Diagnóstico : fortalecimiento y articulación de las capacidades misionales de la Fiscalía General de la Nación en la Investigación Penal en el Ciberespacio

Rosangela López Álvarez

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

2018

345.0268
L663
Ej.2

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

DIAGNÓSTICO, FORTALECIMIENTO Y ARTICULACIÓN DE LAS CAPACIDADES MISIONALES DE LA FISCALÍA GENERAL DE LA NACIÓN EN LA INVESTIGACIÓN PENAL EN EL CIBERESPACIO

101853

ALUMNO:

ROSANGELA LÓPEZ ALVAREZ

DIRECTOR:

MAGÍSTER MANUEL HUMBERTO SANTANDER PELÁEZ

GRUPO DE INVESTIGACION
MASA CRÍTICA

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO

BOGOTA – COLOMBIA

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

DIAGNÓSTICO, FORTALECIMIENTO Y ARTICULACIÓN DE LAS CAPACIDADES MISIONALES DE LA FISCALÍA GENERAL DE LA NACIÓN EN LA INVESTIGACIÓN PENAL EN EL CIBERESPACIO

ALUMNO: ROSANGELA LÓPEZ ALVAREZ

DIRECTOR: MAGÍSTER MANUEL HUMBERTO SANTANDER PELÁEZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTA – COLOMBIA

2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Bogotá, Mayo 2018

Dedicatoria

Al Dios de amor, por caminar junto a mí y darme la salud y la sabiduría para iniciar, mantenerme y culminar este proyecto.

A mí amado hijo, esposo y madre

Posiblemente en este momento no entiendas el alcance de mis palabras, pero para cuando lo sepas, quiero que te des cuenta de lo que significas para mí, eres la razón de que me levante cada día esforzándome por el presente y el futuro, eres mi principal motivador. Como en todos mis logros, ustedes han estado presente.

Agradecimientos

Agradezco a la Escuela Superior de Guerra que me dio el ingreso al mundo de la Ciberdefensa y Ciberseguridad, agradezco la colaboración, asesoría, y conocimientos suministrados. En general, la ayuda recibida por docentes y administrativos que hicieron posible el desarrollo académico y logístico de la Maestría.

Contenido

Lista de Gráficas

Pág.,

Lista de Figuras

Pág.,

Resumen

El aumento en materia de delitos cibernéticos promueve la aparición de diversas formas organizadas y especializadas dedicadas al cibercrimen, visión que reta las capacidades de las entidades enfocadas a desarrollar investigación penal. El presente documento pretende lograr un diagnóstico y análisis sobre la manera actual de cómo la Fiscalía General de la Nación enfrenta los desafíos en la lucha contra el cibercrimen, así como presenta una propuesta de fortalecimiento, mejora y buenas prácticas en aras de lograr una lucha más efectiva sobre los nuevos fenómenos en el ciberespacio.

El problema; desarticulación de estructura organizacional, fragmentación de información, falta de conocimientos especializados por parte de los actores que intervienen en el proceso judicial, denuncias, cifra negra, resultados de las investigaciones penales, legislación adecuada para evidencia física, necesidad de cooperación y colaboración nacional e internacional, incremento de la especialización de los ciberdelincuentes, entre otros, serán los temáticas planteadas como elementos de una radiografía actualizada sobre el estado de situación de la Fiscalía General de la Nación.

Es este sentido se propone el fortalecimiento y articulación de capacidades misionales para la investigación penal en el ciberespacio agrupados administrativamente en una unidad de investigación con responsabilidades estratégicas y operativas como apoyo a los grupos investigativos del cibercrimen, con impacto a los objetivos estratégicos misionales haciendo frente al delito cibernético definidos en Plan Estratégico 2016-2020. (Fiscalia General de la Nación , 2016).

Palabras claves: Ciberseguridad, Ciberdefensa, Ciberespacio, delito cibernético, prospectiva, análisis, investigación penal, cooperación.

1. Introducción

Hace varios años los delitos cibernéticos forman parte de la delincuencia en el mundo, así como es objeto de investigación de la Fiscalía General de Nación. En este sentido las agencias o entidades de investigación y judicialización penal enfrentan el reto del círculo vicioso del cibercrimen (Brown, 2015), el cual analiza tres perspectivas, i)agencias judiciales; en que las mismas no están actualizadas con las tecnologías de los ataques informáticos, poca preparación en la recolección de evidencia digital proveniente de nuevos dispositivos, sumado a la falta de colaboración con el sector de industria tecnológica y entidades homologas. ii) víctimas; existe débil confianza en las agencias de investigación y judicialización, usan pocos o débiles mecanismos de defensa, baja tasa de denuncias y prefieren pagar por el delito informático, por la importancia de la información que pierden y iii) Ciberdelincuentes; estructuras criminales globalizadas, aumento de confianza por el éxito con poco o ningún castigo, al uso de tecnología sofisticada a bajo precio, así como a su experiencia y perfiles motivados a realizar ataques.

Teniendo en cuenta lo anterior, el presente documento pretende lograr un diagnóstico del como la Fiscalía General de la Nación enfrenta los desafíos en materia de delitos informáticos, Ley 1273 de 2009, capacidades actuales, evidenciar puntos de mejora, así como proponer unos tópicos para fortalecer la oportunidad de éxito frente los resultados de la investigación penal en delitos cibernéticos. La finalidad de este trabajo será, entonces, realizar una radiografía actual de la problemática que asume la Fiscalía General de la Nación en el ámbito de enfrentarse como ente investigador y de judicialización en nuestro país ante el cibercrimen, con el objeto de identificar y comprender los distintos desafíos que se necesitan superar para avanzar en propuestas y desarrollos adecuadas para un real y eficaz lucha contra el cibercrimen.

Para lograr tal propósito, el proceso metodológico utilizado está formado de tres preguntas i) ¿qué? donde se identifica una propuesta de investigación, lo que conlleva a definir los propósitos viables de la investigación. ii) ¿por qué? donde se proporciona la necesidad de la investigación, a fin de probar el valor de la propuesta y estudiar una serie de estrategias de investigación. Y iii) ¿cómo? -La importancia de desarrollar una metodología adecuada y métodos específicos para reunir y generar información relevante para el objeto de la investigación, evaluando, analizando e interpretando las evidencias.

Es de mencionar que en el ámbito de este estudio fue de campo, la investigación se realiza donde se desarrolla el problema, y se toma una muestra representativa logrando generalizaciones con base en los resultados obtenidos en la población muestreada.

Una vez planteada la pregunta de investigación, se realizó análisis, delimitación, descripción y se intentó formular una posible solución en busca de impactar o minimizar las dificultades identificadas para darle respuesta a los nuevos fenómenos en el ciberespacio, y brindar un marco adecuado en el fomento de política criminal.

Se formula un diseño de estructura organizacional institucional (Fiscalía General de la Nación) para la policía judicial con dominios especializados en análisis, estrategias y operatividad, en el ámbito del cibercrimen, en aras de proteger el bien jurídico tutelado denominado "de la protección de la información y de los datos" y preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Ley 1273, 2009), contando con analistas, investigadores y fiscales especializados en la investigación y judicialización del cibercrimen, además de contar con infraestructura tecnológica (hardware/software) actualizada en aras de lograr una comprensión

interdisciplinaria de fenómenos, situaciones y casos que permita orientar estrategias investigativas y focos de atención.

En este sentido y con el objetivo de obtener una solución continúa en el tiempo, el diagnóstico y la solución propuesta tiene un alcance de solución en, i) a diagnosticar las capacidades actuales con que la Entidad aborda el cibercrimen o delitos informáticos, ii) identificar las capacidades misionales necesarias para fortalecer la persecución efectiva de criminales en el ciberespacio, y ii) articulación de capacidades institucionales con entidades homólogas y políticas económicas y sociales en el contexto de la seguridad digital.

Para ser posible lo anterior, se recopila y analiza información sobre los centros de investigación o prospectiva del cibercrimen y unidades especializadas policiales, con un alcance a todos aquellos que incorporan última tecnología y procedimientos en la investigación y análisis del cibercrimen, y que han sido implementados en diferentes sectores, y que actualmente son líderes en el sector de lucha contra el crimen en el ciberespacio, dando como resultado el estado del arte.

En el proceso de recopilación y estructuración de información se identifican experiencias empíricas y metodológicas en reconocer la importancia de contar con un centro que agrupe, recopile, analice, y difunda de modo efectivo, información y conocimiento que posean todas las unidades de investigación sobre casos concretos, apoyados en el universo de datos, así como ofrecer una línea de defensa y judicialización conjunta y contundente, posibilitando con ello la toma de decisiones informadas y respuesta oportunas.

Una vez se cuenta con la suficiente información, finalmente se formulan las capacidades misionales y su articulación para realizar investigación penal en el ciberespacio, agrupadas en un centro de Análisis, Investigación y Prospectiva de Cibercrimen enmarcado en las capacidades

necesarias para lograr unidades cibernéticas especializadas dentro de la justicia como uno de los elementos claves en la respuesta adecuada al delito cibernético. Fundamentado en que la investigación y enjuiciamiento del delito cibernético y análisis forense de las pruebas requieren conocimientos, habilidades y destrezas especiales, además de mecanismos legales y cooperación internacional para hacer frente a este fenómeno transnacional.

En consecuencia a lo expuesto, se busca diagnosticar, fortalecer y articular capacidades misionales que permitan consolidar una efectiva persecución de los criminales en el ciberespacio, en aras de lograr una Entidad preparada, con capacidad continúa de análisis e investigación con impacto a los objetivos estratégicos definidos en la investigación penal para hacerle frente al delito cibernético. (Pisaríc, 2017).

2. Problema de Investigación

Dado el marco Jurídico y organizacional de la Fiscalía General de la Nación, así como la aplicación de su misión de ejercer la acción penal, diseño y ejecución de política criminal de estado, y de manera específica para este caso, en delitos informáticos, así como el avance continuo de las tecnologías y la apropiación en la vida del ser humano se hace necesario diagnosticar, fortalecer y articular las actuales capacidades misionales con que cuenta la Entidad. Es así, que se evidencian de forma general algunos factores que fortalecidos internamente serian la base para lograr el objetivo final de desarrollar investigaciones penales destacadas en el ciberespacio. Esto según mejores prácticas internaciones de organismos homólogos e instituciones de cooperación internacional como la Organización de los Estados Americanos (OEA), Banco Interamericano de Desarrollo (BID), entre otros.

i) la segmentación de la información entre las diferentes unidades nacionales contra los delitos informáticos, no existe coordinación en cuanto la alimentación de bases de datos institucionales donde se incorpora las denuncias, asignación de misiones de trabajo y resultados, imposibilitando la idea de minería de datos, prospectiva entre otras con el fin de correlacionar información y proveer situaciones que podrían derivarse de variables conjugadas.

ii) Fragmentación, la información y procesos tienden a estar aislados entre las diferentes unidades investigativas, la identificación, individualización y judicialización (generación de mecanismos procesales para el control de la pena) se da de forma individual por conducta criminal, el sistema de investigación tradicional representa para la Fiscalía General de la Nación

y el trabajo de los fiscales una duplicidad de esfuerzos en el que no se sabe finalmente qué está investigando, más allá del caso que tiene asignado.

iii) Falta de conocimientos especializados por parte de los actores que intervienen en el proceso judicial, como:

- Identificación de todos los flujos de información y captura de la misma, que permita asociación de casos a partir de patrones criminales, es decir que las investigaciones se pueden asociar a partir de patrones criminales, para así llegar a indagar a la organización criminal y no solamente al hecho puntual que solo busca establecer quién perpetró el delito, sino cual fue toda la organización que estuvo detrás.
- Construcción de contextos que permiten comprender la estructura y funcionamiento de la organización; es decir que este tipo de investigación permite es identificar directamente la máquina productora del delito, es decir a la red criminal.
- Realización de investigaciones en contexto que posibilite la interacción entre la clásica investigación criminal y las metodologías de las ciencias sociales como la historia, ciencia política, antropología y ciencias exactas. Esto quiere decir que en la investigación clásica solo participaba el abogado, el investigador y la policía judicial, ahora con la intervención de las demás ciencias del conocimiento, los procesos permitirán entender el fenómeno criminal de por qué paso eso o por qué en una región determinada se ha disparado la delincuencia en determinadas épocas.
- Preservación, procesamiento y validez de pruebas digitales, para luego realizar la judicialización (generación de mecanismos procesales para el control de la pena).

iv) el no compartir información, sin ver las oportunidades de mejora como adolecer de desconocimiento, fragmentación y duplicación de la misma, a través del desarrollo de un sistema de intercambio de información que cuente con los medios de fiscalización y seguridad para la protección de los datos con organismos homólogos nacionales e internacionales.

v) no contar con una fábrica o tanque de pensamiento que facilite el análisis, diseño y seguimiento de problemáticas en Ciberseguridad, ciberdelincuencia, cibercriminalidad y ciberconvivencia entre otros, permitiendo la influencia o generación de política pública o toma de decisiones informada.

Se requiere entonces de un perfeccionamiento organizacional y de procesos que permitan la generación y mantenimiento de capacidades en Ciberseguridad, de capacidades especializadas misionales como, integración de la información, especialización del talento humano, consolidación de mecanismos de cooperación nacional e internacional, entre otros, que finalmente deriven en una Entidad que cuente con las herramientas humanas, jurídicas, relacionales y tecnológicas para ejercer la acción penal frente el cibercrimen. De esta manera de formula la siguiente pregunta. (UNODC-United Nations Office on Drugs and Crime, 2013)

Pregunta: ¿La Fiscalía General de la Nación cuenta con suficientes capacidades (procesos, personas, tecnología) para realizar investigaciones penales destacas en el ciberespacio, con recursos y aptitudes continuas para realizar análisis, investigaciones y prospectiva con impacto a los objetivos estratégicos misionales?

3. Justificación

Existen razones por la cuales vale la pena responder el problema planteado para la Fiscalía General de la Nación, las cuales de desprenden de tres argumentos principales.

1. Responsabilidades adquiridas por la Institución en el marco de su creación, particularmente ejercer la acción penal, así como influir en la política criminal de estado, razones enmarcadas en la misión de la Entidad.
2. Los compromisos que se desprenden de las políticas económicas y sociales del país, para este caso particular el Conpes 3701 de 2011 "Lineamientos de Ciberseguridad y Ciberdefensa y 3854 de 2016 " Seguridad Digital" así:

   El Conpes 3701 de 2011 cuyo objetivo fue generar lineamientos de política en Ciberseguridad y Ciberdefensa orientados a desarrollar estrategia nacional que contraste el incremento de las amenazas informáticas de significancia para el país, así como recoger los antecedentes nacionales e internacionales, y la normatividad del país en torno al tema, centrando su problemática en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y que no existe una estrategia nacional al respecto, estableciendo causas y efectos que permitieran desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. (Departamento Nacional de Política Económica y Social, 2011, pág. 2). Definiendo recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia.

