóstico de necesidades

La encuesta a continuación pretende identificar los aspectos principales que la Entidad debe enfrentar en las investigaciones sobre delitos que afecten la información y los datos, consignados en la Ley 1273 de 2009 y así, establecer las capacidades con que debería contar, al implementar un Centro Cibernético de Investigación.

La encuesta está dividida en 5 partes, cada una de las cuales corresponde a las capacidades relacionadas en el modelo DOMPI y una parte adicional que señala aspectos generales de quien realiza la encuesta.

La población a quién está dirigida la encuesta corresponde a los investigadores y fiscales que desde la variable de delitos informáticos manejan este tipo de situaciones a nivel nacional.

PARTE 1. DOCTRINA

Pregunta 1. Conoce si la Fiscalía General de la Nación cuenta con documentación en el sistema de gestión de calidad que oriente sobre las actuaciones relacionadas con la investigación de delitos informáticos?

SI NO

Si la respuesta es afirmativa, nombre uno

Pregunta 2. Conoce algún tipo de proyecto institucional que apoye la labor de investigadores en la obtención de elementos materiales probatorios en el ciberespacio?

SI NO

Si la respuesta es afirmativa, descríbalo

Pregunta 3. Conoce si dentro del Direccionamiento Estratégico de la Entidad, existen condiciones que favorezcan las actividades de investigación de delitos que utilicen los medios electrónicos como medio o como fin?

SI NO

PARTE 2. ORGANIZACIÓN

Pregunta 4. Conoce los perfiles criminales de los ciberdelincuentes?

SI NO

Si la respuesta es afirmativa, nombre uno

Pregunta 5. La gran mayoría de investigaciones relacionadas con tecnología, están asociadas a software malicioso o malware. Conoce Ud. si alguno de los grupos asociados la investigación de delitos informáticos, realiza análisis o pruebas con el software malicioso encontrado?

SI NO

Pregunta 6. Existe en la entidad analistas de información dedicados a analizar e informar sobre la afectación que tiene el software malicioso o las técnicas utilizadas en la realización de delitos que utilicen la tecnología como medio o como fin?

SI NO

Pregunta 7. Existe alguna metodología que aplique la Entidad para la investigación de delitos que utilicen la tecnología como medio o como fin? Descríbala

SI NO

PARTE 3. MATERIAL Y EQUIPO

Pregunta 8. El término OSINT hace referencia a la explotación que se da de las fuentes abiertas para obtener información relevante de inteligencia. Ha utilizado este tipo de herramientas?

SI NO

Pregunta 9. La Entidad cuenta con herramientas licenciadas para la identificación y recolección de datos. Conoce sobre estas herramientas?

SI NO

Pregunta 10. Conoce herramientas de correlación de datos?

SI NO

Pregunta 11. Conoce herramientas antimalware?

SI NO

Pregunta 12. Conoce herramientas antiforense?

SI NO

PARTE 4. PERSONAL

Pregunta 13. Considera que cuenta con los conocimientos adecuados para realizar actividades de investigación y/o realizar órdenes a la policía judicial relacionadas con delitos informáticos?

SI NO

Pregunta 14. Conoce personal dentro de la entidad con conocimientos y/o experiencia en investigaciones en el ciberespacio?

SI NO

Pregunta 15. Ha recibido capacitación respecto a delitos informáticos?

SI NO

Pregunta 16. Al obtener direcciones IP, software malicioso, información de los ISP, sabe con claridad que debe hacer para aportar a la investigación de delitos informáticos?

SI NO

PARTE 5. INFRAESTRUCTURA

Pregunta 17. La Entidad cuenta con un espacio o área donde se puedan realizar pruebas con el software malicioso encontrado?

SI NO

Pregunta 18. Los grupos de informática forense y los de delitos informáticos están interconectados a nivel nacional?

SI NO

Pregunta 19. Sabe qué es la Deep Web?

SI NO

Pregunta 20. Sabe si es necesario contar con un sistema informático especial para el ingreso a la Deep Web?

SI NO