Planteamiento de las tablas de organización policial y la estructura organizacional para la creación de la dirección de ciberseguridad de la Policía Nacional

Juan Felipe Mantilla Elizalde

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2019

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

PLANTEAMIENTO DE LAS TABLAS DE ORGANIZACIÓN POLICIAL Y LA ESTRUCTURA ORGANIZACIONAL PARA LA CREACIÓN DE LA DIRECCIÓN DE CIBERSEGURIDAD DE LA POLICÍA NACIONAL

JUAN FELIPE MANTILLA ELIZALDE
Autor

MAGÍSTER STEVEN JONES CHALJUB
Asesor de Tesis

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTÁ-COLOMBIA
2019

PLANTEAMIENTO DE LAS TABLAS DE ORGANIZACIÓN POLICIAL Y LA ESTRUCTURA ORGANIZACIONAL PARA LA CREACIÓN DE LA DIRECCIÓN DE CIBERSEGURIDAD DE LA POLICÍA NACIONAL

Tesis de Grado

JUAN FELIPE MANTILLA ELIZALDE
Autor

MAGÍSTER STEVEN JONES CHALJUB
Asesor de Tesis

MINISTERIO DE DEFENSA NACIONAL
Comando General de las Fuerzas Militares - Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa
Bogotá, Colombia
2019

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Bogotá, Diciembre 2019

Tabla Contenido

Lista de Gráficas

Lista de Ilustraciones

Lista de Tablas

Resumen

La evolución de la tecnología ha traído consigo amenazas y vulnerabilidades que hace un tiempo no se contemplaban, cada día crece el número de ciberciudadanos los cuales hacen uso de todo tipo de redes y herramientas aumentando con esto las posibilidades para que los ciberdelincuentes cometan todo tipo de delitos, situación ante la cual el gobierno ha tomado acciones tendientes a hacer de los ciberusuarios personas con más conocimientos y capacidades sobre este entorno, estrategia que se ha asumido especialmente desde el Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC. (MInisterio de las Telecomunicaciones y de la Información - MINTIC, s.f.) mediante la creación de dos vectores como directrices de alineación a las estrategias nacionales tanto para el sector público como privado, establecidas en los documentos CONPES 3701 de 2011 y 3854 de 2016 los cuales presentan los lineamientos de Ciberseguridad y Ciberdefensa y la Política Nacional de Seguridad Digital, respectivamente. (Departamento Nacional de Planeación, 2016) (Departamento Nacional de Planeación, 2011).

Estrategia a la cual se ha unido también la Policía Nacional – PONAL, volcando sus esfuerzos para hacer una policía más competitiva en temas cibernéticos con el fin de atender de forma efectiva y eficiente las conductas delictivas que aquejan a los ciudadanos, contando para esto con grupos especializados distribuidos en las direcciones de Inteligencia Policial, Investigación Criminal e INTERPOL, Antisecuestro y Antiextorsión, Protección y la Oficina de Telemática, garantizando la anticipación, prevención, atención e investigación de todo tipo de conductas delictivas en el entorno Ciber.

Este proceso y la búsqueda de tácticas de mitigación, ha conllevado a que las capacidades aumenten significativamente sin generar una completa integración entre las unidades antes mencionadas, que permita la definición de estrategias transversales que abarquen todas las conductas que puedan afectar al ciudadano en el ciberespacio, por tal razón el alcance de este trabajo contempla un diagnóstico y una definición de procesos y funciones mediante la estructura organizacional de una nueva dirección, que permitan unificar estos grupos de la PONAL por intermedio de la creación de la Dirección de Ciberseguridad – (DICIS).

Palabras claves: Ciberseguridad, tablas operacionales, talento humano, amenazas cibernéticas, ataque cibernético, delitos informáticos, incidentes informáticos, Infraestructura crítica, Cibercriminal, GSI, pornografía Infantil.

Introducción

La dinámica del Cibercrimen y su constante evolución exponencial ha propiciado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación, con un alcance local, en la actualidad constituyan organizaciones trasnacionales complejas de Cibercrimen. La diferenciación de roles en las estructuras criminales, el fácil acceso al mercado ilegal de tecnología para el Cibercrimen, la dificultad del rastreo de actividades ilícitas en la internet profunda, las transacciones a través de monedas virtuales, el mercado ilegal de datos y el crimen como servicio, así como la débil armonización de la persecución penal internacional, han facilitado este escenario (Lewis, 2016).

Lo anterior, demanda que las actuales unidades de investigación deben evolucionar para enfrentar a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico, diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los axiomas vigentes. (Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677, 2014)

En este sentido, el Cibercrimen forma parte ya de la realidad criminológica de nuestro mundo, obviamente, esta evolución del Cibercrimen, conlleva un cambio en sus protagonistas esenciales: los criminales, víctimas y unidades investigativas; razón por la cual la Policía Nacional – PONAL, volcando sus esfuerzos para hacer una policía más competitiva en temas cibernéticos con el fin de atender de forma efectiva y eficiente las

conductas delictivas que aquejan a los ciudadanos, cuenta en la actualidad con grupos especializados distribuidos en las direcciones de Inteligencia Policial, Investigación Criminal e INTERPOL, Antisecuestro y Antiextorsión, Protección y la Oficina de Telemática, en aras de lograr anticipación, prevención, atención e investigación de todo tipo de conductas delictivas en el entorno Ciber.

Se destacan en esta parte operativa dos grupos creados a partir de las directrices establecidas en el CONPES 3701, como pioneros del tema Ciber en la Policía, el Equipo de Respuesta de Incidentes de Seguridad Informática –CSIRT PONAL (Policia Nacional de Colombia - CSIRT-PONAL, 2015) y el Centro Cibernético Policial – CCP (Ministerio de Defensa Nacional - Policia Nacional de Colombia, 2018), éste último con una robusta estructura para la atención de delitos informáticos como son: El laboratorio forense más grande del país ubicado en la ciudad de Bogotá D.C., ocho laboratorios regionales, 25 unidades de delitos informáticos capacitadas y especializadas, 150 funcionarios a nivel nacional que hacen las veces de peritos e investigadores, así como varios cuerpos de coordinación administrativa. (Policia Nacional de Colombia - CSIRT-PONAL, 2015).

A pesar de la PONAL tener este significativo componente, las actuales capacidades de respuesta, prevención e investigación no son suficientes para contrarrestar la problemática que se presenta en el ciberespacio. La razón principalmente se debe al crecimiento de amenazas y oportunidades delictivas conjuntas y en contexto, en este entorno las cuales crecen rápidamente, ejemplo, durante los años 2.015 y 2.016, de las

13.103 denuncias por delitos en contra de la ley 1273, tan sólo 498 fueron capturas como resultado de los trabajos realizados por los investigadores durante estos años, es decir tan solo un 3.1%. Para el año 2.017 ya el número de denuncias superaba las 7.450 aproximadamente, mostrando con esto un panorama complejo a la hora de querer atender todos los requerimientos realizados por los denunciantes (Policia Nacional - Investigación Criminal).

Con estos resultados mencionados, podemos observar que los esfuerzos no son suficientes y las cifras dejan entrever que la gran capacidad operativa de la PONAL por sus diferentes grupos trabajando de manera aislada se queda corta ante la necesidad de respuesta, problema que se presenta por múltiples factores, pero principalmente al interior de la institución por la falta de integración de las capacidades, problema que se acrecienta cada día por el aumento individual de capacidades en talento humano y herramientas de los grupos y equipos de la PONAL dedicados a la prevención e investigación de ciberdelitos.

Al interior de la PONAL se evidencia el fortalecimiento en capacidades cibernéticas aisladas por Dirección, ejemplo es la creación del Cibergaula (DIASE), el grupo de Componentes de Delitos Cibernéticos (DIPRO), el Grupo de Análisis del Espectro (DIPOL) y el Centro de Capacidades para la Ciberseguridad de Colombia C4 (DIJIN) (Policia Nacional - PONAL) (Policia Nacional de Colombia - CSIRT-PONAL, 2015) (Policia Nacional - Investigación Criminal) (Mayor Saavedra - Centro Cibernetico Policial), grupos que sin duda alguna tienen los más altos estándares de calidad, pero que

a su vez generan que el problema de tener los esfuerzos aislados crezcan cada vez más.

Claramente la Policía Nacional trabajó en la alineación en temas ciber de acuerdo a lo establecido en el Conpes 3701, con la creación del CCP y el CSIRT, sin embargo se queda corta en la alineación al Conpes 3854 que establece dentro de su política digital, la unificación de criterios y estrategias las cuales para la institución policial, deberían verse reflejadas en la unificación de esfuerzos de todos estos grupos creados, a fin de no generar duplicidad de funciones y tareas que en algunos de los casos conlleva al desgaste operacional de las unidades y la segmentación de la capacidad operativa lo que lleva a fragmentar la capacidad de combatir un delito como fenómeno y lo termina convirtiendo en casos aislados, impidiendo con eso ser más eficientes y oportunos en la labor encomendada. (Conpes 3854 - Seguridad Digital, 2016)

Dado lo anterior, se evidencia la necesidad de hablar de la creación de la Dirección de Ciberseguridad de la Policía Nacional (DICIS), como el ente integrador y unificador de la totalidad de las capacidades investigativas y operativas. Sin embargo, esto requiere de un conocimiento claro de la estructura organizacional de la DICIS y del personal que debe participar en esta construcción con sus respectivas funciones. El propósito es contar con las personas más idóneas posibles; es decir, que ostenten las competencias requeridas por los diferentes perfiles según los cargos.

Pregunta:

Por las razones anteriormente expresadas, la pregunta de investigación que este

documento responde es la siguiente:

¿Cuáles deberían ser las tablas TOP y la estructura organizacional de la Dirección de Ciberseguridad de la Policía Nacional como nueva dependencia de la PONAL, para responder de manera efectiva a los delitos cibernéticos?

Con el fin de dar respuesta a esta pregunta, en primera instancia se remite a la misión encomendada a la Policía Nacional, la cual se encuentra plasmada en el artículo 218 de la Constitución Política de Colombia (Constitución Politica de Colombia 1991). Ésta dicta que el fin primordial de la Institución es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas y asegurar que los habitantes de Colombia convivan en paz, (Constitución Politica de Colombia 1991) esta misión no solo está encaminada a salvaguardar la seguridad física de los colombianos sino también la evolución exponencial de la tecnología utilizada por cada uno de los ciudadanos como parte de sus labores diarias, esto ha hecho que la PONAL despliegue procesos de prevención e investigación de conductas que ocurren en el ciberespacio, escenarios virtuales que hace algunos años no se contemplaban como factores de riesgo para la seguridad y bienestar de los colombianos.

Igualmente, y tomando como ejemplo están las buenas prácticas internacionales, destacando entre ellas **CTIIC (*Cyber Threat Intelligence Integration Center***, traducido "Centro de Integración de Inteligencia contra la Amenaza Cibernética"). como una nueva agencia del gobierno federal de los Estados Unidos que será un centro de fusión

entre las agencias existentes y el sector privado para uso en tiempo real contra ataques cibernéticos. (Office of the Director or National Intelligence, 2016).