Inmediatamente el Conpes 3854 de 2016 incorpora plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital, avanzando más allá de temas de Ciberseguridad y Ciberdefensa, y reconociendo que la seguridad digital es importante para todos los ciudadanos, para que gestionen y conozcan riesgos asociados con su interacción con la economía digital, teniendo como componentes la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación. (Conpes 3854 - Seguridad Digital, 2016)

Además, integra objetivos de lucha contra el crimen y la delincuencia en internet, temas que aborda la misionalidad de la Fiscalía General de la Nación. Y donde se resalta entre el diagnostico relacionado la problemática asociada a ausencia o debilidad en las siguientes capacidades:

- "No se cuenta con los recursos humanos, técnicos y financieros suficientes para enfrentar nuevos tipos de crimen, delincuencia y fenómenos en el entorno digital, bajo un enfoque de gestión de riesgos" (Conpes 3854 - Seguridad Digital, 2016, pág. 41).
- "El marco jurídico para contrarrestar el delito cibernético y para gestionar los delitos en los que estén implicados evidencias electrónicas no es adecuado" (Conpes 3854 - Seguridad Digital, 2016, pág. 42).
- "No existe conciencia sobre los nuevos tipos de cibercrimen y ciberdelito" (Conpes 3854 - Seguridad Digital, 2016, pág. 55).
- "Se identifica que el número de fiscales capacitados para lograr construir un caso validado sobre pruebas electrónicas es limitado. Lo anterior, porque a pesar que se han tenido algunos programas de formación especializada, aún hace falta institucionalizar estos

esfuerzos y ampliar los mecanismos de colaboración entre la fiscalía y la policía, obteniendo de esta forma un apoyo en la resolución de casos de delitos cibernéticos" (Conpes 3854 - Seguridad Digital, 2016, pág. 42).

- "Los jueces, fiscales y policías no tienen capacidades suficientes en materia de delitos informáticos, ni en los aspectos técnicos y jurídicos de la obtención de evidencia digital" (Conpes 3854 - Seguridad Digital, 2016, pág. 43).
- "El incremento continuo de la comisión de las conductas delictivas cibernéticas y su reincidencia, entre otros factores, se debe al desconocimiento por parte de los administradores de justicia de la conducta criminal informática" (Conpes 3854 - Seguridad Digital, 2016, pág. 43).

Ahora, sumado a lo anterior, la Entidad también se ve inmersa en el desarrollo del el objetivo estratégico 3 del Conpes 3854 de 2016, que indica, "fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos" (Conpes 3854 - Seguridad Digital, 2016, págs. 5,53-60), aplicando las siguientes estrategias:

- Socializar y concientizar las tipologías de cibercrimen y ciberdelincuencia a las múltiples partes interesadas.
- Socializar periódicamente a las múltiples partes interesadas respecto de los avances frente al fenómeno de cibercriminalidad y sobre los delitos informáticos que atenten contra la seguridad nacional en el entorno digital.
- Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes.

- Diseñar contenido educativo especializado y capacitar a los funcionarios responsables de garantizar la seguridad en el entorno digital en el país, así como aquellos encargados de la judicialización de delitos cibernéticos.
- Se debe encaminar a construir un marco jurídico maduro que apoye los procesos judiciales, juzguen conductas de manera efectiva, apoyen procesos de investigación estructural, y cuente con la capacidad de adaptarse dinámicamente en función de las circunstancias imperantes. (Conpes 3854 - Seguridad Digital, 2016, págs. 5,53-60).

Es así, entonces que la Fiscalía General de la Nación debe identificar las actuales capacidades con las que cuenta frente al anterior diagnóstico realizado por los anteriores Conpes, así como desarrollar, fortalecer y articular capacidades teniendo en cuenta los desafíos actuales frente el cibercrimen, dando respuesta efectiva a su misión, y ser parte de la solución a la problemática planteada, aunando finalmente en fortalecer las capacidades de las partes interesadas y garantizar un desarrollo seguro en el ciberespacio desde la práctica del ejercicio de la acción penal.

Por lo anterior las capacidades desarrolladas deben incorporar respuestas a la segmentación, fragmentación, falta de conocimientos especializados, así como debe permitir el intercambio efectivo de información, análisis y prospectiva del comportamiento del fenómeno cibercriminal.

3. La constante evolución de las amenazas en el ciberespacio, que obliga a las agencias judiciales constantemente a desarrollar y fortalecer capacidades, así como propender una integración con otras instituciones del estado, en procura de ejecución operacional y la optimización de recursos. Esto teniendo en cuenta que el ciberespacio es una red y la mejor forma de combatirlo es en red.

Puede indicarse entonces, que la razón de ser de este documento se fundamenta en apoyar las siguientes funciones a nivel interno: i) investigar y perseguir delitos contra datos informáticos y sistemas; ii) investigar y perseguir delitos cometidos por medios de datos y sistemas informáticos; iii) la realización de informática forense con respecto a pruebas electrónicas. (Ballesteros & Hernandez, 2014). Y externo: i) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, ii) fortalecer la defensa y soberanía nacional en el entorno digital, iii) generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en judicialización de los delitos en el ciberespacio. (Conpes 3854 - Seguridad Digital, 2016).

Finalmente este trabajo busca no solo satisfacer las obligaciones mencionadas si no realizar un ejercicio de diagnóstico, fortalecimiento y articulación de las capacidades de la Fiscalía General de la Nación en virtud de los requerimientos del contexto estratégico de la seguridad digital y el rol cada vez mayor de las tecnologías en las actividades cotidianas y criminales de la sociedad, ejercicio apalancado en mejores prácticas y recomendaciones de entidades homologas nacionales (colCERT, Centro Cibernético Policial, Comando Conjunto Cibernético – CCOC, CSIRT Gobierno y Sector Privado), así como organizaciones internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OECD) y de la Organización de Estados Americanos (OEA).

4. Objetivos

4.1 Objetivo General

Propuesta de fortalecimiento de capacidades investigativas en el ejercicio de la acción penal en el ciberespacio.

4.2 Objetivos Específicos

- Diagnosticar las capacidades actuales con que la Fiscalía General de la Nación aborda y realiza la investigación penal en los delitos informáticos.
- Identificar las capacidades misionales necesarias para abordar la investigación penal en el ciberespacio con una persecución efectiva de los criminales e identificar las capacidades de Ciberseguridad que permitan la continuidad y sostenimiento en la misma.
- Articulación de capacidades institucionales con entidades homólogas y políticas económicas y sociales en el contexto de la seguridad digital.
- Definir requerimientos esenciales para el diseño de una unidad administrativa que permita el análisis, investigación y prospectiva de cibercrimen, orientado al desarrollo de la investigación penal en el ciberespacio.

5. Desarrollo de la investigación penal en el ciberespacio

5.1. Estado del Arte

5.1.1 Antecedentes A Nivel Mundial

Para dar inicio y poder contextualizar sobre la actualidad de los centros de observación o investigación de cibercrimen, se debe delimitar el tema de estudio, sus relaciones con otros objetos, identificar actores, avances y sobre todo cuales son las tendencias actuales existentes en aras de conocer el conocimiento acumulado sobre el mismo; ello a partir del concepto que se pretende desarrollar en la Fiscalía General de la Nación.

En este sentido, tal concepción compromete un centro de estudios e investigación que potencializara las capacidades humanas y técnicas para abordar de forma actualizada los hechos que revistan fenómenos criminales en el ciberespacio; logrando a su vez visibilidad e inteligencia prospectiva sobre amenazas, en pro de detectar y reducir riesgos ante nuevos fenómenos criminales, esto basado en la recopilación de experiencias en las investigaciones técnicas, compartición de conocimiento de entidades homologas, y en enjuiciamiento de delincuentes.

Es así, que todo se origina en la inclusión de la tecnología en todos los ámbitos y escenarios de desarrollo de la existencia humana, dando pie a la creación de un nuevo dominio artificial creado medios informáticos denominado ciberespacio (Diccionario de la Real Academia Española (DRAE), 2010), del cual nadie tiene el control absoluto. Este nuevo dominio se ve aprovechado por los cibercriminales quienes encuentran un espacio donde pueden desarrollar toda su actividad delictiva fortaleciendo sus opciones de economía, anonimato, ubicación y velocidad de ataque. (Centro Superior de Estudios de la Defensa Nacional, 2012)

Inicialmente el delito cibernético nace como un tema altruista o romántico (Salom, 2011) , donde se defendían causas idealistas, se realizan acciones como, acceso a equipos de cómputo, robo de información, para luego evolucionar a organizaciones criminales con comportamientos que aprovechan las innovaciones tecnológicas y agujeros de seguridad para agilizar operaciones y obtener grandes rentabilidades, con acciones como ataques a sistemas scada, denegación de servicios y guerra electrónica. Esto, para finalmente llegar al concepto de Ciberdefensa (Conpes 3854 - Seguridad Digital, 2016), como el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales y Ciberseguridad, (Conpes 3854 - Seguridad Digital, 2016) como el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Es así, que el cibercrimen se considera una amenaza en la era digital en un mundo globalizado y conectado aumentando los riesgos y vulnerabilidades en la sociedad, y aún más de los países desarrollados, dada su dependencia a la tecnología. Enfrentar y combatir, ahora y en el futuro, este fenómeno supone una de los mayores retos y dificultades de todos los tiempos. (OTAN, 2011) (Centro Superior de Estudios de la Defensa Nacional, 2012).

Para el caso de la Fiscalía General de la Nación y otros organismos estatales de investigación criminal, exige a fiscales, investigadores y analistas del cibercrimen mantenerse a la velocidad del mismo, con iniciativas penales, aplicación de la ley y generación de política criminal para

lograr efectividad capaz de prevenir y enjuiciar a los criminales. Además de tener en cuenta que solo habrá éxito a través de una comunidad nacional e internacional interconectada que trabaje como uno solo.

El cibercrimen compromete daño a los ciudadanos, organizaciones, empresas, sistemas scada, entre otros, enmarcados de manera general en las legislaciones sobre delitos informáticos contemplados en los diferentes países. A continuación una corta recopilación de tipologías de actualidad relativos a actos de cibercriminales basado en información de fuentes abiertas y de denuncias allegados a la Entidad, que introducen a los problemas que a la fecha que se han investigado sobre el fenómeno de delitos en el ciberespacio. (Salom, 2011) (Consejo de Europa, 2001).

- Fraudes originados en el comercio electrónico.
- Fraudes en banca electrónica
- Carding
- Crime as Service
- Ciberespionaje
- Ciberterrorismo
- Delitos económicos a través del uso de la moneda digital
- Ataques a infraestructuras SCADA
- Pornografía infantil a través de la tecnología
- Robo de propiedad intelectual
- Usurpación de identidad
- Estafas en línea

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Secuestro de información

Siendo conscientes que los anteriores eventos de acuerdo a su desarrollo perfectamente pueden alcanzar un impacto global, las organizaciones y los diferentes países buscan estrategias analíticas y operativas para hacer frente a los mismos. Donde uno de los enfoques de las estrategias es realizar análisis de la situación en el marco internacional identificando generadores de amenazas, identificación y análisis de infraestructuras críticas en el rol de Defensa Nacional, concluyendo en el plan de protección TI (Tecnologías de la Información) y TO (Tecnologías de la Operación).

Dado lo anterior, se evidencia la necesidad de gestionar la Ciberseguridad, y judicializar el cibercrimen en todos los sectores de una sociedad como, organizaciones particulares, empresas, infraestructuras críticas y los ciudadanos del común, donde se realice análisis e investigación cibercriminologica sobre la manifestación y evolución del delito, estableciendo causas, efectos e impactos que permitan formular recomendaciones y asesorar la construcción de estrategias de prevención e intervención del delito, en aras de orientar la toma de decisiones del mando

institucional, entidades gubernamentales y no gubernamentales, que impacte en la política pública criminal.

Como evidencias empíricas y metodológicas que se han utilizado para enfrentar este fenómeno, ha sido la de reconocer la importancia de contar con un sistema informático que soporte, procese información y origine productos provenientes de la coordinación entre agencias nacionales, internacionales, sector académico y empresarial, que tenga como función recopilar, analizar y difundir información y conocimiento que posean todas las entidades sobre casos y nuevos fenómenos de cibercriminalidad para que los que toman las decisiones y medidas de respuesta, proporcionando inteligencia de fuentes abiertas y cerradas, así como ofrecer una línea de defensa y judicialización conjunta y contundente. (EFE Agencia, 2015)

Teniendo en cuenta las funciones anteriores, se propone el fortalecimiento de las capacidades actuales enmarcadas administrativamente en un Centro de Análisis, Investigación y Prospectiva de cibercrimen, donde se mejore los tiempos de respuesta de procesos penales, y donde se integren un equipo pluridisciplinario que genere conocimiento y capacidad de afrontar problemas complejos. Es decir, el objetivo es lograr productos conceptuales, teóricos y prospectivos orientados a alcanzar el máximo conocimiento de fenómenos cibercriminales e incidir en la prevención y construcción de política criminal y seguridad ciudadana.

Entre los organismos e instituciones que tienen estas competencias o que son fuente de información se encuentran los siguientes:

- **España**

El Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia (CNI) que tiene a su cargo la gestión de la seguridad del ciberespacio en las tres administraciones del Estado. (Centro Criptologico Nacional, 2016)

El CCN-CERT es el Centro de alerta nacional que coopera con todas las administraciones públicas para responder a los incidentes de seguridad en el ciberespacio y vela también por la seguridad de la información nacional clasificada. (Centro Criptológico Nacional, 2016).

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) que depende del Ministerio del Interior. (Centro Nacional para la Protección de las Infraestructuras Críticas, 2010)

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) dependiente del Ministerio de Industria, Turismo y Comercio, encargado de velar por la Ciberseguridad de las PYMES y los ciudadanos en el ámbito doméstico. (Instituto Nacional de Ciberseguridad de España S.A, 2016)

El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, responsables de combatir la ciberdelincuencia. (Grupo de Delitos Telemáticos Unidad Central Operativa, 2011)

La Agencia Española de Protección de Datos, dependiente del Ministerio de Justicia, así como las Agencias de Protección de Datos de la Comunidad de Madrid y de la Generalitat de Cataluña. (Agencia Española de Protección de Datos, 2014)

El Consejo Nacional Consultivo sobre Ciberseguridad (CNCCS) con el objetivo de fomentar la defensa del ciberespacio y colaborar con las entidades públicas y privadas. Entidad Privada. (Cyberseguridad, 2010).

- **Europa**

ENISA (European Network Information Security Agency). Agencia nacional de Seguridad de la Información y Redes Europea. (Enisa, 2016).

El Centro Nacional de Excelencia en Ciberseguridad (CNEC) es un proyecto europeo en el que participa la Universidad Autónoma de Madrid, centro que está integrado en el Instituto de Ciencias Forenses y de la Ciberseguridad, aportando inteligencia, investigación, y tecnología para luchar contra la delincuencia en la red. (Centro Nacional de Excelencia en Ciberseguridad, 2016)

Centro Europeo contra el Cibercrimen de la Europol (EC3). Ubicado en La Haya (Países Bajos), el EC3 proporcionará soporte operacional a los países de la UE, dará acceso a experiencia técnica en las investigaciones conjuntas y fomentará la puesta en común de los recursos para ayudar en la prevención del cibercrimen y en el enjuiciamiento de los delincuentes. La actividad del EC3 pondrá especial foco en aquellos ciberdelincuentes que centran su actividad en delitos financieros y de banca online. Asimismo, la explotación sexual de menores a través de Internet y ataques dirigidos contra sistemas de información e infraestructuras también serán áreas prioritarias de investigación en este centro. (Europol, 2016)

International Cyber Security Protection Alliance (ICSPA), estará dirigido por Europol, su partner estratégico, y en él analizará las tendencias actuales en materia de cibercrimen y cómo ésta puede evolucionar en los próximos ocho años y más adelante. (ICSPA, 2014).

INCIBE. Instituto Nacional de Ciberseguridad. (INCIBE. Instituto Nacional de Ciberseguridad, s.f.) El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Energía, Turismo y Agenda Digital (MINETAD) a través de la Secretaría de Estado y para la Sociedad de la Información y Agenda Digital (SESIAD), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la Ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la Ciberseguridad a nivel nacional e internacional.