Paso a seguir de manera operativa, se realiza un análisis de las capacidades ya existentes en el talento humano de las unidades policiales que intervienen en el ciberespacio logrando con esto brindar a la institución una propuesta de la estructura orgánica proyectada para una nueva Dirección (Dirección de Ciberseguridad- DICIS). A continuación, se identifican las tablas de Organización Policial (TOP), tablas que permitan identificar los diferentes roles y perfiles necesarios para la estructura orgánica de la DICIS. Dirección que concentrara los diferentes grupos investigativos con dominios especializados en la investigación del cibercrimen, con el objetivo de 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, la valoración la solución propuesta tiene un alcance en, a) diagnosticar las capacidades actuales con que la PONAL aborda el cibercrimen o delitos informáticos, b) identificar las capacidades misionales necesarias para fortalecer la persecución concentrada, en contexto de criminales en el ciberespacio, c) identificar las tablas de Organización Policial (TOP), tablas que permitan identificar los diferentes roles y perfiles necesarios para la estructura orgánica de la DICIS y d). Definir la estructura orgánica proyectada para Dirección de Ciberseguridad- DICIS.

De esta manera, este trabajo tiene como misión evidenciar la importa de unificar criterios, procesos y esfuerzos, con el único fin de permitir a la PONAL ser más eficientes en el proceso ciber y brindar una respuesta oportuna ante los requerimientos ciudadanos, igualmente ver que la Policía ya cuenta con las capacidades tanto de personal como de herramientas e infraestructura para avanzar positivamente en la creación de una dirección que integre estas unidades atomizadas.

Finalmente, este documento visualiza que la mayoría de las funciones ya se realizan en la institución, pero no existe una integración entre ellas, lo que lleva a que existan duplicidad de funciones y limitaciones en la función de estrategias que abarquen todas las conductas que puedan afectar a un ciudadano en el ciberespacio.

1. Problema de Investigación

Teniendo en cuenta el marco jurídico y organizacional de la Policía Nacional, así como la aplicación de su misión la cual es mantener las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y de manera específica para este caso, en delitos informáticos, se evidencian de forma general algunos factores que fortalecidos serian la base para el logro de capacidades de prevención, anticipación, mitigación, investigación y judicialización en el desarrollo de la investigación penal destacada en el ciberespacio, como son:

- No se tienen integradas en una sola dirección, todas las unidades ciber de la Policía Nacional.
- No se cuenta con la estructura organizacional de la DICIS.
- La policía no tiene unificadas las capacidades investigativas y operativas con las que cuenta.
- Se tiene una carencia de lineamientos tácticos operacionales.
- No hay una delimitación de las funciones tanto operativas como administrativas.
- No se tienen determinadas las cantidades de funcionarios por grupos, sus respectivos perfiles y capacidades.

La desintegración de las capacidades se puede observar en los esfuerzos no alineados realizados al interior de la Policía. Es así como podemos observar la creación en un principio y gracias a los parámetros establecidos por el CONPES 3701, del CCP y el CSIRT PONAL,

los cuales dieron inicio las capacidades de la policía en el ciberespacio, luego vino la creación del Cibergaula para la investigación de delitos como el cibersecuestro, posterior a este la creación de la Unidad de Delitos Cibernéticos cuya misionalidad se enfoca en la prevención e investigación de los delitos cibernéticos cometidos en contra de menores de edad, y por último el C4 como el Centro de Capacidades para la Ciberseguridad de Colombia, este último integrando tan solo las capacidades Ciber de la DIJIN.

Esto hace que no se tengan parametrizados y estandarizados las capacidades investigativas y operativas lo que conlleva a la carencia de criterios tácticos operacionales, pues no hay delimitación de funciones. Al no alinear los esfuerzos, todas las unidades realizan trabajos aislados y en ocasiones similares que traducido al problema presentado sería la duplicidad de tareas. (Policía Nacional - Investigación Criminal).

Es importante que la Policía Nacional, tome como referentes las buenas prácticas utilizadas por las diferentes organizaciones a nivel mundial, entre estas las de países cuyas uniones está basada en la ayuda mutua en busca de la protección de las naciones ante ataques enemigos, ejemplo de estos encontramos en las políticas digitales de las OTAN, la OEA y la Unión Europea entre otras.

Para la OTAN, su fin principal, es generar un compromiso por parte de sus integrantes, para mejorar su seguridad informática y armonizar sus capacidades con las del resto de los aliados, así como poner en línea la doctrina estadounidense, británica o francesa que establece que el ciberespacio debe ser designado oficialmente como un dominio de las

operaciones aliadas. Eso permitirá integrar este entorno en el proceso de planeamiento de la defensa, gestionar mejor los recursos existentes y orientar la obtención de cibercapacidades ofensivas, pero además forzará a todos los aliados a desarrollar cibercapacidades reales y efectivas. (THIBER, 2016).

Para la Organización de los Estados Americanos OEA, se estableció la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética, con esta se proporcionó el mandato que permite especialmente al Comité Interamericano contra el Terrorismo (CICTE), trabajar en asuntos de Seguridad Cibernética.

La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio.

Entre los principales objetivos de la OEA, se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio (Cibernética, 2018)

Otro ejemplo es la Estrategia de Ciberseguridad generada por la Unión Europea, que incluye entre su contenido principal, la estrategia de implementación de un Marco Político de Ciberdefensa (MPCD) este marco político establece la integración de capacidades y el fortalecimiento de las estrategias de protección a infraestructuras de los países y su Ciberdefensa, así como el intercambio de conocimientos y capacidades que permitan a los integrantes de la UE brindarse apoyo en una lucha contra los ciberterroristas (España, 2015).

Estos ejemplos, permiten establecer que se requiere entonces en la Policía Nacional de un perfeccionamiento organizacional y de procesos que permitan la unificación de capacidades en Ciberseguridad, es decir, la unificación del talento humano con capacitación en ciberseguridad en una única unidad y que esto permita a su vez establecer la estructura organizacional de la DICIS para lograr ejercer una eficiente y oportuna prevención, anticipación, mitigación y judicialización frente el Cibercrimen.

2. Justificación

Existen diferentes razones por la cuales vale la pena justificar la solución al problema planteado el cual se presenta como fenómeno y por qué se requieren la unificación de esfuerzos en una sola unidad.

1. La misión de la Entidad en el marco de su creación, particularmente en su misión, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz , así como su misión donde para el 2022 la Policía Nacional se proyecta como una institución fundamental para la construcción de un país equitativo y en paz, garante y respetuoso de los derechos humanos, afianzando la convivencia y seguridad a través del control del delito, la educación ciudadana, prevención, mediación y articulación institucional e interinstitucional como ejes centrales del servicio.

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 con 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, y centrando su problemática en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al

respecto, estableciendo causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. (Departamento Nacional de Política Económica y Social, 2011, pág. 2)

También implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. Este objetivo permitirá conformar organismos con la capacidad técnica y operativa necesaria para la defensa y seguridad nacional en materia cibernética. Para alcanzarlo se hace necesario que el Gobierno Nacional implemente las siguientes instancias: (Departamento Nacional de Política Económica y Social, 2011, pág. 20). para la Policía Nacional:

> Entregan a la Policía Nacional la responsabilidad de la Ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos, desarrollando labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país. informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en Ciberseguridad y trabajará de forma coordinada con el colCERT. Así mismo establecen para Policía, que su CCP estará conformado por el equipo que designe la Policía Nacional, el cual estará encargado de dar respuesta operativa a los delitos cibernéticos. Para su operación, el CCP incorporará en su estructura el Comando de Atención Inmediata Virtual - CAI Virtual, un grupo de prevención, uno de gestión de incidentes y

> otro de investigación. El CAI virtual tendrá la labor de recibir toda la información y reportes de delitos cibernéticos, clasificando las conductas delictivas encontradas. Adicionalmente, podrá recibir solicitudes de charlas, cursos o visitas para difundir temas de seguridad pues está a cargo de los procesos de difusión y prevención del delito cibernético, siempre en coordinación con el colCERT. El CCP se encargará de la investigación y apoyará la judicialización de los casos que se materialicen y se tipifiquen como delitos informáticos. (Departamento Nacional de Política Económica y Social, 2011, pág. 26).

En esta misma línea, el CCP buscará la colaboración de programas que apoyan la implementación del sistema penal oral acusatorio tales como el International Criminal Investigative Training Assistance Program - ICITAP, ATA, OPDAT y organismos nacionales como la Escuela de Investigación Criminal, Criminalística y de Ciencias Forenses de la Fiscalía General de la Nación, la Escuela Judicial Rodrigo Lara Bonilla, entre otros, para establecer planes de capacitación jurídica en lo referente a la seguridad informática para policía judicial, fiscales y jueces. (Departamento Nacional de Política Económica y Social, 2011, pág. 27).

> Igualmente, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), será garante de la gestión operativa de los incidentes de Ciberseguridad el sector privado y la sociedad civil. (Departamento Nacional de Política Económica y Social, 2011, pág. 22).

Estas tareas encomendadas a la PONAL dan cuenta de la alta responsabilidad entregada a la entidad, la cual requiere para esto ser efectiva en el cumplimiento de esta labor y para hacerlo, en este ámbito de ciberdelincuencia tan avanzado, necesita unir sus esfuerzos y unificar criterios de prevención e investigación, los cuales puede lograr en la alineación de todos los grupos y unidades que tratan los ciberdelitos dentro de la institución.

Luego el Conpes 3854 de 2016 establece la Política Nacional de Seguridad Digital, conteniendo 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).

La política digital establecidas en el Compes 3854, igualmente incorpora a la PONAL con responsabilidades de ámbito nacional, para que sea integradora de capacidades no solamente en el ámbito público, sino en el privado, labor que exige estar al margen del problema y liderar una campaña de prevención entre todas las partes interesadas.

Puede indicarse entonces, que el documento se fundamenta en apoyar estas funciones más a nivel interno en concordancia con el CONPES 3854 que dice así:

unificar capacidades de Ciberseguridad con un enfoque de gestión de riesgos de seguridad digital, entrelazar esfuerzos de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la seguridad digital en busca de evitar llegar a ser insuficientes y desarticulados, fortalecer la seguridad de los ciudadanos y del Estado en el entorno digital, con enfoque de gestión de riesgos entre otros. (Conpes 3854 - Seguridad Digital, 2016).

Estas responsabilidades enmarcadas en los Compes y constitucionalmente, hace que la policía se esfuerce por redoblar sus capacidades y de esta manera cumplir la labor encomendada, estos arrojos se ven reflejados en la creación de diferentes grupos dedicados a la mitigación del problema, grupos que se crean bajo la necesidad y objetivos trazados por cada dirección, ejemplo de estos es: si el delito se enfoca al secuestro, el grupo es creado dentro de la DIASE y solo se enfocará en este delito, pero sí de ataques en las redes se trata, el caso lo tomará el CSIRT, los anteriores solo para tener un ejemplo como referente.

Entonces en este trabajo mostramos la necesidad de crear una única unidad que recoja todas las capacidades en temas cibernéticos de la PONAL y a su vez implementar la creación de las Tablas de Organización Policial (en adelante TOP), las cuales se detallarán más adelante y tendrían como misión la de estandarizar las cantidades de personal requerido en cada uno de los cargos de la DICIS junto con las capacidades y perfiles de cada funcionario para de esta manera dar paso y poder generar la estructura organizacional de la misma.

3. Objetivos

3.1. Objetivo general

Propuesta para la articulación de capacidades en ciberseguridad de la Policía Nacional, planteamiento de las tablas TOP y la estructura organizacional para la creación de la Dirección de Ciberseguridad de la Policía.

Propuesta de fortalecimiento y articulación de capacidades misionales investigativas de la Policía Nacional en los delitos cibernéticos.

3.2. Objetivos específicos

- Diagnosticar las capacidades actuales con que la Policía Nacional aborda y realiza la investigación penal de los delitos cibernéticos.

- Identificar las capacidades actuales con que la Policía Nacional aborda y realizar la investigación de los delitos cibernéticos.