- **Estados Unidos**

CTIIC (*Cyber Threat Intelligence Integration Center*, traducido "Centro de Integración de Inteligencia contra la Amenaza Cibernética"). Su misión: coordinar las actuaciones de las distintas Agencias ante un ataque cibernético. (Office of the Director or National Intelligence, 2016)

Desde principios de los años noventa, se inician las unidades especializadas que investigan la ciberdelincuencia en diferentes países y han sido evolucionando desde entonces, dado que el delito cibernético y otros tipos de delitos, las pruebas crecen exponencialmente, cabe esperar que más países establezcan tales unidades y que su tamaño y alcance de trabajo aumenten en el futuro.

A continuación de presentan tres enfoques adoptados por los fiscales de varios estados de los Estados Unidos para crear capacidad para combatir el cibercrimen, considerándose ejemplos de buenas prácticas. (Pisaríc, 2017)

Unidad Cibernética dedicada en Cyber Crime en Mississippi. (Pisaríc, 2017) Oficina con jurisdicción estatal, con poderes de detención y autoridad de Gran jurado para investigar y acusar. Fiscales del Departamento de Justicia a Nivel Federal pueden asumir casos en cualquier Corte en el Estado. Se establece una dependencia dedicada a la cibercriminalidad como responsable de cibercrimen, y tiene unos procesos autónomos, investigadores y forenses.

Esta Unidad consta de un abogado, tres investigadores y un examinador forense. Cuenta con un laboratorio forense de informática, que acepta casos para el análisis de todo el Estado. Un porcentaje de los casos son solicitudes de análisis forense de computadoras recibidas de la oficina de aplicación de la ley local, y la única razón para negar el servicio forense es, si forensemente (técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.) ha comenzado anteriormente en otra parte. El resto de casos son solicitudes de asistencia desde la oficina de un fiscal o la policía local.

Modelo estatal del grupo de trabajo del delito cibernético en Maine. (Pisaríc, 2017) El Departamento de Policía de Maine promovió la idea de formar una asociación contra el cibercrimen en 1999, como responsables de investigar la delincuencia informática.

Hacen parte de esta asociación tres investigadores y tres examinadores forenses de informática y dos abogados que brindan apoyo legal. Desde allí se coordina y realiza la luchas contra el crimen informático a través de investigaciones de todo el Estado; realizan exámenes forenses de computadoras; responden solicitud de asistencia de otros organismos encargados de hacer cumplir la ley, citan a proveedores de servicios de Internet; conducen programas de entrenamiento para las agencias policiales en la investigación de casos de Internet; conducen programas de internet seguro para el público en general. Cada agencia es responsable de los casos dentro de su propia jurisdicción, y está capacitada en técnicas de investigación de delitos cibernéticos. Esta asociación inicio con casos de personas desaparecidas y de delitos contra niños en internet.

New Hampshire - Modelo de Expertos Forenses Distribuidos / Procesamiento de Delito cibernético. Este modelo se estructuró para que los fiscales locales e investigadores manejen casos de cibercrimen. En 2003 se reunieron los tomadores de decisiones estatales en busca de desarrollar un plan para hacer frente a la ciberdelincuencia, obtener consenso y establecer un grupo de trabajo. Finalizada las mesas de trabajo se solicitó a los miembros que destacaran a un personal y realizaran una encuesta de necesidades. La implementación del plan significa que los examinadores forenses en el laboratorio de estado reciben y realizan imágenes forenses a diferentes dispositivos, realizan verificaciones, indexación, y almacenamiento de imágenes indexadas

en una red de almacenamiento, acceso remoto a máquinas forenses, y análisis de lectura sobre medios de comunicación. (Pisaríc, 2017)

- **Brasil**

Centro de Transparencia en América Latina que tendrá como principal función vigilar la actividad de criminales informáticos en las redes y garantizar una mayor protección de las operaciones informáticas. (Microsoft, 2016)

Centro Mundial Contra el Cibercrimen de Microsoft. Creado para combatir los daños económicos y materiales que generan los crímenes informáticos. Este centro tendrá 12 sedes en todo el mundo (Beijing, Berlín, Bogotá, Bruselas, Dublín, Edinboro (E.U.A.), Gurgaon (India), Hong Kong, Múnich, Singapur, Sídney y Washington, D.C.) y una estará en Bogotá. Este Centro tiene sus oficinas de Centrales en Redmond, en el estado de Washington (EUA). Las oficinas ubicadas en estos lugares permitirán a Microsoft identificar y analizar mejores situaciones de malware e infracciones contra la propiedad intelectual, así como compartir las mejores prácticas contra la delincuencia cibernética con los clientes y los socios de la industria a escala mundial. (Enter.co Enterprise, 2016).

- **Singapur**

IGCI. Centro Fusión Ciber está integrado en el Complejo Global para la Innovación de la Interpol (IGCI, en sus siglas en inglés), y que trabajará en coordinación con la central de la organización en Lyon (Francia) y la oficina regional de Buenos Aires. Este centro equipa a la policía del mundo con las herramientas y el conocimiento para atacar mejor las amenazas

criminales del siglo XXI, con unas instalaciones de investigación de última generación para la identificación de crímenes y criminales, entrenamiento innovador y apoyo de operaciones. (Interpol, s.f.).

- **Australia**

Global Prosecutors E-crime Network (GPEN), plataforma GPEN IAP que "permite a los fiscales de todo el mundo para compartir información y experiencias, estar al corriente de las novedades y acceder a las herramientas legales para su uso en procesos judiciales". (GPEN Global Prosecutors E-Crime Network, 2016).

AusCERT Equipo de Respuesta de Emergencia Informática de Australia. (AusCERT, 1993).

- **Inglaterra y Gales**

IAP. "Organización mundial de fiscales y la asociación entre GPEN e ICSPA que permite desarrollar relaciones constructivas con la industria TI y otras fuerzas y cuerpos de seguridad en el ámbito de la ciberdelincuencia" (IAP International Association of Prosecutors, s.f.)

GCSCC Centro Global de Capacidad sobre Seguridad Cibernética (Oxford). (OEA - BID, 2016). El Centro Mundial de Capacidad para la Seguridad Cibernética (GCSCC) es un importante centro internacional de investigación sobre el fomento de la capacidad cibernética

eficaz, promoviendo un aumento de la calidad y el impacto de las iniciativas de creación de capacidad cibernética en todo el mundo. Ha creado un modelo único para medir la madurez de la capacidad de Ciberseguridad en cinco áreas que tiene como objetivo permitir que las naciones se autoevalúen, hagan referencia, planifiquen mejor las inversiones y las estrategias nacionales de seguridad cibernética y establezcan prioridades para el desarrollo de la capacidad.

Trabajando con actores clave de toda la comunidad internacional, el Centro ha comenzado a aplicar con éxito el modelo a nivel mundial, junto con socios como el Banco Mundial, la Organización de Estados Americanos y la Organización de Telecomunicaciones del Commonwealth. El primer informe publicado como resultado de este trabajo se puso en marcha en junio de 2015 en Kosovo.

El Centro también está desarrollando un modelo holístico y robusto para comprender el daño que sufren las naciones como resultado de la falta de capacidad y cómo se puede reducir esto. En conjunto, estos modelos complementarios proporcionarán a las naciones un marco integral para tomar decisiones mejor informadas para optimizar la planificación, evitar la duplicación y permitir inversiones mejoradas en la creación de capacidad. (Global Cyber Security Capacity Centre, 2017)

- **Estonia**

Centro de Excelencia OTAN de Ciberdefensa Cooperativa: se encarga de la investigación y formación en ciberguerra con personal experto de los diez países que lo patrocinan (Estonia como país anfitrión, Alemania, Eslovaquia, España, EEUU, Hungría, Italia, Letonia, Lituania y Turquía). Su misión es mejorar la capacidad y cooperación de la OTAN y sus Estados miembros

en Ciberdefensa mediante el desarrollo de programas y proyectos de I+D+i, formación, análisis de casos reales y consulta. (Ministerio de Defensa, 2011)

- **Colombia**

ColCERT. Grupo de Respuestas a emergencias Cibernéticas de Colombia. Dependencia del Ministerio de Defensa encargado de coordinar la respuesta del país a incidentes de seguridad que afecten su funcionamiento. (colCERT, 2013)

CCP - Centro Cibernético Policial. El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos. Investiga tres grandes grupos. Fraudes electrónicos y lo relacionado con la protección de datos; Ciberterrorismo y pornografía infantil. (Ministerio de Defensa Nacional - Policia Nacional de Colombia, s.f.)

CSIRT PONAL. Equipo de Respuesta a incidentes de seguridad informática. Hace parte del Centro Cibernético Policial CCP, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática de la Policía Nacional, con el fin de proteger su infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. (Policia Nacional de Colombia, 2015)

CCP. Comando Conjunto Cibernético de las Fuerzas Militares. Dependencia adscrita al Comando de las Fuerzas Militares, encargada de coordinar la respuesta a incidentes de seguridad que afecten la seguridad nacional. (Comando Conjunto Fuerzas Militares, s.f.) (Departamento Nacional de Política Económica y Social, 2011).

Ahora, teniendo en cuenta la relación de algunas unidades nacionales e internacionales que trabajan desde diferentes enfoques o alcance el fenómeno del cibercrimen, se evidencia la ausencia de unidades especializadas en entidades que ejercen la acción penal que agrupen, consoliden, recolecten y analicen información sobre hechos ciberdelictivos que afectan la seguridad y convivencia ciudadana en un territorio, que generen análisis confiables y prospectiva, permitiendo retroalimentar el proceso de formulación y evaluación de políticas que buscan prevenir, atacar y judicializar eventos asociados a delitos en el ciberespacio. (MinTIC, 2016) (Eltiempo.com, 2016).

5.1.2 Antecedentes en la Fiscalía General de la Nación

La Fiscalía General de la Nación cuenta con la misión de ejercer la acción penal y participar en el diseño de la política criminal del Estado; y de forma específica cuenta con las unidades investigativas de:

i. Delitos Informáticos de la Dirección Nacional de Investigación CTI y de la Dirección Nacional de Seccionales y Seguridad Ciudadana que tienen por competencia, conocer investigaciones y casos adelantados por la ley 1273 de 2009.

ii. Informática Forense de la Dirección Nacional de Investigación - CTI, área de Criminalística, cuya misión es realizar los análisis forenses a la información almacenada en redes y medios de almacenamiento digital involucrados en la comisión de delitos, en apoyo a las investigaciones conforme a los requerimientos procedentes de autoridades judiciales y policía judicial, recolección, adquisición de evidencia digital y adquisición de imagen forense.

iii. Eje Temático de Cibercriminalidad, Protección de la información, de los datos y de los sistemas informáticos adscrito a esta dirección que fue creado a partir de resolución 571 de febrero de 2016 y conoce exclusivamente de casos asignados especialmente por el Fiscal General de la Nación o por recomendación del Comité Nacional de Priorización. (Presidencia de la República de Colombia, Decreto 016 de 2014)

En este entendido, la Entidad cuenta con dos Grupos especializados en la investigación de delitos informáticos conformados por funcionarios con funciones de policía judicial, y un Eje temático de Cibercriminalidad, Protección de la información, de los datos y de los sistemas informáticos conformado por fiscales, que priorizan casos de connotación provenientes de las diferentes unidades nacionales.

Es de mencionar que internamente no existe un único repositorio de información, los casos de investigación son de alcance al fiscal que los lleva, carencia de asociación de casos, y falta de comunicación efectiva de información, investigación de caso a caso. De ahí la necesidad de buscar mecanismos que posibiliten la articulación, producción, tratamiento, asociación, interpretación y análisis de los datos e información sobre el cibercrimen, aumentando la capacidad de detección, investigación y alertas tempranas de nuevas amenazas, así como diseñando y definiendo estrategias de prevención, control y judicialización del delito.

Razones por las cuales se proyecta el fortalecimiento y articulación de capacidades misionales frente la investigación penal en el ciberespacio, considerando un resultado de coordinación entre las diversas sectores internos y externos a la Entidad, que sean fuente de información para el cumplimiento de la misión institucional, ejercer la acción penal y participar en el diseño de la política criminal del Estado.

> Con el objetivo de fundamentar la necesidad del fortalecimiento y articulación de capacidades de análisis, investigación y prospectiva de cibercrimen para la Fiscalía General de la Nación, se presenta el diagnóstico al interior de la Entidad en el año 2013, basado en la incidencia de los delitos informáticos en el país y las constantes denuncias de usuarios de la red y la banca, se buscó fotografiar en ese momento el estado de la delincuencia informática en Colombia. Análisis que se realizó en conjunto con la Dirección Nacional de Seccionales y Seguridad Ciudadana y la oficina del Vicefiscal General de la Nación. (Fiscalia General de la Nación, 2013, págs. 13,14).
>
> Tal diagnostico determinó que los tres delitos más denunciados entre el 2009 y el 2015 estaban relacionados con el Hurto por medios Informáticos, Acceso abusivo a un sistema informático y la violación de datos personales; delitos que concentran el 70% de las denuncias. Finalmente, se encontró que el 92% de los casos aún se encontraban en etapa de indagación y menos del 1% en etapa de ejecución de penas. (Fiscalia General de la Nación, 2013, págs. 20,21).

Con vista, en lo anterior, se tomó la decisión de implementar un plan de dos fases que consistía en la priorización de casos relacionados con la delincuencia informática y el fortalecimiento técnico y jurídico de los funcionarios que adelantaban las investigaciones. En lo

relacionado con el área de capacitación y fortalecimiento técnico, se inició un plan de capacitación a funcionarios en técnicas y herramientas informáticas forenses a los funcionarios del CTI en las seccionales y nivel central. Se celebró el primer simposio nacional sobre delitos informáticos en el cual se capacitó a 150 funcionarios a nivel nacional en la investigación de ciberdelitos en el área jurídica y tecnológica. Igualmente se aprobó el plan de instrucción de 10 servidores de policía judicial que se certificarán como peritos internacionales en las áreas de análisis de malware y forense de redes.

Finalmente, se fortalecieron los grupos de investigación con la contratación de investigadores de CTI con experiencia en áreas con falencias en la Fiscalía; tal como programación y el conocimiento de las plataformas SCADA y S400 para el control de estructuras críticas y transacciones financieras.

Desde el punto de vista de la priorización, se plantearon seis líneas de trabajo regional (Bogotá, Valle, Antioquia, Bolívar, Tolima y Norte de Santander). En estas se seleccionaron 60 casos que correspondían a los delitos de más alto crecimiento (Hurto por medios informáticos y acceso abusivo a sistema informático), eran cometidos por estructuras criminales organizadas y en las cuales la víctima era el sector bancario. Donde se hizo énfasis en la estrategia, llegar solo a los expertos informáticos de cada organización y no a los eslabones últimos de la cadena delictiva, lo que permitió una desarticulación efectiva de estructura criminal. Al finalizar el 2015 se desarticulo con éxito 15 estructuras, de las cuales 3 eran de especial connotación por su actividad a nivel nacional. (Información Congreso Asobancaria Vicefiscalia, 2013)

El diagnóstico realizado en la Entidad sobre los delitos informáticos más denunciados penalmente tuvo un alcance de seis años, donde se realizó recolección de información en las diferentes unidades de delitos informáticos en las seccionales de las investigaciones en curso,

tratamientos de datos, análisis de información, se generaron tendencias, que permitieron priorizar investigaciones y necesidades, arrojando como resultado casos de éxito. Tema para determinar que sí este ejercicio se realiza periódicamente y de manera continua se logran avances significativos en la misión de la Fiscalía General de la Nación, entre ellos generar productos como, alertas tempranas, cultura de seguridad e investigación inteligente, capacidad de respuestas a fenómenos actuales, capacitaciones especializadas y prospectiva del cibercrimen, todo ello realizado en cooperación y articulación con unidades homologas nacionales e internacionales.

Finalmente, la meta es mantener "una Entidad informada sobre análisis y prospectiva de amenazas en cibercrimen, actualizada en el tiempo con las habilidades necesarias para entender, administrar, investigar, evaluar el comportamiento y delitos en el ciberespacio, de manera jurídica, técnica y social, económica" (Conpes 3854 - Seguridad Digital, 2016, pág. 42).