- Articulación de capacidades institucionales necesarias para abordar la investigación de los delitos cibernéticos con una persecución en contexto de los fenómenos cibercriminales.

- Identificar la lista de cargos y perfiles con sus respectivas funciones y roles para la estructuración de la Dirección de Ciberseguridad de la Policía Nacional-DICIS.

- Determinar y proyectar la jerarquización orgánica de la Dirección de Ciberseguridad – DICIS.

- Determinar y proyectar la jerarquización de la Dirección de Ciberseguridad – DICIS. Por medio del planteamiento de su estructura organizacional.

4. Metodología

El marco metodológico es la explicación de los mecanismos utilizados para el análisis de nuestra problemática de investigación y cuáles serán los pasos a utilizar para dar solución al problema presentado. El método es el resultado de la aplicación, sistemática y lógica, de los conceptos y fundamentos expuestos en el marco teórico. (APA , 2018).

4.1. Métodos de Investigación.

Este trabajo está basado en un modelo analítico e investigativo, los cuales de manera conjunta dieron paso a la verificación de un problema y de manera paralela la proyección de la solución al mismo. Estos modelos permitieron evidenciar que el problema se presenta por la falta de integración de capacidades en la PONAL y este a su vez genera una reducción en la capacidades investigativas y operativas de la institución en el ciberespacio.

En consecuencia, a lo anterior, el presente trabajo se basa en revisión bibliográfica, enfocada a la manera en que actualmente la policía judicial aborda la investigación de los delitos informáticos y el cibercrimen en Colombia. Por otro lado, se tomó como herramienta de recolección y análisis de información el análisis documental, desde las normas de tipificación de delitos informáticos, normatividad y revisión de convenios como el CONPES.

4.2. Técnicas de Investigación

Ahora, se necesitan procedimientos y medios que hagan operativos los métodos. A este nivel se sitúan las Técnicas. Estas, como los métodos, son respuestas al cómo hacer para alcanzar un fin o resultado propuesto, pero se sitúan a nivel de los hechos o de las etapas prácticas que, a modo de dispositivos auxiliares, permiten la aplicación del método, por medio de elementos prácticos, concretos y bien adaptados a un objeto bien definido. Es así entones, como en el desarrollo de este trabajo se utilizaron las siguientes técnicas. (Monografias, 2005).

4.3. Técnica de Observación.

Se realiza un diagnóstico de los fenómeno de la investigación a través de la operación de las variables que intervienen en el comportamiento del mismo. De manera específica se realizó observación sobre personas, fenómenos, hechos, casos, acciones, situaciones que día a día se presentan en los diferentes grupos que desarrollan investigación, judicialización y prevención en los delitos informáticos y cibercrimen de la Policía Nacional, con el fin de obtener información necesaria para la investigación en curso.

Tipo:

- Observación indirecta: Se precisa a través de las observaciones realizadas anteriormente por otra persona, para este caso se realizó al tener en cuenta libros, revistas, informes, estadisticas, etc.,
- Observación no participante: se tomó información desde afuera, sin intervenir para nada en los grupos investigativos ni operativos.

- Observación no Estructurada: se realiza sin la ayuda de elementos técnicos especiales, para este caso el conocimiento tácito del tema por la experiencia y el tiempo de participación en la institución.
- Observación de Campo: se realiza en los lugares donde ocurren los hechos o fenómenos investigados, directamente en los grupos investigativos de la Policía Nacional, realizando visitas a las unidades que intervienen en el tema como fueron la Dirección de Inteligencia, la Dirección de Policía Judicial e Interpol, la Dirección Antiextorsión y Antisecuestro, la Dirección de Protección y la Oficina de Telemática.

Ítems Observados

- ✓ Rutas de ingresos de casos
- ✓ Designación de misiones de trabajo
- ✓ Técnicas de investigación
- ✓ Organigrama institucional
- ✓ Personal a cargo
- ✓ Personal capacitado
- ✓ Oferta de capacitación
- ✓ Medios logísticos

Resultados:

- Descentralización de procesos investigativos
- Toma de decisiones las cuales no permiten alcanzar completamente los efectos necesarios para que las investigaciones logren la connotación de un todo investigativo.

- Investigaciones por caso a caso
- Diferentes unidades investigando delitos informáticos o cibercrimen
- Diferentes técnicas de investigación
- Diferentes rutas de ingresos de casos
- Medios logísticos apropiados
- Alta carga misional

4.4. Técnica de la Encuesta.

Se realiza recopilación de opiniones por medio de cuestionarios en un universo o muestra específico, con el propósito de aclarar un asunto de interés para el encuestador. De manera específica se realizó lo siguiente. El universo estuvo establecido por los diferentes grupos investigativos de la Policía Nacional que tiene a su cargo la investigación de los delitos informáticos y el cibercrimen en Colombia.

Encuesta diseñada para ser diligenciada por investigadores de los grupos asignados a los delitos informáticos y los jefes de estos, así como se contó con los recursos de personal/ participantes, materiales e instrumentos y procedimientos.

Nombre de la encuesta: Capacidad de la Policía Nacional para combatir los delitos informáticos en Colombia.

Responsable encuesta: Juan Felipe Mantilla Elizalde

Fecha de recolección de la información de campo: 04 de febrero al 25 de abril 2017.

Marco de muestra: Personal del grupo Delitos Informáticos, Informática Forense, Eje de Cibercriminalidad, Apoyo Jurídico, Gestión Contractual, Convenios, Monitoreo y Análisis entre otros.

Lugar donde se realizó: En los grupos de las Direcciones de la Policía los cuales cumplen funciones en el entorno cibernético del país.

Tamaño de la muestra: 54

Técnica de recolección: Cuestionario estructurado vía web.

Fecha del reporte: 10 de mayo de 2017

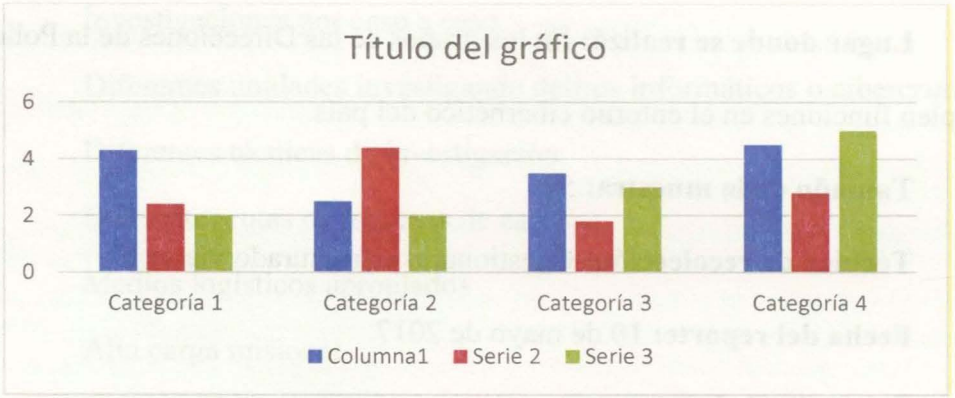
Desarrollo de la Encuesta:

1. Considera usted, que la Policía Nacional actualmente se encuentra en la capacidad de abarcar al 100% la prevención y la investigación de los ciberdelitos en Colombia?

1) Si
2) No

2. ¿Cuáles considera que son las principales razones por las cuales aumentan los ciberdelitos en el país sin que exista una eficaz mitigación del mismo?

a. Ausencias de capacidades del estado
a. Ausencia de políticas unificadas
b. Nuevos delitos informáticos y cibercrimen
c. Riesgos regulatorios



Gráfica 1: Fuente: Elaboración propia, 2018

Análisis:

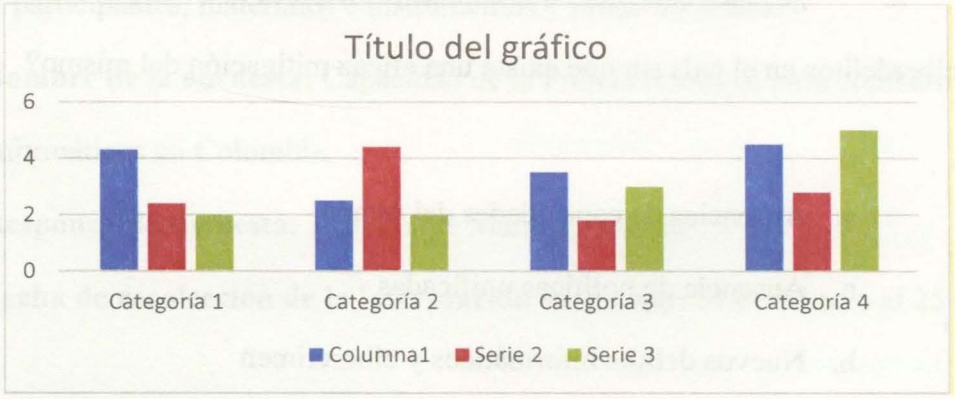
3. ¿Cómo asegura su organización un cumplimiento efectivo contra los delitos informáticos y el cibercrimen?

a. Capacitación actualizada

b. Unificando estrategias de intervención

c. Concentración de capacidades

d. Creación de nuevas especialidades



Gráfica 2. Fuente: Elaboración propia, 2018

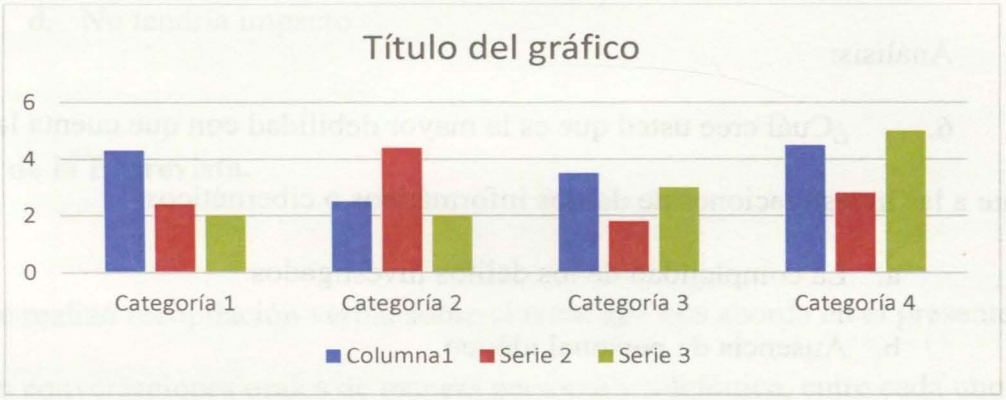
Análisis:

4. Percepción de la capacidad de respuesta de la PONAL ante la prevención, investigación y mitigación del cibercrimen en Colombia.

a. Alta

b. Media

c. Baja



Gráfica 3. Fuente: Elaboración propia, 2018

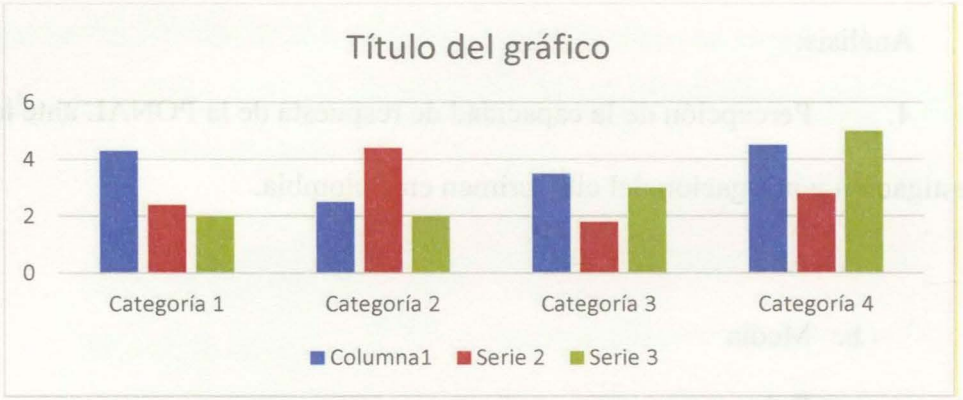
Análisis:

5. ¿Considera usted que la creación de múltiples grupos investigativos contra los delitos informáticos en las diferentes Direcciones Operativas son la solución efectiva para combatir los fenómenos del cibercrimen en su Entidad?

a. De acuerdo

b. Medianamente de acuerdo

c. En desacuerdo

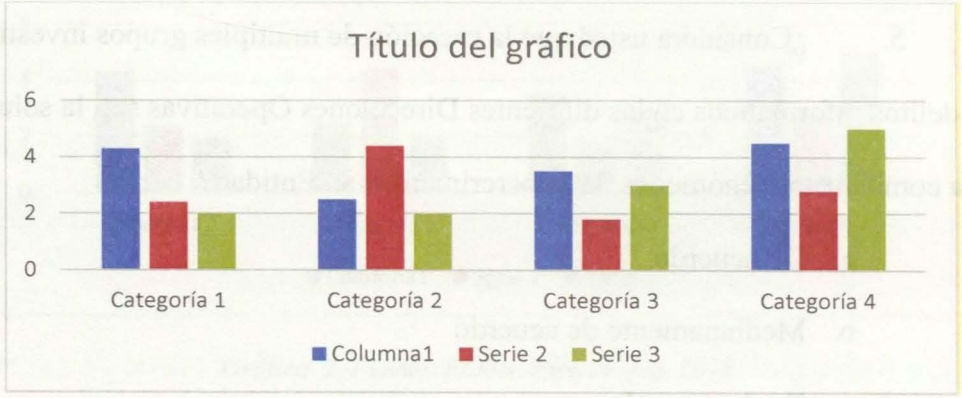


Gráfica 4. Fuente: Elaboración propia, 2018

Análisis:

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

a. La complejidad de los delitos investigados
b. Ausencia de personal idóneo
c. Falta de integración de capacidades
d. Ausencia de medios



Gráfica 5. Fuente: Elaboración propia, 2018

Análisis:

7. ¿Considera usted que la unificación de capacidades investigativas (grupos investigativos) en la PONAL impactaría de manera positiva los resultados contra los delitos informáticos y cibercrimen?

a. Altamente
b. Medianamente
c. Mínimamente
d. No tendría impacto

4.5. Técnica de la Entrevista.

Se realizó recopilación verbal sobre el tema que nos aborda en el presente. Se realizaron conversaciones orales de manera personal y telefónica, entre cada uno de los funcionarios escogidos los cuales estaban adscritos a las unidades que cumplen funciones de ciberseguridad en la policía (entrevistados) y Juan Felipe Mantilla como autor de este trabajo (entrevistador).

Entrevistador:	Juan Felipe Mantilla Elizalde	
Entrevistado 1:	Mayor Richard Gabriel Castro Camacho Jefe Telemática Dirección de Inteligencia	
	La Dirección de Inteligencia Policial	Respuesta
Preguntas 1:	Que grupos componen el	El SECYC está compuesto por cuatro grupos que son: Criptoanálisis, Minería e Datos,

	SECYC y que funciones cumplen estos.	OSINT y Monitoreo, estos grupos cumplen cada uno funciones correspondientes al análisis y observación de los diferentes movimientos que existen en el espectro en función al manejo de frecuencias, redes y comunicaciones. Para ser más puntuales el grupo de Criptoanálisis es el encargado del proceso relacionado al análisis de señales cifradas bien sea en las redes o en comunicaciones de campo abierto, el grupo de Minería de Datos realiza un permanente monitoreo y correlación de información de correos, celulares, redes sociales y whastapp, el grupo OSINT tiene como función, realizar seguimiento permanente a fuentes abiertas y el grupo de Monitores, tiene como responsabilidad realizar verificación, seguimiento y análisis permanente a la DEEPWEP.
Preguntas 2:	Cuantas personas están asignadas a su grupo.	Dentro del grupo de señales SECYC tenemos asignados 16 funcionarios de los cuales 2 son oficiales, 6 son suboficiales y 8 son patrulleros.
Preguntas 3:	Existen la suficiente la capacitación requerida para fortalecer el perfil del personal.	Si existe, el personal que integra el grupo es personal con perfiles académicos alineados a la necesidad que exige las funciones que cada uno realiza, así como las herramientas que manejas para el desarrollo de sus labores. Es importante aclarar que además de las capacitaciones realizadas o que cada uno trae cuando llega nuevo al grupo, ellos están en constante capacitación en diferentes entidades

		o institutos lo cual les permite fortalecer su perfil permanentemente. Para ser más concreto quiero decirle que dentro de este grupo el personal que lo integra tiene su perfil académico de la siguiente manera: 1 con maestría, 2 con especialización estas enfocadas a la ciberseguridad y a la seguridad de la información, 4 ingenieros de sistemas y 9 con curso de análisis de información en inteligencia.
Preguntas 4:	Considera que existe duplicidad de funciones en los grupos que realizan investigación contra los delitos informáticos y cibercrimen.	Para ser puntuales en la pregunta le diría que en el SESYC no, en este grupo cada uno está enfocado en una línea específica en lo que al análisis del espectro se refiere, sin embargo, le podría asegurar que hay dos factores que si considero son débiles a la hora de hablar de una ciberseguridad en el país y son, las primera que acá en DIPOL se realiza análisis de espectro enfatizados en temas como terrorismo y objetivos de alto valor, pero hace falta si hablamos de temas con menores, de extorciones etc., por otro lado creería que dentro de la policía si se deben duplicar funciones de estas, es decir se de grupos en DIJIN y OFITE cumplen funciones similares a las que nosotros hacemos.

Entrevistador:	Juan Felipe Mantilla Elizalde	
Entrevistado 2:	Teniente Coronel Alex Uriel Durán Santos Jefe Centro Cibernético Policial	
	La Dirección de Policía Judicial e Interpol	Respuesta
Preguntas 1:	Que funciones cumple el CCP	Quisiera empezar diciendo que el Centro Cibernético Policial es el grupo más grande en cuanto a prevención, análisis e investigación de delitos informáticos se refiere con que cuenta la PONAL, sus funciones están enfocadas a todo el espectro cibernético del país, abarcando los convenis internacionales con grupos y entidades dedicadas a la ciberseguridad en otros países, liderar la prevención de los ciberdelitos por medio de charlas a colegios, entidades estatales y empresas, investigación de los delitos cibernéticos denunciados a través del CAI virtual, el monitores de redes sociales y del espectro entre otros.
Pregunta 2:	Que grupos componen el Centro Cibernético Policial	El CCP lo componen cuatro grupos los cuales tienen subgrupos estos se organizan de la siguiente manera: El Centro de Capacidades para la Ciberseguridad el cual lo componen el CAI virtual, el subgrupo de trabajo conjunto con el FBI de los Estados Unidos, el subgrupo de trabajos conjuntos y convenios con EUROPOL y el grupo de prevención. La Unidad Investigas la cual la componen el subgrupo contra delitos económicos, subgrupo

		contra delitos de alta tecnología y subgrupo contra la pornografía infantil.
Preguntas 3:	Cuantas personas están asignadas a su grupo	El CCP está integrado por 64 funcionarios en total, de los cuales 8 son oficiales, 13 son suboficiales y 43 son Patrulleros.
Preguntas 4:	Existen la suficiente la capacitación requerida para fortalecer el perfil del personal	Si, el personal que integra el CCP es personal capacitado e idóneo para cumplir las tareas que a cada uno le son asignadas, de hecho, estas tareas son asignadas de acuerdo al perfil del funcionario, las capacidades que este tenga frente a cada área, a su vez los funcionarios son incorporados a esta unidad una vez se les ha realizado el estudio del perfil. El CCP cuenta como anteriormente le mencioné, con 64 funcionarios, de los cuales 3 son funcionarios con estudios en Maestría, 5 con especialización, 7 ingenieros, 24 tecnólogos y 25 son técnicos en investigación criminal. Sumado a esto para el CCP es muy importante que el personal este en constante aprendizaje y actualización, es por esto que se tienen alianzas con diferentes entidades y otras policías a nivel internacional, con las cuales se realizan capacitaciones al personal constantemente y de esta manera lograr que estén a la vanguardia en cuanto a novedades del entorno cibernético y en herramientas para el monitoreo y la investigación del mismo.
Preguntas 5:	Considera que existe duplicidad de funciones en	Si, en algunos casos si, como le mencionaba anteriormente el CCP considero es la unidad más completa que se tienen en la Policía para

	los grupos que realizan investigación contra los delitos informáticos y cibercrimen.	atender todo el tema en cuanto a delitos cibernéticos se refiere y se encarga de realizar investigación a delitos denunciados, así como prevención a los mismos, y si revisamos otras unidades vemos que en DIASE existe también investigación en delitos como los cibersecuestros y en DIPRO existe la prevención de delitos contra menores por medio de las redes, estos dos como ejemplo para tener una idea de que hay otras unidades en la policía atendiendo delitos en el entorno cibernético, los cuales para hacerlo tienen que enfocarse en la prevención, anticipación e investigación, dejando ver que directa o indirectamente si existe la duplicidad en las funciones encomendadas a la policía en contra del cibercrimen

Entrevistador:	Juan Felipe Mantilla Elizalde	
Entrevistado 3:	Capitán Walter Alejandro Linares Guerra Jefe Telemática Dirección de Protección	
	La Dirección de Protección	Respuesta
Preguntas 1:	Que funciones cumple su grupo	El Grupo Contra la Pornografía Infantil, es un grupo de la Dirección de Protección enfocado especialmente a la prevención de los delitos contra menores por medio del cibercrimen, aquellos enfocados a la pornografía infantil, a la extorción, la explotación sexual, el chantaje, las amenazas y la corrupción entre otros.

		Nuestra finalidad está enfocada principalmente a la prevención de los delitos en las redes, prevención que se realiza por medio de campañas en los colegios de educación media y en algunas ocasiones universidades. No obstante, enfocados en la prevención, también se realiza investigación de delitos denunciados por los padres de menores afectados por alguno de los delitos enunciados anteriormente.
Preguntas 2:	Cuantas personas están asignadas a su grupo	El grupo tiene asignados 13 funcionarios en total, de los cuales 1 es oficial, 5 son suboficiales y 7 son patrulleros.
Preguntas 3:	Existen la suficiente la capacitación requerida para fortalecer el perfil del personal	En la gran mayoría de los casos si, el personal que traemos a trabajar al grupo es personal que cumple con un perfil educativo que es acorde al necesitado para cumplir las funciones de prevención e investigación. Para el caso del Grupo Contra la Pornografía Infantil que lo conforman funcionarios con nivel educativo de maestría, especialización y técnicas de investigación, a pesar de tener perfil universitario que hace que sean idóneos en el tema, si hace falta en ocasiones tener mayor oportunidad de retroalimentación y actualización de técnicas y herramientas, así como tener convenios con entidades para fortalecer el perfil de nuestros funcionarios.
Preguntas 4:	Considera que existe duplicidad de funciones en los grupos que	En ocasiones sí, porque nosotros desarrollamos funciones que se que se hacen en todos los grupos de las direcciones, este es el caso de prevenir y de investigar, sin duda son funciones

	realizan investigación contra los delitos informáticos y cibercrimen.	que realizan todos para poder dar solución a los casos que a cada uno les salen, entonces sin nosotros prevenimos o investigamos casos con menores, también lo va a hacer el Cibergaula si de una extorsión se trata, esto para traer un ejemplo.