6. Metodología

La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la indagación. Y responde al "cómo" se realizará el estudio para responder al problema planteado. Sobre el tipo de investigación, Canales (1996) señala: "Hay diferentes tipos de investigación, los cuales se clasifican según distintos criterios (...)" (p. 53). Citado de (Arias, 1999)

6.1 Nivel de Investigación

El nivel de investigación se refiere al grado de profundidad con que se aborda un objeto o fenómeno, en las cuales se incluyen la investigación exploratoria, descriptiva o explicativa. En este caso en particular se desarrolló una investigación descriptiva y explicativa, la primera en la caracterización del fenómeno del cibercrimen, la actualidad del proceso investigativo en el ciberespacio, y explicativa donde se propuso definir el por qué la necesidad de crear capacidades especializada en la investigación penal en el cibercrimen.

6.2 Diseño de Investigación

La estrategia que se adoptó para responder al problema planteado se basó en:

- *Investigación Documental:* se basó en la obtención y análisis de datos y documentos digitales e impresos provenientes de fuentes abiertas y documentación de la Fiscalía General de la Nación. (Misión, visión, organigrama, funciones de los grupos relacionados con la investigación de penal en el ciberespacio.

- *Investigación de Campo:* se basó en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna. Ejemplo: se realizó entrevistas y encuestas a personal de la Fiscala General de la Nación (investigadores y fiscales) relacionados con la investigación de penal en el ciberespacio.

Para realizar la propuesta de solución al problema de investigación se realizaron los siguientes procesos, iniciando con la elaboración de una encuesta diseñada para ser diligenciada por investigadores de los grupos asignados a los delitos informáticos, así como se contó con los recursos de personal/ participantes, materiales e instrumentos y procedimientos.

Nombre de la encuesta: Cibercrimen en la FGN - Percepción del cibercrimen en La FGN

Responsable encuesta: Rosangela López Álvarez

Fecha de recolección de la información de campo: 4 de mayo al 29 de julio 2016.

Marco muestral: Personal del grupo Delitos Informáticos, Informática Forense, Eje de Cibercriminalidad, Apoyo Jurídico y Gestión Contractual.

Ciudades donde se realizó: Nivel Central y Dirección Seccionales.

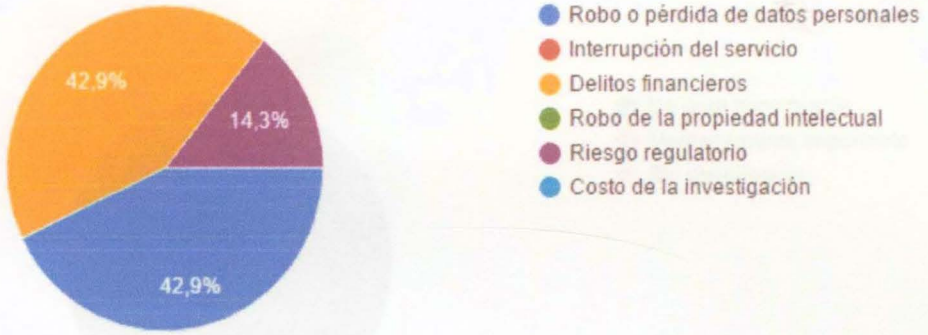
Tamaño de la muestra: 100 encuestas.

Técnica de recolección: Cuestionario estructurado vía web.

Fecha del reporte: 02 de agosto de 2016.

6.3 Desarrollo de la Encuesta

1. ¿Cuáles son las preocupaciones en torno al cibercrimen en la investigación penal?



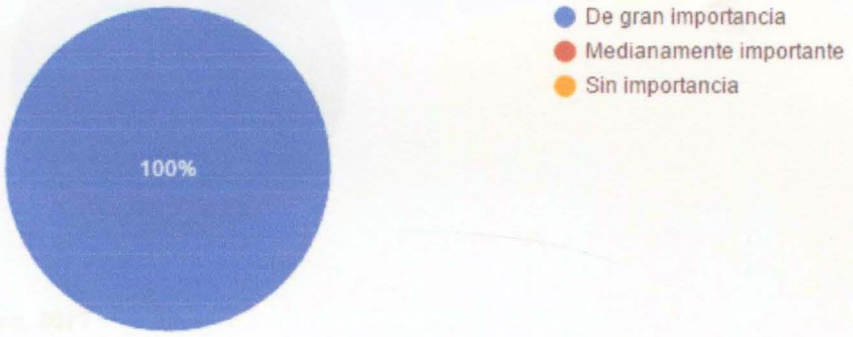
Fuente: Elaboración propia, 2017

Gráfica 1. Preocupaciones en torno al cibercrimen

Análisis

El resultado de la pregunta No. 1, nos indica que 42, 9% de los funcionarios encuestados consideran que la preocupación en torno al cibercrimen en la investigación penal se enfoca en los delitos financieros y en el robo o pérdida de datos personales; el 14.3% se enfoca en el riesgo regulatorio.

2. ¿Qué consideración tiene para usted la cooperación internacional frente a la investigación de delitos cibernéticos?



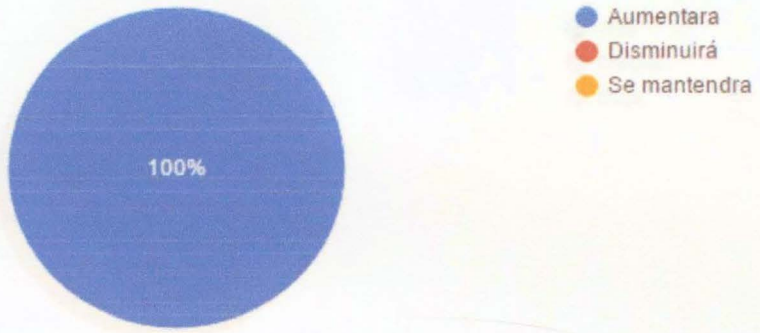
Fuente: Elaboración propia, 2017

Gráfica 2. La cooperación internacional frente a la investigación de delitos cibernéticos

Análisis

El resultado de la pregunta No. 2, nos indica que 100% de los funcionarios encuestados consideran que la cooperación internacional es de gran importancia en la investigación de delitos cibernéticos.

3. Percepción de los riesgos del cibercrimen en los próximos doce meses



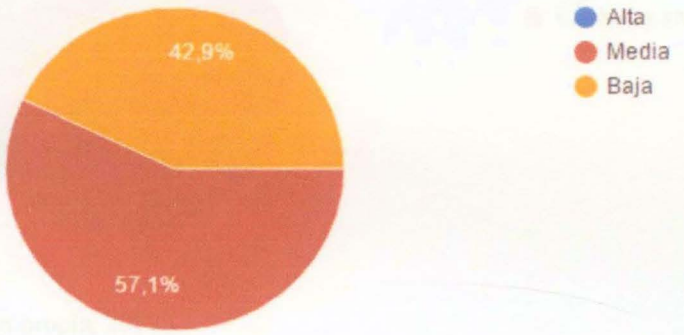
Fuente: Elaboración propia, 2017

Gráfica 3. Percepción del cibercrimen en los 12 meses

Análisis

El resultado de la pregunta No. 3, nos indica que 100% de los funcionarios encuestados consideran que la percepción de los riesgos del cibercrimen en los próximos doce meses aumentara.

4. Percepción de la capacidad de respuesta de la FGN ante la presencia y evolución de nuevos fenómenos del cibercrimen.



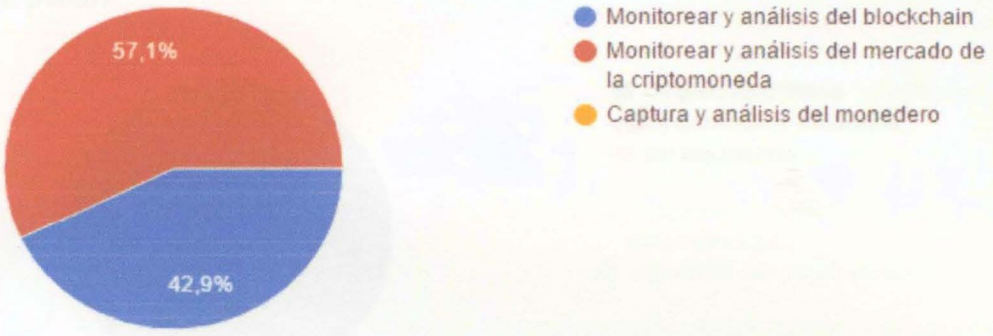
Fuente: Elaboración propia, 2017

Gráfica 4. Percepción de la capacidad de respuesta de la FNG

Análisis

El resultado de la pregunta No. 4, nos indica que el 57,1% de los funcionarios encuestados consideran la capacidad de respuesta de la FGN ante la presencia y evolución de nuevos fenómenos del cibercrimen es baja; el 42,9% que es media.

5. Entre las mejores técnicas investigativas para rastrear bitcoin se encuentra:



Fuente: Elaboración propia, 2017

Gráfica 5. Técnicas investigativas para rastrear Bitcoin

Análisis

El resultado de la pregunta No. 5, nos indica que el 57,1% de los funcionarios encuestados consideran que entre las mejores técnicas investigativas para rastrear el bitcoin se encuentra, monitorear y analizar el mercado de la criptomoneda; el 42,9% considera que es monitorear y analizar el blockchain.

6. ¿Cuál cree usted que sería el aporte del análisis y la prospectiva del cibercrimen en la investigación penal?

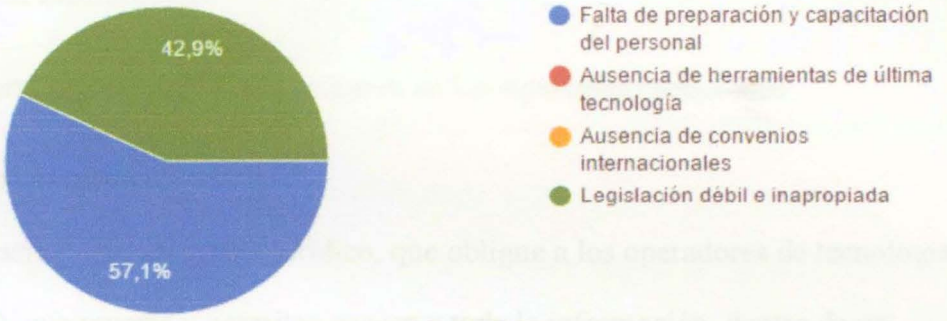
Fuente: Elaboración propia, 2017

Gráfica 6. Aporte del análisis y la prospectiva del cibercrimen

Análisis

El resultado de la pregunta No. 6, nos indica que el 100% de los funcionarios encuestados consideran que el aporte del análisis y la prospectiva del cibercrimen, es de gran importancia en la investigación penal.

7. ¿Cuál cree que es la mayor debilidad con que cuenta la Entidad frente las investigaciones de delitos informáticos o cibernéticos?



Fuente: Elaboración propia, 2017

Gráfica 7. Mayor debilidad de la entidad en los delitos informáticos

Análisis

El resultado de la pregunta No. 7, nos indica que el 57,1% de los funcionarios encuestados consideran que la mayor debilidad con que cuenta la Entidad frente las investigaciones de delitos informáticos o cibernéticos es la falta de preparación y capacitación del personal. El 42,9% la legislación débil o inapropiada.

8. ¿Cuál sería su opinión para fortalecer las capacidades actuales con que cuenta la Fiscalía General de la Nación para estar preparada para abordar los nuevos fenómenos investigativos del cibercrimen?

De manera general las respuestas se agruparon en las siguientes precisiones:

- Crear convenios internacionales
- Fortalecer la legislación, con un marco jurídico, que obligue a los operadores de tecnología (bienes y servicios), que reporte y permitan acceso a toda la información, dentro de un contexto legal.
- Se deben adquirir más y mejores herramientas, de igual manera se debe capacitar y preparar al personal con el fin de estar preparado para realizar las investigaciones de los últimos fenómenos del cibercrimen; se debe evitar la rotación del personal en estas áreas.
- Las unidades investigativas deben tener un componente de análisis.

7. Propuesta de Solución a la Problemática Planteada

7.1 Capacidades Necesarias de Ciberseguridad en el Desarrollo de la Investigación Penal en el Ciberespacio.

Los modelos de construcción de capacidades son definidos como aproximaciones conceptuales que se enfocan en comprender los obstáculos, posibilitando a las personas, gobiernos u organizaciones realizar sus objetivos de desarrollo a la vez que mejoran y potencializan las habilidades y recursos que les permiten alcanzar resultados medibles y sostenibles. (Certsi - Cert de Seguridad e Industria, 2016).

La Constitución Política de Colombia en el artículo 250, define que la Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo, es decir impone al denunciante una carga informativa que permita inferir razonablemente que el hecho denunciado efectivamente existió, compromiso de rodear de credibilidad su declaración de conocimiento y de aportar información, no pruebas, que permitan construir una hipótesis de investigación. (Corte Constitucional Republica de Colombia, Sentencia C-1177/05, M.P. Jaime Córdoba Triviño, 2005)

Así mismo, la entidad en su labor misional, apoya la implementación de las políticas de gobierno relacionado con el desarrollo económico y social del país - CONPES. (Consejo Nacional de Política Economica y Social, CONPES, 2016). Para este documento su enfoque está en la Política de Ciberseguridad y Ciberdefensa (Conpes 3701) y la Política Nacional de

Seguridad Digital (Conpes 3854), donde la Fiscalía General de Nación tiene la responsabilidad de realizar la investigación penal y realizar recomendaciones en política criminal sobre la delincuencia cibernética, encaminados a construir un marco jurídico maduro que apoye los procesos judiciales, juzguen conductas de manera efectiva, apoyen procesos de investigación estructural, y cuente con la capacidad de adaptarse dinámicamente en función de las circunstancias imperantes. (Departamento Nacional de Planeación, 2016) (Departamento Nacional de Planeación, 2011).

Se suma a lo anterior el Plan Estratégico 2016 – 2020 de la Fiscalía General de la Nación, el cual contempla los siguientes objetivos estratégicos (Fiscalia General de la Nación, 2016):

1. Impactar de forma contundente el crimen organizado
2. Impactar la corrupción de mayor impacto
3. Combatir la violencia como fenómeno priorizado
4. Contribuir al fin del conflicto armado sin impunidad
5. Mejorar el acceso a la justicia
6. Fortalecer la acción penal en el territorio
7. Consolidar políticas de manejo estratégico de la carga de trabajo
8. Gestionar y optimizar los recursos financieros
9. Fortalecer la infraestructura tecnológica
10. Optimizar los procesos y fortalecer el Sistema de Gestión Integral
11. Desarrollar el talento humano

La investigación y el ejercicio de la acción penal están focalizadas en el crimen organizado y sus economías ilegales, la corrupción de mayor impacto, la violencia homicida y la contribución

al fin del conflicto armado sin impunidad. También se concentran esfuerzos en garantizar un mejor servicio a la ciudadanía, una mejor atención a las víctimas y aumento de presencia de la entidad. Todo esto, a partir de la consolidación de políticas para el manejo estratégico (priorización de casos) de la carga de trabajo, el fortalecimiento de la infraestructura tecnológica, la optimización de los procesos internos de la Fiscalía General de la Nación, el fortalecimiento del sistema de gestión integral y el buen desarrollo del talento humano.

Ahora, en desarrollo de impactar los objetivos estratégicos números 1, 6, 9 y 11 para combatir esta forma creciente de criminalidad (delincuencia cibernética), se necesita una comprensión detallada del fenómeno del cibercrimen, donde se considere intervinientes, beneficios, atractivos entre otros. Esto a partir de la compresión de que los delitos cibernéticos comportan importantes cuestiones de procedimiento y novedad (moderna tecnología, conocimiento especializado, mayor globalización). (N. Kshetri, s.f.).

En atención al rol que cumplen los jueces, fiscales, investigadores y analistas en el proceso judicial en torno a casos relacionados con el cibercrimen, no son suficientes las competencias técnicas de estas instancias a la fecha, (Organización of American States - BID, 2016), a pesar de los desarrollos normativos en la materia, se requiere la revisión y mejoramiento de cada una de las instancias judiciales, así como de las sanciones administrativas y disciplinarias sobre la comisión o prevención de un delito informático.

Es así, entonces que la Fiscalía enfoca su misionalidad en realizar investigaciones penales de conductas punibles que atenten contra el bien jurídico de la "protección de la información y de los datos" de que trata el Titulo VII BIS, Capítulos Primero y Segundo de la Ley 599 de 2000 y los delitos conexos y la Ley 1273 de 2009 tipos penales relacionados con móviles informáticos.

Estas investigaciones comprometen nuevas capacidades investigativas, consistentes en ampliar las destrezas y habilidades de fiscales y policía judicial para ejercer sus funciones acorde con este fenómeno, siendo indispensable capacitarlos en la materia y así, facilitar la comprensión respecto del ámbito de aplicación de la comisión de dichas conductas, y la posibilidad de fortalecer las herramientas jurídicas para encuadrar la conducta del delito informático dentro del Código penal, igualmente considerando el alcance globalizado de este fenómeno contar instrumentos de intercambio de información que permitan respuestas instantáneas y resultados tangibles por y para las partes interesadas en todo el mundo. (Consejo Nacional de Política Economica y Social, CONPES, 2016) (Organización of American States - BID, 2016)

Lo anterior, traería consigo que fiscales, investigadores y analistas conozcan las afectaciones a la seguridad digital y la comisión en contexto de delitos cibernéticos, avanzando de manera más efectiva en la investigación de estas conductas. En ese orden de ideas, la capacitación, análisis, compresión y cooperación internacional del cibercrimen son fundamentales y contribuyen a una mejora en la judicialización de este tipo de conductas. (Consejo Nacional de Política Economica y Social, CONPES, 2016)

Luego de realizar un diagnóstico interno al marco jurídico y organizacional de la Institución (Fiscalia General de la Nación, 2017), así como los resultados de la encuesta realizada a investigadores y analistas donde concluyen:

- Que la cooperación internacional es de gran importancia a la hora de investigar delitos informáticos.
- Donde la percepción de los riesgos asociados al cibercrimen es que aumentaran.

- Donde la percepción de la capacidad investigativa de la Fiscalía General de la Nación ante el cibercrimen oscila entre media y baja.
- Donde se reconoce que el análisis y la prospectiva son de gran importancia en la investigación penal del cibercrimen.
- Donde se percibe que las mayores debilidades frente a la investigación penal del cibercrimen se centra en la ausencia de capacitación del personal y la inapropiada legislación.

Ahora, teniendo en cuenta los anteriores resultados se proponen factores que consolidados son la base para el desarrollo de las capacidades propuestas (capacitación, investigación, análisis, compresión y cooperación internacional del cibercrimen) como son:

i) **segmentación y fragmentación** de la información, debe contarse con la unificación y concentración de la información originada, procesada y administrada por las diferentes unidades nacionales de los grupos investigativos de delitos informáticos, informática forense, así como los grupos de las policías Judiciales Especializadas que abordan el cibercrimen. Esto tendrá un alto impacto en la alimentación de bases de datos institucionales, en la configuración de estrategias de acceso a datos, uniformidad de información, abordaje por fenómeno y no por caso, dando como resultado la posibilidad de realizar minería de datos, análisis en contexto y judicializaciones efectivas.

ii) Nivel insuficiente de **Conocimiento y formación** orientados a mejorar las capacidades y competencias específicas de los actores que intervienen en un proceso de investigación penal, (Fiscales, Policía Judicial) a través de la construcción de una base de conocimientos y la sensibilización en materia de cibercrimen como una prioridad en la Institución, lo anterior fundamentado en que la capacitación sobre delitos cibernéticos y nuevos modus operandis es el

mayor de los obstáculos que encuentra la justicia a la hora de dar respuesta a las víctimas. (Asociación Argentina de Lucha Contra el Cibercrimen AALCC, 2015)

Parte del problema con respecto a la escasez de preparación en la investigación penal se deriva de la falta de infraestructura educativa, formación enfocada a fortalecer los conocimientos, técnicas y habilidades en los operadores de justicia en la identificación, investigación y persecución penal de estos delitos, desarrollando temáticas como análisis forense digital, fuentes de evidencias, ocultamiento y destrucción de información, incautación y análisis de dispositivos móviles y monederos electrónicos, así como conocer los fundamentos legales para el manejo y la incorporación de la prueba en el proceso penal y en la protección de los derechos de las víctimas. (Fiscalia General de la Republica - Escuela de Capacitación Fiscal, 2016), esto en búsqueda del objetivo de contar con la capacidad de realizar las diligencias de investigación, actos urgentes de comprobación y pruebas periciales idóneas para la determinación de la existencia del delito y de la participación en ellos.

Frente este panorama pocos países ofrecen programas de educación a nivel de posgrado, hay mayor oferta en programas de formación profesional. También debe mencionarse los incentivos para la formación y la educación en la región. Hay ofertas destinadas a educación y formación en seguridad de la información. Se ofrecen cursos sobre seguridad cibernética en las universidades, los cuales otorgan títulos de grado y maestría, como la maestría en Ciberseguridad y Ciberseguridad en Colombia. Universidades de la región de América Latina y el Caribe están solicitando acreditación en los cursos de seguridad cibernética, por ejemplo en Bolivia, Brasil, Colombia, Panamá, Perú, entre otros. (Organización of American States - BID, 2016)

iii) Intercambio de información con organismos homólogos y especialistas en este campo. Es esencial fomentar el desarrollo de mecanismos de **cooperación e intercambio de información** a

nivel de nacional e internacional, sobre base de un esfuerzo multisectorial, dada la naturaleza sin frontera de los delitos cibernéticos, y la necesidad de la armonización de los marcos legales. (Organización of American States - BID, 2016)

Los delitos cibernéticos han desafiado la jurisdicción territorial y, por lo tanto, no es una necesidad de un país sino global, subrayando aún más la carga que supone la cooperación. Más allá de las preocupaciones técnicas de la mala atribución de los atacantes y las dificultades de la evidencia digital, algunos de los principales obstáculos legales internacionales incluyen la falta de reglas procesales requeridas, determinar la jurisdicción y encontrar medios efectivos de comunicación. Por otra parte, puede presentarse que un incidente cibernético no es siempre reconocido como un crimen en la nación víctima sino por la nación de la que se originó el ataque. Por lo tanto, debería realizarse un examen exhaustivo de las leyes sustantivas y procesales a nivel nacional e internacional al país que se va a solicitar ayuda antes para que la cooperación internacional puede ser eficaz, o incluso posible. (Talihärm, s.f.)

De manera concluyente, teniendo en cuenta la naturaleza sofisticada y el impacto del cibercrimen sobre el delito convencional (N. Kshetri, s.f.), así como el diagnostico interno de la entidad frente a factores a fortalecer, se presenta la propuesta de capacidades misionales necesarias para abordar de manera actualizada investigaciones penales de delitos cibernéticos, impactando de forma contundente el crimen organizado, con una entidad informada y actualizada en el tiempo.

Dado lo anterior se detallan ***capacidades misionales*** propuestas:

- Análisis y diagnóstico
- Formación y educación
- Cooperación Nacional e internacional

i) **La capacidad de análisis y diagnóstico** hace referencia a contar con los medios necesarios para desarrollar análisis, consistente en identificar y contextualizar fenómenos del cibercrimen, desarrollar conceptos basado en la compresión de los mismos, así como establecer los mínimos de comportamiento de un hecho delictivo. Lo cual debe permitir conocer el antes, el ahora y el posible futuro de delitos en el ciberespacio, así como evidenciar las potencialidades necesarias para afrontarlos.

Lo anterior, implica fuentes de información abierta e interna, desde la web hasta procesos y expedientes judiciales de las investigaciones penales que adelanten los grupos investigativos. Esta capacidad busca lograr a través de los procesos de recolección, análisis y evaluación de información de estados de desconocidos a conocidos, donde las tipologías o manifestaciones del cibercrimen sean entendidas y los responsables de las mismas judicializados. (Chismon & Ruks, 2014)

El objetivo de esta capacidad suministrar información de calidad (compilada, analizada y procesada), así como determinar situaciones y hechos que permitan la orientación de los esfuerzos de los grupos investigativos de delitos informáticos, además de incorporar análisis de situaciones y prospectiva, que permitan establecer las necesidades de seguimiento y actuación de corto plazo, así como los requerimientos para profundizar en conductas y anomalías detectadas.

Para el desarrollo de este objetivo se propone informes con la siguiente periodicidad. (Blanco, 2015)

- **Informe Mensual:** Este informe deberá contener la evolución ejecutiva de fenómenos de interés para los grupos investigativos y fiscales adscritos a las secciones de delitos informáticos con alcance al mes anterior, evidenciando los principales hechos acontecidos, la evolución de las situaciones y casos observados, nuevos desarrollos, concepto y prospectiva

del analista sobre cada fenómeno o situación en particular. El informe deberá incluir indicadores, alertas, tendencias, perfilaciones y correlación de información comparada con el mes, el trimestre, el semestre y el año anterior, de tal manera que se obtenga de manera sencilla un seguimiento y comprensión de los principales indicadores obtenidos y analizados.

- **Informe trimestral:** Este informe deberá incorporar un análisis profundo de las situaciones analizadas y observadas durante el periodo inmediatamente anterior. A diferencia del producto anterior, este informe deberá profundizar en el análisis de las situaciones más preocupantes detectadas, así como un análisis de prospectiva que tome como insumos los análisis de Indicadores y alertas, las conclusiones y concepto de los analistas, suministrando información de carácter estratégico para la toma de decisiones en el corto y mediano plazo.
- **Informe Anual:** El informe anual es el medio por el cual se comunica la evolución y prospectiva de las situaciones y fenómenos consolidados durante el año anterior, las actividades de prevención y lucha realizadas para combatir los mismos, la eficiencia en el combate de los mismos y el impacto logrado mediante el uso de los informes y análisis estratégicos en la lucha contra el delito. Así mismo, deberá presentar la evolución de los Indicadores & Alertas durante el periodo, propuestas de priorización y otro tipo de actividades que se consideren esenciales para el desarrollo exitoso de los objetivos de la Dirección.
- **Propuesta de Iniciativa Investigativa:** En este informe el Analista(s) presentan a consideración las propuestas para el desarrollo de iniciativas investigativas que puedan derivar en casos, de acuerdo a la información obtenida, el procesamiento y el análisis de la situación o caso; presentando la hipótesis y la argumentación (sustentada en documentos,

análisis e información de soporte) que le permita a los coordinadores de los grupos de delitos informáticos determinar el desarrollo de la citada iniciativa.

- **Informes de Coyuntura**: Estos informes buscan comunicar de manera eficiente, el desarrollo de situaciones o hechos que requieran de la atención de manera urgente, facilitando la preparación de los grupos investigativos y fiscales para enfrentar hechos o situaciones coyunturales, con información analizada y procesada adecuadamente, facilitando el desarrollo de cursos de acción y actuaciones de la Dirección.

ii) **Capacidad de Cooperación Nacional e internacional.** La naturaleza sin fronteras y cada vez más sofisticada de la ciberdelincuencia requiere respuestas instantáneas y con resultados tangibles por y para las partes interesadas en todo el mundo, entre ellas, las Agencias de aplicación de la Ley, Organizaciones internacionales, Equipos de respuesta de emergencia y proveedores de Internet. Por lo tanto, el papel de la cooperación internacional penal en el contexto de los incidentes cibernéticos es crucial. El ciberespacio ha desafiado el principio fundamental de la jurisdicción territorial y enfatiza por lo tanto aún más la carga de éxito transfronterizo en el principio de cooperación. (Talihärm, s.f.).

Esta capacidad se fundamenta en que la legislación interna, investigación y enjuiciamiento de incidentes cibernéticos rara vez requiere de un sólo país y la creciente gama de ejemplos de delitos cibernéticos subraya la importancia de una red global y la cooperación. (Talihärm, s.f.)

Los retos y las tendencias del cibercrimen apuntan a la necesidad global de investigación en red, conciencia sobre instrumentos internacionales para compartir información, así como orientación hacia la interpretación y aplicación adecuada de los mismos. Resaltando, que estas tendencias demuestran que una mejor coordinación entre las organizaciones internacionales y

una comprensión global de los instrumentos legales ya existentes, beneficiaria enormemente el estado actual de la cooperación penal internacional en el dominio cibernético. La cooperación internacional en materia penal se basa en tres pilares: (Talihärm, s.f.).

- Tratados o convenciones multilaterales
- Tratados bilaterales
- Reglamentos regionales o de organización.

Los acuerdos pueden incluir disposiciones relativas al procedimiento para la fabricación de solicitudes, las condiciones sobre el uso de la ayuda, así como los procedimientos para denegar la asistencia. Es de mencionar que entre las organizaciones internacionales que son instrumento de cooperación internacional en el cibercrimen se encuentran Naciones Unidas, el Consejo de Europa (COE) y la Unión Europea y la Oficina Europea de Policía (Europol).

iii) Conocimiento y formación. Esta capacidad compromete el desarrollo habilidades para sustentar los objetivos de la Ciberseguridad y la investigación penal en ciberespacio. Capacitación especializada a fiscales, policía judicial y analistas, en procura de alcanzar y mantener conocimientos que permitan la ejecución de la investigación penal.

En la investigación de los cibercrimen, es esencial entender tres aspectos fundamentales: motivación de los delincuentes; cómo se eligen las víctimas; y cuáles son los detalles del crimen. En el caso de los delitos informáticos, que técnicas comunes de investigación se modifican para permitir al investigador acercarse a la escena del crimen digital. Aspectos que serían las columnas de las capacitaciones propuestas. (Cloud Publications- International Journal of Advanced Computer Science and Information Technology, 2014).

Al hablar de esta capacidad y su fortalecimiento, la Entidad cuenta con la Dirección de altos estudios que es la encarga de la construcción y divulgación de programas educativos que apoyen el eficiente desarrollo del ejercicio de la acción penal, algunos programas cubiertos con personal interno, y otros con cooperación nacional e internacional, organismos con escuelas de formación como la Policía Nacional, Consejo Superior de la Judicatura, ICITAP, entre otras. Actualmente se viene desarrollando un curso denominado "cibercriminalidad" con alcance a fiscales, investigadores y funcionarios de otras entidades, en procura de construir conocimiento en legislación y de actuaciones de policía judicial frente a una investigación de un delito informático, así como generar redes para compartir capacidades interinstitucionales.

Con las anteriores capacidades la Institución debe ser capaz de conocer y comprender el concepto, desarrollo y las manifestaciones del cibercrimen, así como fortalecer sus propias investigaciones, diseñar y ejecutar política criminal de Estado que garantice el acceso efectivo a la justicia, la verdad y la reparación de las víctimas de los delitos, generando confianza en la ciudadanía. (Fiscalia General de la Nación, 2017), es decir:

- Debe existir entendimiento y comprensión de concepto y evolución de las amenazas, así como desarrollar una aproximación a las implicaciones a corto, mediano y largo plazo, logrando soluciones y estrategias que se basen en el conocimiento y el análisis de los datos (*Big Data*) (IBM, s.f.), para la oportuna toma de decisiones.
- Todas las investigaciones (proceso, resultados) que adelanta la Fiscalía General de la Nación deben ser evaluados y registrados de manera que aporten conocimiento en forma de lecciones aprendidas, en aras de alcanzar un nivel de comprensión de los hechos denunciados.