Entrevistador:	Juan Felipe Mantilla Elizalde	
Entrevistado 4:	Mayor Andrés Felipe Campos Villamil. Jefe Cibergaula	
	La Dirección Antiextorsión y Antisecuestro	Respuesta
Preguntas 1:	Que funciones cumple su grupo	El Cibergaula fue creado para apoyar la labor que realiza la Dirección de Antiextorsión y Antisecuestro, combatiendo directamente los delitos informáticos y la extorción cibernética que emplean los criminales con el fin de pedir a sus víctimas pago a estas extorsiones.
Preguntas 2:	Cuantas personas están asignadas a su grupo	El Cibergaula lo conforman desde el año 2016, 15 funcionarios en diferentes grados y nivel educativo.
Preguntas 3:	Existen la suficiente la capacitación requerida para fortalecer el perfil del personal	Si, el personal integrante del grupo es personal altamente capacitado para el desarrollo de las funciones, en este momento tenemos personal con estudios en maestría, en especialización, ingenieros y otros técnicos investigadores, sumado a este perfil, es para el Gaula una prioridad estar

		capacitando a su personal, es por eso que se cuenta con alianzas estratégicas educativas con universidades y con países tales como Corea del Sur, España y Estados Unidos entre otros.
Pregunta 4:	Considera que existe duplicidad de funciones en los grupos que realizan investigación contra los delitos informáticos y cibercrimen.	Considero que, si existe duplicidad de funciones, pues a pesar de que cada unidad se enfoca en un tipo de delito diferentes, todos finalmente llevan los mismos componentes operativos y de prevención.

Entrevistador:	Juan Felipe Mantilla Elizalde	
Entrevistado 4:	Mayor Jaime Hernán Rojas Parra. Jefe CSIRT PONAL	
	Oficina de Telemática	Respuesta
Preguntas 1:	Que funciones cumple su grupo	
Preguntas 2:	Cuantas personas están asignadas a su grupo	El CSIRT está conformado por 15 policías y una no uniformada para un total de 16 personas, este personal esta distribuidos de la siguiente manera: 3 son oficiales, 8 son suboficiales, 4 son patrulleros y una no uniformada.
Preguntas 3:	Existen la suficiente la capacitación	El personal de este grupo es un personal altamente capacitado puesto que la misma institución se ha encargado de liderar la

	requerida para fortalecer el perfil del personal	manera de hacer de cada uno de ellos funcionarios idóneos, es así como se han entregado becas para capacitar a estos integrantes del CSIRT en temas como maestrías y especializaciones en ciberseguridad y seguridad de la información. En el momento de estos integrantes tenemos 5 con perfil de maestría, 4 con especialización, 4 ingenieros de sistemas y 3 con tecnología en telemática.
Pregunta 4:	Considera que existe duplicidad de funciones en los grupos que realizan investigación contra los delitos informáticos y cibercrimen.	No podría decirle con certeza que tanta duplicidad puede existir en esta labor a nivel interno institucional porque no conozco a fondo la función de los otros grupos, lo que sí podría traer como ejemplo, fue un caso investigativo de un delito informático que se estaba trabajando paralelamente con el CCP y no nos habíamos dado cuenta entonces los dos grupos estaban haciendo este, finalmente al enterarnos, unimos esfuerzos y terminamos de manera más eficiente y oportuna el caso entre los dos grupos.

Análisis:

Por medio del proceso de investigación anteriormente realizado a las unidades de la Policía que desarrollan labores ciber, en compañía de los responsables y comandantes de cada grupo, se logró establecer, que:

- Existen en la PONAL cuatro Direcciones Operativas y una oficina que desarrollan estas labores en el ámbito cibernético, estas unidades son: La Dirección de Inteligencia Policial, la Dirección de Policía Judicial e Interpol, la Dirección Antiextorsión y Antisecuestro, la Dirección de Protección y la Oficina de Telemática.

- Establecer que dentro de las cinco unidades policiales donde desarrollan procesos ciber, existen 16 grupos dedicados a la prevención, investigación, análisis y operacionalización del delito y en algunos casos estos procesos se repiten, lo que demuestra la duplicidad de las labores que realizan en cada unidad, duplicidad que genera desgaste del personal y una no alineación de estrategias que permitan contrarrestar de manera más eficiente el delito.

- Se estableció que se presenta duplicidad de funciones, por parte de los 16 grupos dedicados a la prevención, investigación, análisis y operacionalización del ciberdelito.

Conclusiones

Como resultado de las tres técnicas de recopilación de información se logra establecer que el núcleo del problema se centra en la atomización de los grupos y la duplicidad de la misión de cada uno, pues el común denominador de las funciones fue, la Prevención, Pornografía infantil, la Investigación, el Monitoreo de Redes, Monitoreo del Espectro, el Análisis y los Convenios con otras entidades.

Estos modelos dieron los parámetros para conocer las capacidades actuales de la Policía Nacional dentro de su entorno cibernético, tanto en el personal como en los procesos, cuantas personas especializadas en el tema están ejerciendo estas funciones y que tipo de conocimientos y capacitación tienen estos policiales. Al igual que las

capacidades, se pudo conocer cuáles son las funciones que están realizando estos grupos y por ende con este cruce de información revisar cuales de estas están siendo duplicadas.

La información entregada por los responsables de los procesos deja ver que el personal que actualmente cumple funciones de ciberseguridad en la Policía Nacional suma 117 funcionarios, los cuales están organizados en 15 oficiales, 35 suboficiales, 66 patrulleros y 1 no uniformado lo que permite ver que las capacidades de talento humano con las que se cuenta son bastante altas y favorecen la posibilidad de iniciar la unificación de estas capacidades para la creación de la DICIS.

El personal adscrito a los grupos que cumplen funciones referentes a la ciberseguridad tiene una alta calificación formativa, puesto que se encontró que: 9 tienen título en maestría, 11 en especialización, 18 como mínimo en ingeniería y 53 en tecnologías y cursos de investigación, todas estas capacitaciones a fin con el área de la ciberseguridad y la seguridad de la información.

Se pudo observar que es una prioridad para las unidades mantener en permanente capacitación y actualización al personal que integra estos grupos, ya que según lo informado por quienes los lideran, se tienen convenios con universidades, instituciones nacionales e internacionales de países tales como Estados Unidos, España, Corea del Sur, Chile, Estonia e INTERPOL entre otras para adelantar cursos de capacitación en diferentes aspectos que permitan ser más idóneos en el ámbito investigativo y realizar referenciaciones e intercambio de información.

Se logra establecer que efectivamente el personal de las unidades de la PONAL que cumplen funciones en los aspectos de la ciberseguridad al servicio del país, están enfocados en parámetros similares tales como la prevención, el monitoreo de redes, monitoreo del espectro, análisis, investigación y convenios lo que nuevamente deja ver la posibilidad de integrar todas estas capacidades.

Finalmente, por medio del modelo exploratorio, se encontró y se proyectó una solución, fortalecer y unificar las capacidades investigativas con las que actualmente cuenta la PONAL, para ello se proyecta la estructura orgánica ideal para la unidad que unificará estas funciones, estableciendo parámetros para el desarrollo de las mismas y proyectando el modelo organizacional, estableciendo con exactitud la cantidad de personal necesario estableciendo los cargos y perfiles de la nueva unidad y la capacitación requerida para fortalecer el perfil del personal.

5. Desarrollo del concepto de Ciberseguridad

5.1. Estado del Arte

Hablar de ciberseguridad y ciberdefensa en Colombia, es hablar de temas relativamente nuevos, esto si tomamos como base los hechos de tipo cibernéticos acontecidos en otros países los cuales hoy en día lideran estos esquemas, así como decir también que en nuestro país solo hasta el año 2009 amparados en la ley 1273 "de la protección de la información y de los datos" se comenzaron a juzgar este tipo de prácticas realizadas en la red, prácticas que talvez se cometían antes del año 2009 pero aun así comparados con otros países, siguen siendo relativamente nuevas; sin embargo Colombia ha sido un país resiliente ante este proceso y se ha adaptado rápidamente para hacerle frente al mismo, así como lo han hecho sus entidades gubernamentales para nuestro caso de referencia la Policía Nacional.

Esta realidad ha servido para que, el gobierno colombiano se dé cuenta y entienda la vulnerabilidad en la que se encuentra el país en el tema Ciber, permitiéndole con esto prepararse para organizar estrategias que den paso a contrarrestar este fenómeno; La estrategia principal está dada en el Conpes 3701 (Departamento Nacional de Planeación, 2011) y el Conpes 3854 de 2016 que establece los parámetros de Ciberseguridad y Ciberdefensa, y fija la ruta a seguir en los próximos años con la Política de Seguridad Digital. (Departamento Nacional de Planeación, 2016).

Como parte de estas estrategias, el gobierno establece que, en Colombia tanto en

las entidades públicas como privadas, se deben implementar estrategias para preparar a entidades, sistema judicial, a estudiantes en los colegios, a la Policía Nacional y las Fuerzas Militares buscando de esta manera la protección de los intereses de los ciudadanos al igual que los intereses de la nación. (Departamento Nacional de Planeación, 2016).

¿Cómo afronta la Policía Nacional el tema de la Ciberseguridad en el país?

Para la Policía Nacional, la Ciberseguridad está relacionada directamente a su misión constitucional establecida en el artículo 218 de la Constitución Política de Colombia, y cuya finalidad principal para este documento se basa en la protección de los bienes y honra de las personas en el entorno Cibernético, así como la generación de estrategias de prevención y mitigación de los riesgos, la recepción de las denuncias de incidentes informáticos y la investigación y judicialización de los mismos, asumiendo la decisión dada en el conpes 3701 de 2011.

Por esta razón la Policía Nacional durante los últimos ocho años ha volcado sus esfuerzos en el fortalecimiento de capacidades y adquisición de herramientas que le permitan un control del entorno Cibernético, de tal forma que las estrategias generadas permitan prevenir delitos y a su vez detectar los que sean cometidos por parte de ciberdelincuentes. (Departamento Nacional de Planeación, 2016) (Departamento Nacional de Planeación, 2011).