- Debe haber una gestión y aplicación de instrumentos nacionales e internacionales de cooperación que permita la obtención de pruebas en el contexto transnacional de manera técnica y jurídica que se pueden utilizar en la persecución e investigación cibernética.

Ahora, una vez identificadas y definidas las capacidades misionales mínimas requeridas en la investigación preliminar frente a conductas punibles en el ciberespacio, se deben asociar conceptos de seguridad de la información en aras de garantizar los objetivos misionales de la entidad y la continuidad del negocio.

7.2 Capacidades en Ciberseguridad

En este contexto, y en aras de lograr permanencia, continuidad y evolución de las capacidades misionales deben considerarse las capacidades de seguridad cibernética que abarcan el espectro de defensa de la plataforma, aplicativos y red que sustentan las capacidades misionales, protegiendo los activos necesarios para desarrollar la funcionalidad de la Entidad, y entre los más importantes la información y las personas, contemplando soluciones que incluyan aspectos organizativos, procedimentales y tecnológicos.

Desarrollando las capacidades esenciales en Ciberseguridad, se encuentra en primera instancia la conciencia situacional (percepción, compresión, proyección), definida como el nivel necesario de continuar mejorando y ser capaz de conocer, dinámicamente, el nivel de seguridad de los sistemas al alrededor posibilitando una utilización adecuada de los recursos y la aplicación de los principios de la gestión de riesgos mediante información de las amenazas y modelos probabilísticos obtenidos del análisis de los datos. (Pérez, 2013).

Es una representación mental y comprensión de los objetos, eventos, gente, estados de los sistemas, interacciones, condiciones ambientales y cualquier otro tipo de factores de una situación específica que puedan afectar al desarrollo de las tareas humanas, bien sean estáticas o dinámicas. "Saber lo que ocurre para poder disponer lo que debe hacer" (Endsley, 2000).

En segunda instancia, valoración dinámica del riesgo (ISO, CobiT, ISACA, ITIL), con base a la normatividad, tendencias, impacto y técnicas vigentes para ambientes de investigación penal a nivel nacional e internacional.

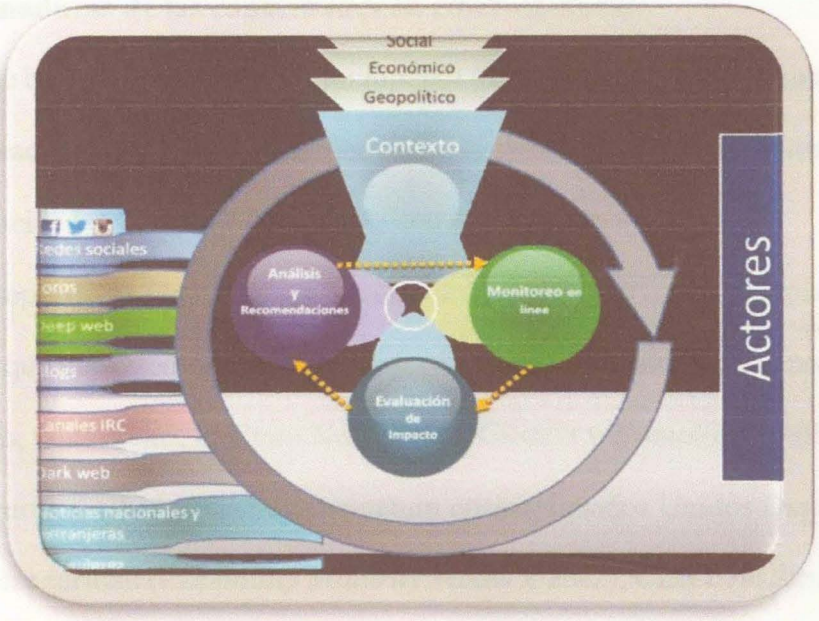
Las principales funciones asociadas a la gestión de la Ciberseguridad según el modelo de control propuesto por el Instituto Nacional de Estándares y Tecnología Norteamericano (NIST - National Institute of Standards and Technology, 2014), son identificar, proteger, detectar,

responder, recuperar. Si bien la seguridad no existe en un cien por ciento, pero sí es posible hacer las organizaciones más seguras. Para ello, la anticipación es clave. Hay que ir por delante de los ataques siendo capaces de detectarlos y prevenirlos. Además, se puede limitar de forma significativa el daño si se reacciona de forma rápida y decidida ante cualquier intento de comprometer el entorno. Todo esto requiere continuidad y constancia en la vigilancia. (NIST - National Institute of Standards and Technology, 2014)

En este sentido, las organizaciones deben realizar un análisis detallado de la exposición a estos riesgos, e implantar una estrategia de gestión ante los mismos, que comprometa los conceptos de Ciberseguridad y ciberresilencia. (NIST - National Institute of Standards and Technology, 2014)

Como tercera capacidad en Ciberseguridad se relaciona la ciberinteligencia (Universidad de Alcala de Henares - Madrid, 2016), proceso de adquisición y análisis de información de fuentes abiertas e institucionales para identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los ciberactores, ciberdelincuentes, y ofrecer cursos de acción con base en el contexto particular de la organización, que mejoren la toma de decisiones.

El proceso general que se sigue para la generación de ciberinteligencia consta de cinco pasos, identificación del objetivo o misión, recolección de información, análisis, identificación de hallazgos, todo esto para finalmente llegar a elementos que son relevantes y que ayudan a confirmar o rechazar las hipótesis planteadas, o que ayuden a responder las preguntas establecidas, finalmente la difusión, hacer conocer a las partes interesadas los resultados y cursos de acción propuestos.



Fuente: (Polanco, 2016).

Figura 1. Flujo de trabajo ciberinteligencia. (entradas-proceso-salidas)

Esta imagen describe el proceso general que se requiere para la generación de ciberinteligencia. Como son: determinación de objetivo (social, económico, geopolítico), definir y colección de fuentes de información a utilizar (redes sociales, bases de datos privadas, deep wep, etc), análisis de información (diversas técnicas y herramientas visuales), identificación de elementos relevantes, y por último difusión a los actores (socialización y cursos de acción propuestos).

7.3 Modelo de madurez de las capacidades en ciberseguridad

Finalmente, se hace necesario definir un modelo de madurez para determinar el nivel de desarrollo de capacidades en Ciberseguridad con que cuenta la Entidad, así como definir el nivel al cual cada capacidad debe llegar de acuerdo con la escala definida.

Frente este propósito se identifican diferentes modelos de madurez de capacidad de la Ciberseguridad, que permiten reforzar las capacidades de intercambio de conocimientos y mejores prácticas, tales como, Instituto Nacional de Ciencia y Tecnología (NIST), marco para la mejora de la seguridad cibernética infraestructura crítica, Estados Unidos Departamento de Energía de Ciberseguridad (*Capability Maturity Model* C2M2), CERT *resiliencia Modelo de gestión* (CERT RMM) del *Software Engineering Institute de Carnegie Mellon*, Metodología para desarrollar arquitecturas de seguridad centradas en los negocios, riesgos y oportunidades, tanto a nivel de empresa como de soluciones, que mediblemente apoyan los objetivos empresariales (SABSA).

En este caso el interés es evaluar y mejorar las capacidades de Ciberseguridad, por lo tanto, se considera que el modelo C2M2 es el adecuado, por lo que busca desarrollar un entendimiento y una medición lógica de las políticas, procesos y procedimientos involucrados en el desarrollo de la seguridad cibernética de una organización, centra su objetivo en apoyar el desarrollo y medición en curso de las capacidades de Ciberseguridad dentro de cualquier organización mediante:

- Fortalecimiento de las capacidades de las organizaciones en materia de Ciberseguridad;
- Permitir que las organizaciones evalúen de manera efectiva y consistente sus capacidades de Ciberseguridad;

- Compartir conocimientos, mejores prácticas y referencias relevantes entre las organizaciones como un medio para mejorar las capacidades de seguridad cibernética;
- Permitir a las organizaciones priorizar acciones e inversiones para mejorar la Ciberseguridad; y
- Apoyar la adopción del Marco de Seguridad Cibernética del Instituto Nacional de Estándares y Tecnología (NIST).

En resumen, se plantea una metodología que permite identificar las capacidades fundamentales para apoyar la investigación penal en el ciberespacio, apoyándose en capacidades de Ciberseguridad, y finalmente enmarcarlas en un proceso de evaluación para medir la madurez de las mismas.

7.4 Requerimientos Esenciales para la Conformación de un Centro de Analisis y Prospectiva de Cibercrimen Orientado al Desarrollo de la Investigación Penal en el Ciberespacio

Se propone un plan de trabajo general y algunos requerimientos indispensables que deben tenerse en cuenta en el proyecto de "Diseño de un Centro de Análisis, Investigación y Prospectiva de cibercrimen y prospectiva de cibercrimen", entre ellos la definición del perfil del personal, formación, equipamiento, organización y estructura interna.

7.4.1 Ubicación.

Se trata de una unidad especializada de policía judicial dentro de la FGN. El director del Centro de Análisis, Investigación y Prospectiva de cibercrimen debe tener el mismo nivel de un director de Departamento. Deberá depender del Fiscal General de la Nación como jefe máximo de las

policías judiciales, dependiente del Cuerpo Técnico de Investigación CTI. Desde esta ubicación organizacional deberá coordinarse con las policías judiciales de las diferentes Unidades Nacionales y Seccionales, así como con las otras policías judiciales.

7.4.2 Composición.

El Centro de Análisis, Investigación y Prospectiva de Cibercrimen estará compuesto por perfiles multidisciplinarios y se conformara por analistas e investigadores de policía judicial, con nivel académico e instrucción mínimo de especialización. Esto se requiere con el fin de garantizar la integración a las dinámicas relacionales con los actores y fenómenos en el ciberespacio de interés en el ámbito de una investigación caracterizados por fuertes tecnicismos.

La actuación exitosa de un Centro de Análisis, Investigación y Prospectiva de cibercrimen depende en gran medida de la calidad, determinación, motivación y liderazgo de su personal, cooperación y participación de todos los sectores internos y organismos homólogos en el sector público y privado, así como el relacionamiento y la cooperación con el sector académico e internacional.

1. **Personal:** (Pisaríc, 2017)

El Centro de Análisis, Investigación y Prospectiva de Cibercrimen, Investigación y Prospectiva estará compuesta por perfiles multidisciplinarios, que harán parte como investigadores de policía judicial y analistas, con nivel académico e instrucción mínimo especializado. Esto se hace necesario con el objetivo de facilitar que dicho personal se integre de

manera fácil y rápida a las dinámicas de los nuevos fenómenos relacionadas con el campo a investigar.

La selección del personal adecuado para realizar las funciones dentro del centro es fundamental. Por lo tanto, es importante tener un procedimiento de selección del personal que identifique los diferentes roles que deben funcionar en el centro. Se deben contemplar requisitos esenciales del personal para combatir el cibercrimen, que se ve reflejado en las funciones básicas de una unidad de cibercrimen como son: investigación, análisis, asistencia legislativa, educación y / o divulgación pública y capacitación.

Investigadores: Los investigadores son los responsables de realizar la investigación y la reconstrucción de los hechos de los delitos informáticos de manera general, son personas que tiene un entrenamiento general en cuestiones de informática forense, son profesionales en seguridad informática, y ciencias afines, son los primeros en llegar a la escena del crimen, encargados de recolectar las evidencias que ahí se encuentran.

Deben ser profesionales formados esencialmente para llevar a cabo análisis e investigaciones de delitos informáticos. Deberán tener amplios conocimientos y habilidades técnicas en el campo de la informática y afines, así como también conocimientos de derecho, sobre todo en derecho penal informático, y procesal penal. Dicho personal debe estar en constante aprendizaje y entrenamiento dado que la tecnología informática y las modalidades comisivas de esta clase de infracciones que están en constante cambio con el tiempo.

Los investigadores deben tener conocimiento de manera específica en computadoras, internet, policía judicial, legislación que rige el delito cibernético e idiomas extranjeros, en el manejo de evidencia y documentación, al igual que en reconstrucción del delito, y la localización de

elementos de convicción dentro de la red, en el momento de actuar como Técnicos en escenas del Crímenes Informáticos, o también llamados *First Respondenders* (Universidad UNIANDES, s.f.)

De igual manera dependiendo de su función, tienen cualificaciones específicas, la investigación penal y las TIC, y, dependiendo del tamaño del centro, su jurisdicción y tareas, el proceso de selección debe tener lugar dentro de un tiempo razonable y tener como criterio las aptitudes y la integridad de los candidatos.

De igual manera debe tenerse en cuenta la estructura de creación del centro, es decir los ejes o líneas de acción (pornografía infantil, ventas de bases de datos y productos bancarios, software malicioso, ollas virtuales, esquema ponzi Bitcoin, mercados criminales en línea (tráfico de drogas, asesinato por contrato, distribución de malware, lavado de dinero), fraude informáticos, ciberterrorismo), entre otras, lo que implica que además de tener conocimiento en tecnología y legislación, también se debe poseer conocimiento del eje o línea de manera específica.

Por ejemplo, si una de las líneas es analizar e investigar la pornografía infantil, el personal de análisis e investigación designado a esta área deberán tener conocimiento entre otros, en psicología y en investigaciones relacionadas con menores, mientras que los investigadores del eje de delitos contra la propiedad intelectual tendrán que poseer conocimientos de los derechos propiedad intelectual, secretos comerciales, así como sobre las investigaciones desarrolladas por la academia, y otros datos sensibles. De igual forma, los que investiguen sobre ataques a infraestructura crítica, deberán tener conocimiento sobre la infraestructura tecnológicas asociadas a servicios vitales para la sociedad, el sector público y privado. (FBI, 2017)

Ahora, en la definición de habilidades especializadas que se hacen necesarias para todas las investigaciones de cibercrimen se encuentran:

> Preparación de órdenes de captura de pruebas digitales; técnicas de entrevista e interrogatorio, así como determinar el origen y trazabilidad de evidencia digital; voluntad y capacidad para recibir información, formación especializada, certificaciones en especialidades, computadores, redes y análisis forense; preservación especializada de la escena del crimen y habilidades de examen; conocimiento práctico de Internet; capacidad de trabajar en equipo con entidades homologas. (National Center for Justice and the Rule of Law, 2007 p. 24)

De manera específica para las investigaciones encubiertas y proactivas requieren que el investigador considere la creación y el mantenimiento de un agente encubierto. Los investigadores deben estar familiarizados con diversas facetas de la cultura, el "lenguaje" utilizado en las diferentes aplicativas de chat y redes sociales. Finalmente, los investigadores deben estar familiarizados con la tipología de los delincuentes de Internet.

Fiscales. Los fiscales de cibercrimen son los que lideran las investigaciones en la acción penal. Deberán proponer y supervisar las operaciones del centro; dirigir a analistas, investigadores y peritos forenses sobre la cantidad y el tipo de pruebas necesarias para la investigación y acusación que definen la acción penal.

> Los fiscales destacados para la investigación de delitos informáticos deberán contar con los siguientes conocimientos y habilidades: 1) conocimiento de la normatividad de los delitos informáticos y relacionados donde se vea incluida la tecnología ya sea como medio u objeto. 2) familiaridad con tecnología informática e forense informática; 3) compromiso de continuar capacitándose en los aspectos tanto

jurídicos como técnicos del enjuiciamiento del cibercrimen. (Centro para la Justicia y el Estado de Derecho, 2007, p. 26).