Dentro del marco de fortalecimiento de estrategias, se han desplegado diferentes actividades tales como, la creación del Centro Cibernético Policial, el Equipo de Respuesta de Incidentes de Seguridad Informática, Cibergaula y el Centro de Capacidades para la Ciberseguridad de Colombia – C4-, así como laboratorios forenses, laboratorios de investigación y la adquisición de herramientas de software y hardware de altas capacidades tecnológicas como instrumentos de apoyo para los investigadores. (Departamento Nacional de Planeación, 2011). (Comando Conjunto Cibernético, 2018) (CC-CSIRT POLICIA , 2018) (Policia Nacioanal-Centro-Capacidades-Ciberseguridad, 2018). Dependencias que son desarrolladas en detalle en la sección de 'La evolución en Ciberseguridad para la Policía Nacional de Colombia'

Basado en las anteriores capacidades, la Policía Nacional logro evidenciar como en el año 2017 el Cibercrimen se incrementó a nivel global en un 28.30% respecto al año inmediatamente anterior, esto hizo que este fenómeno se convirtiera en el reto más grande para los países en el mundo, puesto que las actividades ilícitas físicas mutaron al campo virtual es decir los delitos se convirtieron en ciberataques sofisticados que en su momento no fueron detectados, para el caso de Colombia en solo el 2017, 446 empresas reportaron haber sido víctimas de estas modalidades. (Policia Nacional - Investigación Criminal)

En la medida que aumenta el uso de la red y las redes sociales, aumentan las

víctimas de estos delincuentes, el 55.3% de los incidentes reportados al CCP fueron estafas hechas a los usuarios por medio de la internet, convirtiéndose este como el delito con mayor afectación a los colombianos, esto nos permite entender que el fenómeno cultural que se nos presenta es la falta de conocimiento y el buen usos de la red a la hora de realizar cualquier tipo de transacción llámese compra o adquisición de servicios y esto va de la mano con la falta de educación que tienen los ciudadanos a la hora de dar uso a estos recursos electrónicos. (Centro Cibernetico Policial - Policia Nacional , 2018)

Es así entonces, que para la Policía Nacional los delitos cibernéticos se convirtieron en un reto como parte de la estrategia para afrontar este fenómeno por medio de la prevención y la investigación, generando múltiples estrategias y alianzas de cooperación que han permitido a la Policía Nacional articular esfuerzos con las policías y grupos cibernéticos de otros países, lo cual potencializa y hace más eficiente la investigación y operacionalización de resultados en contra de ciberdelincuentes. (Centro Cibernetico Policial - Capitan Miranda, 2018)

Se resaltan para estas alianzas: la integración y el trabajo conjunto con la Policía Civil Investigativa PID de Chile, la Policía de la Guardia Civil Española, El European Cybercrime Centre de EUROPOL entre los destacados.

Como han afrontado la Ciberseguridad a nivel global en los países del mundo

Entendiendo los países que los delitos que atentan contra la información y los datos ocurren en un territorio sin fronteras (ciberespacio), y así, como que esté ha tenido un desarrollo sin igual en las últimas dos décadas, con el crecimiento de modalidades delictivas insospechadas, los ha obligado a comprender las características y particularidades que especializan este tipo de fenómeno (tiempo, espacio, deslocalización, transnacionalidad, neutralidad, descentralización), con el objetivo de lograr una efectiva persecución, investigación y enjuiciamiento de estos delitos (HERNÁNDEZ, 2014) (LLINARES, 2015). (CISCO, 2018) (Consejo de Europa en Estrasburgo, 2001) (MAYA, 2017) (Naciones Unidas -12° Congreso de las Naciones Unidas Sobre la Prevención del Delito y Justicia Penal , 2010)

En este sentido y de manera general se podría indicar que el ciberespacio, no está situado en un sitio en concreto, sino que, en sentido funcional, está en todos a la vez, pero, en sentido físico, en ninguno, lo que ha generado respuesta de los países, bajo las siguientes estrategias que permitan afrontar el tema más objetivamente:

- Marco de regulación con alcance Internacional. Convenio de Budapest. En la lucha contra el cibercrimen, ya son más de 56 los países que adhirieron al pacto o primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

- Cuerpos de policías internacionales: fuerza policial internacional que tenga el poder necesario para perseguir a las organizaciones criminales que operan en la red. Cada país miembro tendría que cooperar con los demás.
- Cooperación entre empresas y gobiernos.
- Despliegue interagencial: Joint Cybercrime Action Taskforce "J-CAT" del EC3 Europol, INTERPOL, AMERIPOL, Centro Europeo Contra el Cibercrimen EC3 Europol.
- Intercambio de información a nivel mundial y compromiso de la sociedad para identificar, prevenir, detectar, responder y recuperarse de ataques cibernéticos
- Incorporar el término 'resiliencia' los ecosistemas digitales.
- Promoción – concientización de las responsabilidades y beneficios, cuidados, buenas prácticas en el uso del ciberespacio.
- Promulgación de leyes específicas con el propósito de proteger adecuadamente el nuevo bien jurídico de la seguridad de los datos, la información y las funciones de los sistemas informáticos. En el caso de Colombia la Ley 1273 de 2009.

Ahora, en esta lucha de cooperación y articulación de esfuerzo en la lucha contra el cibercrimen de los países, se resalta las contribuciones de los siguientes Organismos y Acuerdos:

- **Organización de los Estados Americanos – OEA** (Organización de los Estados Americanos , 2018).

Con el surgimiento de Internet y la extensión de su uso a nivel masivo en la región durante la última década, surgieron nuevas amenazas y formas de cometer delitos. Con el fin de apoyar a los Estados Miembros en su lucha contra el crimen cibernético, la Organización, a través del Comité Interamericano contra el Terrorismo (CICTE) y del Programa de Seguridad Cibernética, está trabajando en el desarrollo de una agenda sobre seguridad cibernética en las Américas. En cooperación con una amplia gama de entidades nacionales y regionales de los sectores público y privado, tanto en asuntos políticos como técnicos, la OEA fomenta y fortalece las capacidades de seguridad cibernética entre los Estados Miembros a través de asistencia técnica y capacitación, mesas redondas sobre política, ejercicios de gestión de crisis e intercambio de mejores prácticas para el uso de tecnologías de la información y la comunicación. (Organización de los Estados Americanos , 2018)

En la Asamblea General de la OEA en 2004, los Estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04), proporcionando así el mandato que permite a la Secretaría del CICTE trabajar en asuntos de Seguridad Cibernética. La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio. (Organización de Estados Americanos - OEA, 2018)

Entre los principales objetivos de la Secretaría, se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio. (Organización de Estados Americanos - OEA, 2018).

- **Organización del Tratado del Atlántico Norte (OTAN)**

La Organización del Tratado del Atlántico Norte "OTAN" ha tomado acciones respecto a la ciberseguridad de los países integrantes de la organización y consideró que la seguridad de los Estados realmente se encuentra en peligro inminente permanente, al considerar que los ataques a los países y sus ciudadanos puede presentarse de cualquier manera e incluso utilizando como arma cualquier estrategia. Por tanto, los expertos empezaron a considerar que era necesario replantear las políticas de seguridad, puesto que todos los esquemas aparentemente controlados desde la época de la guerra fría estaban totalmente derrumbados, y cualquier cosa podía poner en riesgo la seguridad ya que los ataques no eran necesario hacerlos con armas para causar daño. (OTAN, 2015)

Por tanto, la OTAN replantea su estrategia y crea una política de Ciberdefensa para los países aliados, elaborando y aprobando en el año 2008 por primera vez en la

historia, la Política de Ciberseguridad definiendo tres pilares fundamentales respecto al ciberespacio: (Revista de la OTAN, 2018)

- *Subsidiariedad*: la ayuda se proporciona únicamente ante una petición, y en caso de no haberla se aplica el principio de responsabilidad exclusiva de cada país soberano.
- ***No duplicación***: evitar duplicaciones innecesarias de estructuras o capacidades a nivel internacional, regional y nacional obligando a las naciones a ***unificar sus capacidades*** incluyendo las capacidades con otros países.
- *Seguridad:* una cooperación basada en la confianza, teniendo en cuenta lo sensible que puede ser la información de los sistemas a la que se debe ofrecer acceso, y sus posibles vulnerabilidades.

Posterior a esta política, la Ciberseguridad pasa a ser una actividad fundamental y principal dentro de la Organización del Tratado del Atlántico Norte como lo establece la política de Ciberseguridad Mejorada. En esta política se reafirman ante todos sus integrantes los principios que les asisten respecto a la indivisibilidad de la seguridad de los Aliados, de prevención, de detección, de resiliencia, de recuperación y de defensa, lo cual ***los compromete finalmente a unir esfuerzos en pro de un trabajo de defensa cibernética que propicie la protección cibernética de todos los integrantes de la organización.*** (OTAN, 2015) (Revista de la OTAN, 2018).

Para Colombia, a pesar de no ser una integrante directa de la OTAN, mantiene

una relación con la organización, ya que a partir de este año comenzó a formar parte de las buenas prácticas de esta bajo la figura de socio global, convirtiéndolo en el primer país de Latinoamérica en ser integrante global de esta organización. (Revista de la OTAN, 2018).

Esto permite que Colombia pueda realizar intercambio de conocimientos militares con los países integrantes y dar aplicabilidad a estas estrategias en nuestro entorno Ciber convirtiéndonos en el país de la región con mejores experiencias y capacidades en temas relacionados a la Ciberseguridad.

Igualmente, el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE), publico el "Manual de Tallín" (Tallinn Manual on the International Law Applicable to Cyber Warfare), documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra.

El CCD COE es un Centro de Excelencia que recoge la capacidad de Ciberdefensa de la OTAN, creado en el año 2008, en Tallín (Estonia), y que pretende aunar los esfuerzos de los países que patrocinan el centro: Estonia, Letonia, Lituania, Alemania, Hungría, Italia, Polonia, Eslovenia, España, Holanda y Estados Unidos. Este Manual no es un documento oficial por tanto no refleja la doctrina de la OTAN, ni la postura de las organizaciones o estados representados, ni la del propio centro CCD COE. Es un documento que recoge las opiniones de un grupo de expertos independientes que trabajaron durante 3 años en este tema.

Identifica por un lado el derecho internacional que puede aplicarse a la ciberguerra y, por otro, se establecen 95 normas que deberían regir este tipo de conflictos. Aborda temas como la soberanía, la responsabilidad de los estados, el "jus ad bellum", el "jus in bello", el derecho humanitario internacional y la ley de neutralidad, entre otros. Cada norma definida tiene asociada una explicación que establece la regla de base en tratados y describe cómo el grupo de expertos interpretaría las normas aplicables en el contexto cibernético. También recoge los desacuerdos del grupo en cuanto a la aplicación de cada regla.

- **Unión Europea**

Convenio Sobre la Ciberdelincuencia – Budapest (Consejo de Europa en Estrasburgo, 2001).

Este convenio como se mencionó anteriormente, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Y el cual se basa en cuatro capítulos, en los que además de definirse una serie de terminologías en común, se establecen tres ejes esenciales para hacer frente a los delitos informáticos:

En el primer eje se aborda el tema de los delitos informáticos, y tiene como

objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática. Es decir, en este capítulo se definen los delitos y se los clasifica en 4 categorías:

- Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.
- Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
- Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
- Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

El tercer eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición. La evidencia digital es volátil e intangible, es decir, puede desaparecer o ser alterada muy rápido, por lo que las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas. Para esto, se requiere un proceso penal ágil y eficiente, con esfuerzo organizado por parte de los países. En este capítulo se establece la red 24×7, un punto de contacto que debe funcionar las 24 horas, los 7 días a la semana y asegurar una rápida asistencia entre las partes.

De esta manera, y según se define en el preámbulo del convenio, la armonización en ciberdelincuencia se logra tipificando conductas de delitos informáticos similares en todos los países, unificando normas procesales de cualquier delito que tengan evidencia digital y a través de una cooperación internacional, similar y armónica en todos los países.

A continuación, tomaremos algunos países potencias en ciberseguridad en el mundo como referencia, para ver cómo han afrontado junto con sus entidades gubernamentales las amenazas y los ciberdelitos y que acciones han tomado al respecto las cuales les han servido como punto de partida para que estos países sean efectivos al momento de crear tácticas que permitan evitar acontecimientos a futuro y generar

políticas que les obliga unificar criterios y capacidades en un mismo musculo y una misma líneas, también revisaremos como la PONAL ha migrado y volcado muchas de sus capacidades para generar estrategias de tipo preventivo y operativo ante estos delitos.

1) ESTONIA

Estonia, un país báltico que fue reconocido como el primer país en recibir un ataque de tipo cibernético, tuvo que asumir una realidad para la cual no estaba preparada pero que a la final la dejo convertida en una potencia mundial en ciberdefensa. Por motivos políticos y de tipo étnico luego de mover una emblemática y significativa estatua de bronce de un soldado del ejército ruso, desato un complejo choque el cual termino en un estratégico ataque realizado por Rusia a esta nación.

Este ataque comenzó el 27 de abril de 2007, en donde Estonia fue blanco de enormes ataques cibernéticos los cuales duraron en algunos casos semanas, las páginas de las entidades bancarias colapsaron, al igual que los medios de prensa y algunos organismos gubernamentales y estos debido a un alto tráfico de solicitudes realizadas a las paginas las cuales causaron su bloqueo.

Esto causo que durante semanas los usuarios no pudieran usar cajeros electrónicos o bancos, así como el que los empleados estatales no pudieran trabajar usando medios electrónicos entre otros, este ataque logro colapsar la nación entera por semanas, sin embargo, Estonia aprendió de esto y fue ejemplo a nivel mundial ya que paso a ser un

pequeño país báltico a ser una potencia mundial en temas de ciberdefensa y ciberseguridad.

Este ataque hizo que las acciones tomadas por el gobierno de Estonia hicieran de esta nación una potencia cibernética y referencia a otros países, aquí se integraron todos los organismos del estado con capacidades que permitieron crear un único musculo de defensa del país, así como la creación de un equipo de civiles de más de 25.000 voluntarios que se suman al grupo de defensa del país, lo que le ha permitido a Estonia ser más efectiva en temas de protección cibernética y ciberdefensa.

Como afrontó entonces Estonia los ciberataques y los ciberdelitos:

1) Generando una estrategia nacional cibernética

2) Generando una cultura en los ciudadanos sobre la mentalidad de la seguridad cibernética, tanto en gobierno, como en sector privado y sociedad.

3) Incluyeron en sus marcos educativos, el desarrollo nacional de la educación de seguridad cibernética, generando iniciativas en estas áreas.

4) Generaron conciencia e incluyeron esta responsabilidad a la empresa privada generando la necesidad de invertir en la protección y la seguridad de su información.

5) Generaron un marco legar específico para los delitos cibernéticos.

6) Incorporó tecnologías a sus entidades de seguridad a fin de fortalecer la investigación.

Estonia fue uno de los primeros países en elaborar una estrategia nacional de ciberseguridad. El gobierno actualizó en 2014 su estrategia de 2008, con una versión revisada que cubre el período 2014–17. La estrategia es el documento básico de planificación de la ciberseguridad y un elemento de una estrategia más amplia de seguridad nacional. La nueva estrategia se basa en su predecesora, pero vuelve a evaluar su enfoque a la luz de los cambios en el entorno de las amenazas. La estrategia estonia de ciberseguridad 2014–17 tiene varios objetivos, entre ellos:

- Revitalizar un enfoque integral y de todo el gobierno sobre la ciberseguridad.
- Crear un nivel muy alto de competencia y concienciación sobre la ciberseguridad en los organismos, las empresas y el público.
- Fortalecer la regulación para asegurar los sistemas de información.
- Apoyar los esfuerzos para poner en marcha la cooperación internacional en ciberseguridad.

La estrategia se centra en garantizar la prestación de servicios vitales, aumentando la capacidad del país para combatir la ciberdelincuencia y mejorando su capacidad de defensa nacional. Aunque la tarea se asigna a diversos organismos en el plano nacional, la perspectiva general de Estonia busca evitar la compartimentación de responsabilidades para asegurar una respuesta coordinada en caso de un incidente cibernético nacional significativo. Entre las tareas que define la estrategia se cuentan desarrollar el marco jurídico, mejorar la cooperación internacional y ampliar el número de expertos y soluciones para la ciberseguridad.

Estonia realizó cambios organizativos importantes para brindar apoyo a su estrategia de ciberseguridad. En 2009, se creó un Consejo de Seguridad Cibernética, encargado de apoyar la cooperación entre organismos y supervisar la ejecución de la estrategia, y que depende de la Comisión de Seguridad del Gobierno de la República (un cuerpo ministerial). A la Autoridad del Sistema de Información de Estonia (Riigi Infosüsteemi Amet, o RIA) se le concedieron poderes y recursos adicionales para la protección de las redes públicas. En el seno de la RIA, se creó un Departamento de Protección de las Infraestructuras Críticas de Información.

La RIA llevó a cabo un proyecto de mapeo de infraestructuras críticas para identificar los servicios vitales que dependen de medios cibernéticos y formó una comisión para promover la cooperación público-privada. Las unidades de delitos informáticos de la Dirección de la Policía y la Guardia de Fronteras se fusionaron en 2012. En 2011 se creó una Unidad de Defensa Cibernética como parte de la Liga de Defensa de Estonia, una organización voluntaria de defensa interna2 que lleva su experiencia del sector privado al ámbito público.

El Consejo de Seguridad Cibernética supervisa la aplicación general de la estrategia de ciberseguridad de Estonia y cuenta con el apoyo del Ministerio de Economía y Comunicaciones, que coordina la ejecución de la política de ciberseguridad entre los organismos gubernamentales, la sociedad civil, las empresas privadas y las instituciones educativas. Todos los organismos involucrados en ciberseguridad3 presentan un informe

anual al Ministerio de Economía y Comunicaciones sobre las medidas que hayan adoptado y sus resultados. (Lewis, 2016)

1. ISRAEL

Otro país que nos permite referenciarnos para ver sus capacidades y potenciales cibernéticos es Israel, otra de las potencias cibernéticas del mundo que ha tenido que migrar ante la inminente amenaza que permanece en el ciberespacio en contra de sus entidades estatales, entidades bancarias, plantas de generación de energía e hidroeléctricas entre otras pues es Israel uno de los países del mundo que más ataques cibernéticos recibe a diario, con un aproximado de 100.000 ataques al día.

El aparato de defensa cibernética de Israel es uno de los mejores del mundo. Un estudio comparativo de 23 países desarrollados situó a Israel como el mejor en defensa cibernética, junto con Suecia y Finlandia.1 Pese a ello, tanto las estrategias como la organización siguen evolucionando en el país. Cada día, grupos hostiles a nivel estatal y no estatal ponen a prueba las defensas cibernéticas. Los órganos gubernamentales y las infraestructuras críticas —en particular el sector eléctrico— reciben ataques con regularidad. Las políticas de ciberseguridad de Israel han ido cambiando en respuesta a una mayor dependencia del ciberespacio para actividades políticas, militares y económicas, lo que significa que, sin una ciberseguridad adecuada, un adversario determinado podría frustrar objetivos estratégicos clave sin enfrentarse a Israel con un ejército convencional. Israel resolvió que las estructuras organizativas civiles y militares,

las responsabilidades y la normativa para proteger los sistemas informatizados —que estaban muy compartimentadas— eran insuficientes para permitir una defensa integral en el ciberespacio

Estas situaciones hacen de Israel una nación resiliente al tema cibernético y le permitió afrontar de manera rápida la ciberseguridad adoptando estrategias tales como:

1) Crearon un ciberejercito como la primera línea de ciberdefensa del país.

2) Atraen nuevas ideas con el Cybertech una feria internacional de tecnología cibernética que reúne a más de 5000 expertos al año los cuales dejan en este escenario centenares de ideas de protección.

3) Incentivan la industria cibernética lo que le generado que al día de hoy tengan más de 220 empresas dedicadas a la ciberseguridad.

4) Desarrollaron el gran complejo CyberSpark el cual se dedica al I+D+i militar sobre seguridad cibernética.

5) Generaron alianzas de tipo bilateral en una iniciativa conjunta con Estados Unidos esta definirá estrategias preventivas que permitan bloquear riegos y amenazas que pudieran llegar a atentar contra las infraestructuras críticas de ambos países.

6) En 1997, se puso en marcha el proyecto de gobierno electrónico israelí, denominado Tehila, con el objetivo de proteger la conexión de las oficinas gubernamentales a Internet y ofrecer un alojamiento seguro para los sitios web del gobierno.

7) En 2002, se aprobó la Resolución 84/B del Comité Ministerial de Seguridad Nacional sobre la responsabilidad de proteger los sistemas informáticos en el Estado

de Israel. La resolución se convirtió en la política nacional de defensa cibernética.

8) En 2010, debido al aumento de las amenazas en el ámbito cibernético, el Primer Ministro dirigió la creación de la Iniciativa Cibernética Nacional, un grupo de trabajo para formular planes nacionales con el objetivo de situar a "Israel entre los cinco países más avanzados en el campo cibernético".

9) Crearon la Oficina Cibernética Nacional de Israel (INCB), cuya finalidad era es la de trazar un panorama general de todos los órganos de inteligencia y definir el estado de la situación nacional en materia de ciberseguridad basada en:

- Mejorar la educación, basándose en mejores prácticas de base y una I+D interdisciplinaria avanzada.
- Desarrollar una infraestructura de conocimiento e I+D.
- Crear un "escudo protector" en todo el Estado a partir de los productos de I+D nacional, y hacer frente a los problemas de privacidad.
- Desarrollar una capacidad nacional operativa en el ciberespacio.
- Mejorar la defensa combinando medidas legislativas técnicas y no técnicas y participando en iniciativas internacionales, especialmente con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, para promover la defensa cibernética.
- Implantar tecnologías únicas, desarrolladas a nivel nacional, y fomentar las adquisiciones locales.
- Crear un organismo nacional para la política cibernética integral de Israel.

Como otro de los esfuerzos de Israel para afrontar los delitos cibernéticos en el país, en febrero de 2015, Israel anunció la creación de una nueva autoridad nacional de

defensa cibernética. Sus principales funciones serían las siguientes:

1) Gestionar, controlar y llevar a cabo esfuerzos operativos a nivel nacional para proteger el ciberespacio, gracias a un enfoque sistémico que ofrezca soluciones defensivas completas y constantes frente a los ataques cibernéticos.

2) Operar un equipo de respuesta ante emergencias cibernéticas (CERT).

3) Consolidar y fortalecer la resistencia de la economía mediante medidas de preparación y regularización.

4) Diseñar y poner en práctica una doctrina nacional de defensa cibernética.

5) Realizar las tareas que el Primer Ministro pudiera determinar, en consonancia con la misión designada por la Autoridad.

Según la decisión programada, una Dirección Cibernética Nacional incluiría las sedes cibernéticas nacionales, como unidades independientes en la Oficina del Primer Ministro. La autoridad tendrá la responsabilidad de lograr sus objetivos y llevar a cabo su misión, mientras que las sedes cibernéticas nacionales dirigirán los ámbitos de la política y la estrategia nacional sobre competencia cibernética y reforzarán el papel de Israel en cuanto país a la vanguardia mundial en el campo de la ciberseguridad. (Lewis, 2016)

Todos los anteriores con una única finalidad y es la de unir las ideas y capacidades en temas cibernéticos generando una línea de defensa, basada en la unión de capacidades militares y civiles en pro de la defensa nacional.

2. RUSIA

Otra de las potencias se trata de Rusia, de quienes se puede establecer que cuentan con uno de los ciberejercito más poderosos del mundo, tras la ola de ataques recibidos por parte de Estados Unidos e Israel a sus instalaciones atómicas, Rusia desde el 2010 ha doblado y centralizado sus capacidades en la organización y fortalecimiento de un ciberejercito, el cual se dedica específicamente al espionaje, ciberataques que puedan causar daño físico a la infraestructura de otros países y las guerras informativas en los medios de comunicación y redes sociales.