Peritos Forenses: Todas las investigaciones de cibercrimen incluyen información digital o datos propios de la tecnología usada, lo que obliga a fiscales e investigadores a solicitar la asistencia o asesoramiento del personal especializado en el are forense. Los datos de datos y pruebas digitales son parte integral de un número cada vez mayor de investigaciones penales. Por lo tanto, el aumento y estrecha relación de las pruebas digitales e informáticas con el trabajo de fiscales e investigadores evidencia la necesidad de los forenses informáticos internos.

Ahora ya que los peritos informáticos son los responsables de procesar toda la evidencia digital o informática obtenida por los investigadores de delitos informáticos, estos requieren tener un alto grado de especialización en el área de sistemas e informática, y de manera específica deberán contar como mínimo con los siguientes conocimientos y habilidades:

- Esterilización de medios de almacenamiento magnético y óptico.
- Selección y entrenamiento en software de recuperación y análisis de datos.
- Análisis de registros de auditoría y control.
- Correlación y análisis de evidencias digitales.
- Procedimientos de control y aseguramiento de evidencias digitales.
- Verificación y validación de procedimientos aplicados en la pericia forense.
- Experiencia y certificación en programación y mantenimiento de computadores y redes informáticas.
- Exhaustivo conocimiento de sistemas operativos informáticos.

- Formación y certificación en herramientas de informática forense.
- Compromiso con la educación continua en informática forense.

Relacionados con los aspectos técnicos de una investigación. Su responsabilidad principal es identificar, recolectar, analizar y preservar adecuadamente la evidencia digital, rastrear, analizar IP y redes de datos, ofrecer apoyo técnico especializado a fiscales, investigadores y diferentes dependencias internas y externas, utilizando herramientas forenses de hardware y software especializadas y la aplicación de técnicas estandarizadas que garantizan el correcto manejo de evidencia digital, así como realizar estudios técnicos a EMP/EF de carácter digital.

Otro contexto, es el hecho de que los peritos forenses de computadoras deben ir a juicio y proporcionar testimonios relativos a los aspectos técnicos de la recuperación y el análisis de datos, la habilidad que necesitan tener es la capacidad de testificar ante un juez.

Analistas: los analistas en cibercrimen estarán formados en el proceso especializado de gestión del conocimiento, expertos en los procesos de detallar un fenómeno criminal para conocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen, lo anterior tiene como objetivo generar conocimiento para poyar la toma de decisiones y la solución de problemas. Y de manera específica deberán contar como mínimo con los siguientes conocimientos y habilidades:

- Capacidad de análisis y de síntesis
- Proactivo, metódico y ordenado
- Capacidad de trabajo bajo presión
- Capacidad de hacer frente a desafíos

- Alta capacidad de investigación personal
- Tener permanente adaptación a los cambios y a las innovaciones tecnológicas
- Habilidades comunicacionales
- Capacidad de análisis de las relaciones entre las diversas partes de una situación o problema.
- Capacidad de descomponer tareas complejas en partes manejables de manera sistemática.
- Capacidad de reconocer las causas posibles de eventos o varias consecuencias de acciones.
- Capacidad de anticiparse a obstáculos y pensar por adelantado acerca de los próximos sucesos.
- Posee pensamiento conceptual: Reúne ideas, asuntos y observaciones en un concepto simple o en una presentación clara.
- Capacidad de Identificar temas claves en una situación compleja.

1. **Recursos Técnicos:** Los recursos especializados de tecnología necesarios para la implementación del proyecto. (Hardware – Software).
3. **Recursos Logísticos:** Los recursos logísticos podrán ser brindados tanto por Entidad, como pueden ser procurados ante organismos Internacionales a base de cooperación o a través del apoyo de las empresas nacionales.
4. **Recursos Económicos y Financiamiento:** El Recurso Económico y el financiamiento estará a cargo de la entidad, así como se podrá contar con el apoyo económico de organizaciones Internacionales y nacionales.

Finamente y teniendo en cuenta lo anterior (perfilamiento de personal), el equipo humano del centro debe contar con analistas, investigadores, peritos forenses, personal administrativo,

empleando la combinación adecuada de personal y los roles, encontrando así las personas adecuadas que representan un reto para cualquier Entidad. Considerando lo siguiente: 1) programadores: dada la necesidad soluciones rápidas a diario. 2) analistas: estrecha colaboración entre especialistas en cibercrimen y analistas ha demostrado ser rentable, especialmente en prospectiva; 3) técnicos: especialistas en redes y equipos; 4) personal administrativo: especialistas conducir la relación coste-eficacia. (Pisaríc, 2017).

5. **Infraestructura:** Los costos asociados con el funcionamiento de un Centro de Análisis, Investigación y Prospectiva de cibercrimen, en términos de personal, equipo y capacitación, representan a una cantidad importante de recursos. Las herramientas, tareas y prioridades del centro serán determinadas por el equipo de trabajo conformado por analistas, investigadores, fiscales, peritos informáticos.

El presupuesto tendrá que hacer parte del presupuesto general de la Entidad, con vigencias anuales, de igual manera se propone solicitar apoyo a organismos internacionales dedicados a la investigación, sanción y prevención de delitos informáticos, entre ellos, Computer Crime Unid del FBI, Unidad Nacional de Crimen de Alta Tecnología (NHTCU) del Reino Unido, la Brigada de Investigación Tecnológica de la Guardia Civil Española, Unidad de Delitos Cibernéticos de México, la Organización de Estados Americanos OEA y la Organización de las Naciones Unidas. (AusCERT, 1993) (Universidad UNIANDES, s.f.).

Debido a la rápida evolución de la tecnología por un lado, y las técnicas para desarrollar el Cibercrimen por el otro, el equipo necesita estar en la vanguardia de la tecnología y constantemente actualizado. Esto con el objetivo de contar con una capacidad de acción

actualizada y efectiva contra el cibercrimen, con impacto en la investigación y enjuiciamiento de ciberdelincuentes.

Por consiguiente, un presupuesto asignado a esta unidad debe dar alcance a costos de personal, de los equipos y programas necesarios, así como costos de utilización de técnicas especiales de investigación.

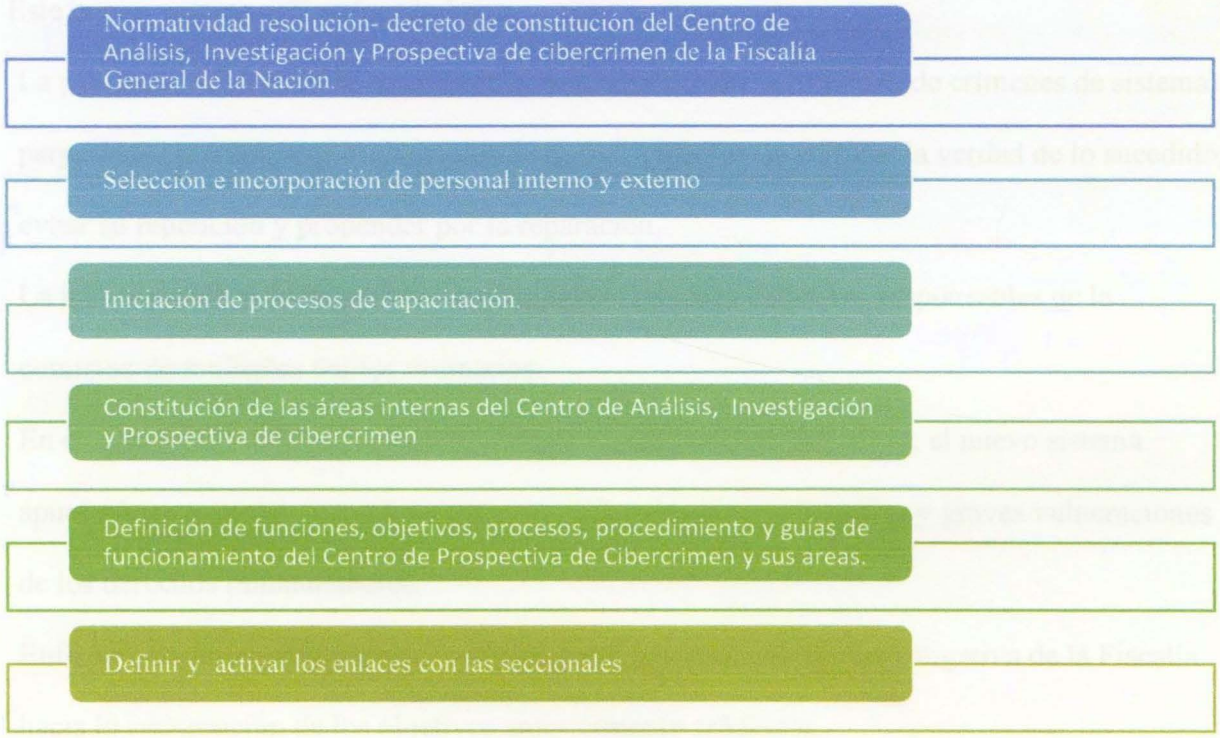
Entre las herramientas básicas de infraestructura física y equipos de tecnología de la Información y Comunicaciones TIC, debe contar:

i. Espacio físico amplio con ventilación e iluminación suficiente, muebles ergonómicos para el personal o equipo de trabajo.
ii. Almacenamiento seguro de datos y Backup gestionados, servicios de manera ininterrumpida de servicios.
iii. Computadores capaces de funcionar en espacios exteriores, entornos exigentes.
iv. Conexiones a internet no institucionales, herramientas forenses por servicio.
v. Software especializado en OSINT (Monitoreo de fuentes abiertas y redes sociales, Dar web (internet oscura)), en correlación y asociación de información, georreferenciación, minería de datos, y tecnologías para el procesamiento forense de sistemas informáticos, y otros dispositivos (Asociación de Jefes de Policía, 2012, p. 15-16).

7.4.3 Cronograma de implementación.

Con respecto a los tiempos de implementación del Centro de Análisis, Investigación y Prospectiva de cibercrimen se considera prioritario activarlo solo a nivel central, iniciando con

los procesos necesarios de capacitación en temas como prospectiva, ciberinteligencia, ataques electrónicos, legislación en delitos informáticos, entre otros. En la siguiente etapa se podrán definir y activar los enlaces con las seccionales según un criterio de gradualidad que considere el impacto de las conductas cibercriminales, en ciertas áreas así como las necesidades del servicio y exigencias particulares que podrían originarse en la materia. Se deberán construir los criterios para determinar de manera objetiva la necesidad de implementación del centro en las seccionales. De manera general se presenta el siguiente plan de trabajo.



Fuente: Elaboración propia, 2017.

Figura 2. Etapas del plan de trabajo - Implementación Centro de Análisis, Investigación y Prospectiva de Cibercrimen

7.4.4 Metodología de análisis e investigación.

El Centro de Análisis, Investigación y Prospectiva de Cibercrimen de la Fiscalía General de la Nación atenderá una metodología por priorización (Fiscalía General de la Nación, 2015), consistente, en una política orientada al diseño e implementación de una técnica de gestión estratégica de la carga de trabajo y del flujo de casos que son puestos en conocimiento de la Fiscalía, para el manejo analítico de la investigación, y del ejercicio de la acción penal.

Este nuevo sistema está enfocado hacia:

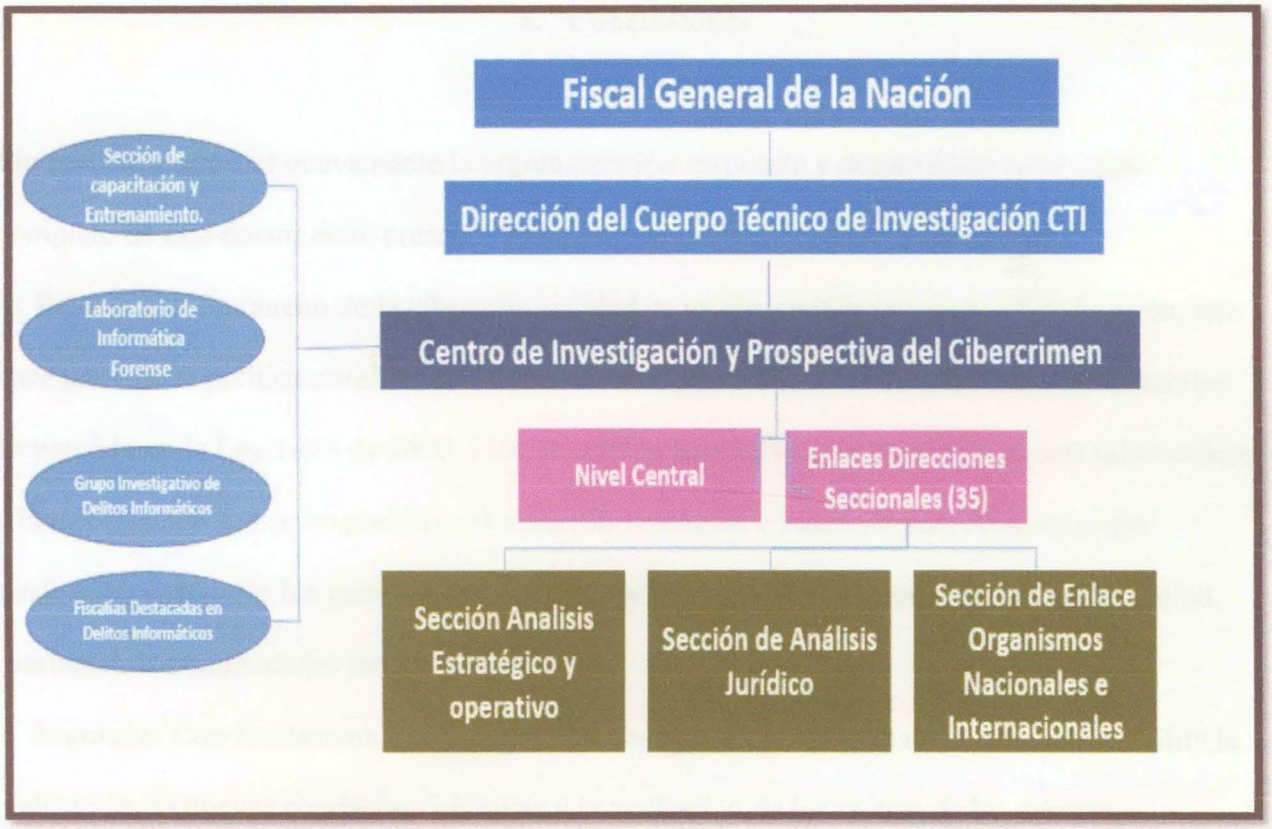
- La persecución efectiva de los máximos responsables de la comisión de crímenes de sistema, perpetrados por aparatos organizados de poder, a efectos de conocer la verdad de lo sucedido, evitar su repetición y propender por la reparación.
- La investigación y desmantelamiento de organizaciones delictivas responsables de la comisión de múltiples delitos ordinarios.
- En el caso de los delitos no perpetrados por organizaciones delictivas, el nuevo sistema apuntará, en especial, a combatir patrones culturales discriminatorios y graves vulneraciones de los derechos fundamentales.
- Enfocar de manera transparente, racional y controlada, la acción investigativa de la Fiscalía hacia la consecución de los objetivos anteriormente señalados.

En este sentido, la investigación en la Fiscalía General de la Nación ha evolucionado desde la lógica de casos o delitos, que considera solo la perspectiva de judicializar hechos aislados u organizaciones delictivas a una dinámica que se centra en fenómenos o estructuras delincuenciales, a su vez en un enfoque de entendimiento y anticipación a situaciones. Dicho

enfoque permite analizar y entender los principales patrones de actividad delictiva en el País y priorizar consecuentemente la investigación y los recursos en esa dedicados. (Fiscalía General de la Nación, 2015).

7.4.5 Estructura Organizativa.

El Centro de Análisis, Investigación y Prospectiva de cibercrimen estará integrado por un componente a Nivel Central y enlaces a nivel seccionales. Se especifica que los enlaces seccionales se irán constituyendo e integrando gradualmente según la disponibilidad de recursos humanos, materiales y acceso a programas de capacitación previstos para el Centro. Se propone la siguiente estructura orgánica.



Fuente: Elaboración propia del autor, 2017.

Figura 3. Estructura Orgánica del Centro de Análisis, Investigación y Prospectiva de Cibercrimen de la Fiscalía General de la Nación

8. Conclusiones

Sin pretender abordar nuevamente la argumentación expuesta y desarrollada en el texto completo de este documento, presento ideas generales que considero importantes.

Primera: el fenómeno de la cibercriminalidad es un tópico inmerso en la globalización, que hace parte de la política criminal del nuevo derecho penal. Para el caso específico de Colombia enmarcado en la Ley 1273 de 2009. Esto basado en la observancia, que los sistemas informáticos y la información son protagonistas del desarrollo nacional e internacional. Al tiempo que trasforman casi todos los parámetros conocido en una sociedad análoga a una sociedad digital, cambiando a comunidades interconectadas.

Segunda: Con fundamento en la presente investigación, el avance de la tecnología facilita la realización de nuevas conductas delictivas y la ocultación de los rastros de las mismas, dificultando cada día más, la investigación y el enjuiciamiento de delitos informáticos, derivando en un nuevo comportamiento y aplicación del derecho penal con innovadores formas de abordar los conocimientos científicos-investigativos.

Tercero: En este sentido, los tipos penales deben ser repensados de común acuerdo con especialistas en tecnología, pues se evidencia un enorme abismo entre la noción jurídica de los delitos y las exigencias técnicas que suponen la comisión en la realidad.

Cuarto: Como complemento y con base en el diagnóstico realizado frente la actuación de la Fiscalía General de la Nación para abordar el fenómeno de la cibercriminalidad se precisa la necesidad de abordar estas investigaciones con un enfoque internacional, con unidades investigativas especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo e, igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de

conductas. Así como el aporte de las mismas en el diseño de política criminal contra la cibercriminalidad.

Quinto: Es así, entonces, que la propuesta de fortalecimiento y articulación de capacidades misionales para realizar investigación y prospectiva contra el Cibercrimen en la Fiscalía General de la Nación, debe permitir un nuevo modelo de investigación cibernética, basado en la unificación, análisis y compartición de información. Generando investigaciones en contexto, con la finalidad de no solo comprender el fenómeno sino también de generar una presencia del Estado en el mundo virtual buscando un ejercicio sano de los derechos a los que tiene todo ciudadano de acceder y beneficiarse de las Tecnologías de la Información, así como la articulación con Entidades nacionales y extranjeras interesadas en garantizar un desarrollo seguro en el ciberespacio desde la práctica del ejercicio de la acción penal.

9. Referencias Bibliográficas

Agencia Española de Protección de Datos (2014). Disponible en: https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

AGPD Agencia Española de Protección de Datos (s.f.) Disponible en: https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Asociación de Jefes de Policía (2012).

Arias, F. G. (1999). *El Proyecto de Investigación,* guia para su elaboración 3edición.

Asociación Argentina de Lucha Contra el Cibercrimen - AALCC (2015). *Los Dominios de Internet y el Delito -Entrevista a Luis Nocera*. Disponible en: http://www.cibercrimen.org.ar/?author=3

AusCERT (1993). *AusCERT*. Disponible en: https://www.auscert.org.au/

Ballesteros, M., & Hernandez, J. (s.f.). *Cibercrimen: particularidades en su investigación y enjuiciamiento*. Madrid: Anuario Juridico y economico Esculialense, XLVLL (2014) 209-234/ISSN:1133-3677.

Blanco, A. P. (2015). *Propuesta Organizacional Grupo Análisis Estrategico*. Bogotá.

Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime:Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*.

Centro Criptológico Nacional (2016). *CCN-CERT*. Disponible en: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=18&Itemid=22

Centro Criptologico Nacional (2016). *Centro Criptografico Nacional - CCN*. Disponible en: https://www.ccn.cni.es/: https://www.ccn.cni.es/

Centro Nacional de Excelencia en Ciberseguridad. (2016). *CNEC Centro Nacional de Excelencia en Ciberseguridad*. Disponible en: http://www.cnec.university/

Centro Nacional para la Protección de las Infraestructuras Críticas (2010). *CNPIC.ES*. Disponible en: http://www.cnpic.es/

Centro para la Justicia y el Estado de Derecho (2007).

Centro Superior de Estudios de la Defensa Nacional (2012). *El Ciberespacio. Nuevo Escenario de Confrontación* . España.

Certsi - Cert de Seguridad e Industria. (s.f.). *Esquema Nacional de Seguridad Industrial*. ENSI.

Chismon, D., & Ruks, M. (2014). Threat Intelligence:Collecting, Analysing, Evaluating. *CPNI*.

Cloud Publications- International Journal of Advanced Computer Science and Information Technology (2014). Computer Crimes: Factors of Cybercriminal Activities.

colCERT (2013). *colCERT Grupo de Repsuestas a Emergencias Ciberneticas de Colombia*. Disponible en: http://www.colcert.gov.co/

Comando Conjunto Fuerzas Militares. (s.f.). *Comando General Fuerzas Militares*. Disponible en: http://cgfm.mil.co/comandos-conjuntos

Congreso de la República de Colombia (2009). Ley 1273 de 2009. *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas*

que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Diario Oficial 47.223 de enero 5 de 2009. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Consejo Nacional de Politica Económica y Social - Departamento nacional de Planeación Conpes 3854 (11 de Abril de 2016). *Documento Conpes 3854 Politica Nacional de Seguridad Digital*. Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consejo de Europa (11 de Noviembre de 2001). *Convenio Sobre la Ciberdelincuencia*. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Consejo Nacional de Política Economica y Social, CONPES. (26 de Diciembre de 2016). *El Consejo Nacional de Política Económica y Social, CONPES*. Disponible en: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

Corte Constitucional Republica de Colombia, (2005) *Sentencia C-1177/05,* M.P. Jaime Córdoba Triviño. Disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2005/C-1177-05.htm

Cyberseguridad, C. N. (15 de 02 de 2010). *Consejo nacional consultivo de cyberseguridad. s21sec*. Disponible en: https://www.s21sec.com/es/blog/2010/02/el-consejo-nacional-consultivo-de-cyberseguridad-alerta-de-la-necesidad-de-incrementar-la-seguridad-en-las-infraestructuras-criticas-del-pais/

Departamento Nacional de Planeación. (2011). *Politica de Ciberseguridad y Ciberdefensa.* Bogotá.

Departamento Nacional de Política Económica y Social - Conpes (14 de Julio de 2011). *Documentos Conpes 3701*. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Diccionario de la Real Academia Española (DRAE). (2010). Ciberespacio. *en su 22ª edición.*

Dokumentalistas. (18 de Febrero de 2015). *Recursos para profesionales de la informacion y la documentación*. Disponible en: http://www.dokumentalistas.com/noticias/obama-crea-el-ctiic-para-impedir-ciberataques/

EFE Agencia. (10 de Febrero de 2015). *Gobierno crea agencia para detectar amenazas ciberneticas y evitar ataques*. Disponible en: http://www.efe.com/efe/usa/sociedad/gobierno-crea-agencia-para-detectar-amenazas-ciberneticas-y-evitar-ataques/50000101-2533620

El Mundo (11 de Febrero de 2015). *Obama crea una agencia especial contra los ciberataques.* Disponible en: http://www.elmundo.es/tecnologia/2015/02/11/54daf347268e3e1d5d8b456b.html.

Elpais.com. (23 de Julio de 2009). Disponible en: http://elpais.com/diario/2009/07/23/ciberpais/1248315865_850215.html

Eltiempo.com. (02 de Diciembre de 2016). Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/estudio-de-impacto-de-ataques-ciberneticos-en-colombia/16764379

Endsley, M. (2000). *Theoretical underpinnings of situation awareness: A critical review. In M.R Endsley & D.J. Garland (eEds.), Situation Awareness Analysis and Measurement. Mahwah, NJ.*

Enisa. (08 de Noviembre de 2016). *European Union Agency for Network and Information Security*. Disponible en: https://www.enisa.europa.eu/

Enter.co Enterprise. (2016). *Microsof abrensu laboratorio global contra el cibercrimen*. Disponible en: http://www.enter.co/especiales/enterprise/microsoft-abre-su-laboratorio-global-contra-el-cibercrimen/

Europol. (2016). *European Cybercrime Centre-EC3*. Disponible en: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-1

FBI. (13 de 07 de 2017). Disponible en: https://www.fbi.gov/investigate/cyber

Fiscalia General de la Nación. (2013). *Informe de Diagnostico Delitos Informaticos año 2013.* Fiscalia General de la Nación , Bogota.

Fiscalia General de la Nación. (2013). *Medición Delitos Informaticos Fiscalia General de la Nación.* Bogotá: ViceFiscalia General de la Nación.

Fiscalía General de la Nación. (2015). *Política de Priorización Directiva 002 de 2015.* Bogotá.

Fiscalia General de la Nación . (2016). *Plan Estratégico 2016-2020.* Bogotá.

Fiscalia General de la Nación. (2017). Disponible en: http://www.fiscalia.gov.co/

Fiscalía General de la Republica - Escuela de Capacitación Fiscal. (24 de Octubre de 2016). *Jefaturas, Coordinadores y Fiscales reciben formación sobre Cibercrimen.* . Disponible en: http://escuela.fgr.gob.sv/jefaturas-coordinadores-fiscales-reciben-formacion-cibercrimen/

Global Cyber Security Capacity Centre. (06 de 02 de 2017). Disponible en: http://www.oxfordmartin.ox.ac.uk/cybersecurity/

GPEN Global Prosecutors E-Crime Network. (2016). *Global Prosecutors E-Crime Network.* Disponible en: http://www.iap-association.org/GPEN/Home

Grupo de Delitos Telemáticos Unidad Central Operativa. (2011). *GDT Grupo de Delitos Telemáticos Unidad Central Operativa*. Disponible en: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

IAP International Association of Prosecutors. (s.f.). *Raising standards for Prosecutors worldwide; improving international co-operation to combat crime*. Disponible en: http://www.iap-association.org/

IBM. (s.f.). *¿Qué es Big Data?* Disponible en: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/

ICSPA. (2014). *International Cyber Security Protection Alliance*. Disponible en: https://icspa.org/

INCIBE. Instituto Nacional de Ciberseguridad. (s.f.). Disponible en: https://www.incibe.es/que-es-incibe

Información Congreso Asobancaria Vicefiscalia. (2013). *Información Congreso Asobancaria Vicefiscalia.*

Instituto Nacional de Ciberseguridad de España S.A. (2016). *INCIBE*. Disponible en: https://www.incibe.es/aviso-legal

Interpol. (s.f.). *Interpol Connecting Polica For a Safer Word*. Disponible en: https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI

Microsoft. (19 de Octubre de 2016). *Microsoft New Center Latinoamerica*. Disponible en: http://news.microsoft.com/es-xl/microsoft-inaugura-centro-de-transparencia-en-brasil-para-atender-a-los-gobiernos-de-latinoamerica/#J3kSCYJ0jsBZTiR6.97

Ministerio de Defensa. (Marzo de 2011). *Documento Infromativo del IEEE 09/2011*. Nuevo concepto de la OTAN. Disponible en: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

Ministerio de Defensa Nacional - Policía Nacional de Colombia. (s.f.). *Centro Cibernetico Policial*. Disponible en: http://www.ccp.gov.co/

MinTIC. (22 de Agosto de 2016). *MinTIC y OEA iniciaron estudio del impacto de incidentes cibernéticos en Colombia*. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-16129.html

N. Kshetri. (s.f.). *Simple Economics of Cybercrime*.

National Center for Justice and the Rule of Law (2007).

NIST - National Institute of Standards and Technology. (2014). *NIST (National Institute of Standards and Technology) (Feb. 2014): Framework for Improving Critical Infrastructure*.

Noticias Universia. (Abril de 2013). *Los delitos más comunes en el ciberespacio son a través del correo electrónico*. Disponible en: http://noticias.universia.es/actualidad/noticia/2013/04/23/1018761/delitos-mas-comunes-ciberespacio-son-traves-correo-electronico.html

OEA - BID. (2016). *Observatorio de la Ciberseguridad en America Latina y el Caribe*.

Office of the Director of National Intelligence . (s.f.). *Leading Intelligence Integration* . Disponible en: https://www.dni.gov/index.php/intelligence-community/members-of-the-ic#cia

Office of the Director or National Intelligence. (2016). *Office of the Director or National Intelligence - united States of America*. Disponible en: https://www.dni.gov/index.php/contact-us

Organización of American States - BID. (2016). *Ciberseguridad ¿Estamos preparados en America*.

OTAN. (2011). *Revista de la OTAN.* Disponible en: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

Pérez, J. R. (2013). La "conciencia situacional" en la ciberdefensa. *Situacional Awareness*.

Pisaric, M. (2007). *Specializacion of Criminal Justice Authorities in Dealing with Cybercrime.*

Pisaríc, M. (2017). Specialization of Criminal Justice Authorities in Dealing with Cybercrime. *Journal of Criminal Justice and Security* , 13.

Ploom (2010).

Polanco, M. (2016). La ciberinteligencia como habilitador de la ciberseguridad. *Magazcitum*.

Policia Nacional de Colombia. (2015). *CSIRT-PONAL*. Disponible en: https://cc-csirt.policia.gov.co/

Presidencvia de la Républica de Colombia(2014) *Decreto 016 de 2014*. Disponible en: http://www.fiscalia.gov.co/colombia/la-entidad/organigrama/

Salom, J. (2011). *El Ciberespacio y el Crimen Organizado*.

Talihärm, A. M. (s.f.). International Criminal Cooperation in the Context of Cyber. *Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia*.

Universidad de Alcala de Henares - Madrid. (2016). *Master en Ciberseguridad.*

Universidad UNIANDES. (s.f.). *CANO JEIMY, Inseguridad Informática:Un concepto dual de la Seguridad.*

10. Anexos

Anexo 1. Encuesta

1. Cuáles son las preocupaciones en torno al cibercrimen en la investigación penal

a) Robo o pérdida de datos personales

b) Interrupción del servicio

c) Delitos financieros

d) Robo de la propiedad intelectual

e) Riesgo regulatorio

f) Costo de la investigación

2. Percepción de los riesgos del cibercrimen en los próximos doce meses

☐ Aumentara

☐ Disminuirá

☐ Se mantendrá

3. Percepción de la capacidad de respuesta de la FGN ante la presencia y evolución de nuevos fenómenos del cibercrimen.

☐ Alta

☐ Media

☐ Baja

4. Que consideración tiene para usted la Cooperación internacional frente a la investigación de delitos cibernéticos?

☐ De gran importancia

☐ Medianamente importante

☐ Sin importancia

5. Entre las mejores técnicas investigativa para rastrear bitcoin se encuentra:

☐ Monitorear y análisis del blockchain

☐ Monitorear y análisis del mercado de la criptomoneda

☐ Captura y análisis del monedero

6. Cuál cree usted que sería el aporte análisis y la prospectiva en el cibercrimen para la investigación penal-

☐ De gran importancia

☐ Medianamente importante

☐ Sin importancia

7. Cuál cree que es la mayor debilidad con que cuenta la Entidad frente las investigaciones de delitos informáticos o cibernéticos.

☐ Falta de preparación y capacitación del personal

☐ Ausencia de herramientas de última tecnología

☐ Ausencia de convenios internacionales

☐ Legislación débil e inapropiada.

Elaboración propia, 2017

BIBLIOTECA CENTRAL DE LAS FF. MM.
"TOMAS RUEDA VARGAS"
201002779