Según las cifras entregadas por el presidente ruso, para el año 2016 las pérdidas que dejaron los ataques en la red superaron los 2 billones de dólares y de acuerdo a la proyección, se dice que para el año 2022 estas podrían superar los 8 billones de dólares, estas otras razones de peso, ha hecho que Rusia afronte estos flagelos con decisiones tales como la de tener su propia red la cual, según los expertos en ciberseguridad de ese país, es inalienable e incorruptible.

Pero para llegar Rusia al top de las potencias cibernéticas del mundo es debido a la manera como ha afrontado los ciberdelitos y los ciberataques que ha recibido y sus entidades de seguridad especialmente la policía ha asumido esta responsabilidad con acciones contundentes, Rusia ha generado estrategias tales como:

1) Ha creado su propia red, la cual han hecho blindada y niveles de seguridad

muy altos, con monitores permanentes haciendo de esta una red inalienable.

2) La policía y las entidades del estado encargadas de la ciberseguridad trabajan en equipo y alianza con las empresas privadas las cuales se especializan en la ciberseguridad.

3) Su ciberejercito dejo de ser defensivo para ser ciberatacante.

4) Por parte del Servicio Federal de Seguridad de Rusia (FSB) fue creado un centro nacional que coordinará la lucha contra los ataques cibernéticos a la infraestructura crítica del país, dentro de las funciones que le dan a este grupo son:

- Coordinación "en temas de detección, alerta y erradicación de las consecuencias de ataques computarizados".
- Intercambio de información entre las instituciones especializadas y con los colegas extranjeros.
- Análisis de los recientes ataques cibernéticos y generación de métodos para enfrentarlos.

5) Se generaron leyes específicas enfocadas al juzgamiento de ciberdelincuentes, con el fin de ser más drásticos con quienes cometan este tipo de delitos.

6) Hizo una alineación legislativa con otros países con el fin de evitar que delincuentes cometan los ciberdelitos en Rusia y se refugien en otra nación.

7) Unificaron esfuerzos con INTERPOL y el G7 con el fin de realizar trabajos en equipo y de esta manera ser más eficiente.

3. COREA DEL NORTE

Corea del Norte debido a la permanente tensión en la que vive con su vecino país, ha tomado la decisión de afrontar la ciberseguridad de manera ofensiva, la postura de ciberseguridad de la refleja el desafío que se plantea. El ciberespacio se ha convertido en un nuevo escenario de conflicto en la península coreana. La creciente capacidad cibernética de Corea del Norte hace que se esfuerce por mejorar su seguridad cibernética. El Libro Blanco de la Defensa de la República de Corea de 2014 subraya que "Corea del Norte cuenta en la actualidad con unos 6.000 soldados de guerra cibernética y lleva a cabo una guerra cibernética, que incluye la perturbación de operaciones militares y ataques contra las grandes infraestructuras nacionales con el fin de causar una parálisis psicológica y física en el Sur". 1 según un informe de 2015, los ataques cibernéticos procedentes de Corea del Norte han acarreado daños económicos para el vecino del sur que ascienden a 800.000 millones de won (US$706 millones).

Estas acciones han llevado a Corea a buscar estrategias y generar líneas de ruta para afrontan de manera eficiente los temas relacionados con su ciberseguridad y su ciberdefensa, estas estrategias iniciaron con la creación del Plan Maestro de Ciberseguridad que se basa en tres pilares: la inversión en capacidades de seguridad, el desarrollo de un marco jurídico y la cooperación internacional. Las tareas emprendidas en su puesta en práctica se agrupan en cinco planes de acción:

- Establecer un sistema de respuesta conjunta de los sectores privado, público y militar.

- Fortalecer la seguridad de las infraestructuras críticas y mejorar la protección de los secretos. Detectar y bloquear los ataques cibernéticos a nivel nacional.
- Poner en marcha medidas disuasorias contra la provocación cibernética y fortalecer la cooperación internacional.
- Crear infraestructuras de ciberseguridad.
- Corea tomo la decisión de unir sus capacidades (Ministerio de Defensa Nacional, el Cibercomando Militar de Corea, Ministerio de Ciencia TIC, la oficina de Planificación del Futuro, el Servicio Nacional de Inteligencia y el Ministerio de Seguridad y Administración Pública, con el único fin de ser realizar un trabajo conjunto que les permitiera ser más efectivos y fuertes en la aplicación de la ciberseguridad y la ciberdefensa de su país.

Su estrategia abarca todos los sectores entre esos el educativo, pues en los temas de formación en ciberseguridad, ha tomado el liderazgo el gobierno mediante las instituciones educativas públicas y en estas ha creado pensum enfocado a la ciberseguridad, así como la universidad de Corea ha creado el Departamento de Defensa Cibernética que es la facultad encargada de esta línea educativa. Pero no se queda solo en el sector público, si bien es cierto que el tema es liderado por el estado, el sector privado está vinculado en esta responsabilidad con el fin de hacer frente al déficit de profesionales en diversas disciplinas tales como ciencia forense digital, biorreconocimiento, aplicación de RFID/USN para la seguridad y consultoría sobre seguridad de la información.

4. ESTADOS UNIDOS

Estados Unidos tiene un complejo conjunto de normas, instituciones y políticas para administrar el desafío de la ciberseguridad. Las iniciativas comenzaron hace casi 20 años, en la década del noventa, pero en los últimos seis años ha surgido un enfoque compacto e integrado. Las autoridades estadounidenses consideran a las amenazas cibernéticas como la principal amenaza estratégica a la que se enfrenta el país.1 Estados Unidos ha experimentado una campaña continua de espionaje económico y delitos financieros a través de Internet y se enfrenta a un riesgo de ataques a sus infraestructuras y servicios críticos. Las pérdidas para la economía estadounidense se elevan a miles de millones de dólares cada año. El último año ha sido particularmente difícil, con ataques coercitivos dirigidos contra Sony Pictures, el Casino Sands y Github, un servicio de alojamiento. Estados Unidos ha detectado que diversos países han examinado su infraestructura crítica en busca de vulnerabilidades con vistas a un ataque cibernético.

Otra de las iniciativas del gobierno estadunidense fue la unión de capacidades dándole paso en el año 2006, a la creación del primer ejército cibernético del mundo, marcando un hito en materia militar, el Comando Cibernético de la Fuerza Aérea Norteamericana, su lema " alcance mundial, vigilancia mundial y poderío mundial" se crea tras la unificación de las capacidades existente en las fuerzas del estado, trayendo sus mejores hombres en el tema para integrar este nuevo cuerpo que sin duda sería para proteger el quinto esquema de ataque, el ciberespacio.

Para el Pentágono fue claro que era necesario unificar las capacidades que se tenían en una sola fuerza cibernética que les permitiera potencializarlas y a su vez convertirse en la primera potencia mundial, pues es claro para ellos mantener el control del ciberespacio y así evitar cualquier tipo de atentado de tipo militar o terrorista como el ocurrido el 11 de septiembre.

Lo anterior permite observar que Estados Unidos ha sido un país que permanentemente es victimizado por el espionaje, el robo de información y todo tipo de delitos informáticos, motivos por los cuales a generados estrategias para afrontar estos delitos por medio de sus autoridades de la siguiente manera:

1) Directiva de Decisión Presidencial 63 (PDD-63), que recomienda a los organismos que tomen todas las medidas necesarias para garantizar la continuidad y la viabilidad de las infraestructuras críticas y la PDD-63 creó la figura de un Coordinador Nacional para la Seguridad, la Protección de las Infraestructuras y el Contraterrorismo.

2) Creo el Centro de Integración de Inteligencia contra la Amenaza Cibernética y Ciberterrorismo (CTIIC, en sus siglas en inglés), agencia centrada en las amenazas cibernéticas, cuya tarea será integrar y analizar información de inteligencia para tratar de evitar ataques en la red. (EFE Agencia, 2015).

3) Crearon alianzas público-privadas que incorporaban al sector privado en temas de seguridad nacional con la guía del gobierno.

4) Creación del Centro de Análisis e Intercambio de Información único.

5) Crean en el 2008 la Iniciativa Integral de Ciberseguridad Nacional (CNCI) Entre sus atribuciones se encuentran:

- La gestión de las redes del gobierno de manera unificada mediante el programa "Trusted Internet Connections".
- La puesta en marcha de sistemas de detección y prevención de intrusiones en todo el gobierno.
- La coordinación de los esfuerzos en I+D.
- La conexión de los centros federales de operaciones cibernéticas.
- El desarrollo y la aplicación de un plan de contrainteligencia cibernética que abarque a todo el gobierno.
- El aumento de la seguridad de las redes confidenciales.
- La expansión de la educación cibernética.
- El desarrollo de estrategias y programas de disuasión.
- La gestión de riesgos de la cadena de suministro.
- La definición del papel del Gobierno federal en materia de ciberseguridad de las infraestructuras críticas.

Estados Unidos es un país líder en tecnología y ciberseguridad de la información. La ciberseguridad se ha convertido en una prioridad de inversión tanto para el gobierno como para el sector privado. El pasado año, empresas de capital de riesgo invirtieron más de US$1.000 millones en ciberseguridad. Diecisiete empresas de capital de riesgo de Silicon Valley se centran en el desarrollo de tecnologías innovadoras de ciberseguridad, y el año pasado invirtieron en más de 230 millones en ciberseguridad. La Agencia de

Proyectos de Investigación Avanzados de Defensa y la Fundación Nacional de Ciencias realizaron también importantes inversiones en I+D en el campo de la ciberseguridad. (Lewis, 2016)

El Gobierno de los Estados Unidos creo la Centro de Integración de Inteligencia contra la Amenaza Cibernética y ciberterrorismo (CTIIC, en sus siglas en inglés), agencia centrada en las amenazas cibernéticas, cuya tarea será integrar y analizar información de inteligencia para tratar de evitar ataques en la red. (EFE Agencia, 2015).

La nueva entidad, ha tomado el modelo para desarrollar su labor al Centro Nacional de Contraterrorismo, puesto en marcha tras los atentados del 11 de septiembre de 2001. Así, el CTIIC recolecta inteligencia, sino que integra y analiza la recopilada por otras agencias gubernamentales para detectar amenazas cibernéticas y prevenir ataques. Además, se propuso una ley que impulse al sector privado a compartir información sobre amenazas cibernéticas con el Gobierno, quien a cambio proporciona protección legal a las empresas bajo ciertas condiciones. (EFE Agencia, 2015).

Teniendo en cuenta lo anterior los países buscan dar respuesta a la naturaleza del carácter transnacional del delito cibernético, a la necesidad de cooperación estrecha entre países para dar respuestas oportunas en el tiempo dadas la naturaleza volátil de las pruebas, así como armonizar las leyes ante tales delitos. Y apoyando uno de estos tres pilares donde se fundamenta el presente trabajo, la unificación y articulación de esfuerzos y capacidades de la Policía Nacional definidos en la creación de la Dirección de

Ciberseguridad – DICIS, y que de manera particular con enfoque al personal -talento humano suficiente y necesario para su vital funcionamiento.

Como ha afrontado Colombia la cibercriminalidad

La respuesta de Colombia ante este gran fenómeno ha sido muy positiva, aunque el tema es relativamente nuevo en nuestro país como se mencionó anteriormente, aun así Colombia se ha destacado como uno de los países con una madurez intermedia para afrontar el ciberdelito en la región, esto según el informe ¿Estamos preparados en América Latina y el Caribe?, (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016) donde el BID y la OEA presentaron a las autoridades el Informe Ciberseguridad 2016, que muestra que la región de Latinoamérica es altamente vulnerable ante posibles ciberataques. Los participantes identificaron la necesidad de contar con apoyo de los organismos internacionales para sensibilizar a los líderes políticos y a los ciudadanos, construir capacidades y unir esfuerzos en los equipos de gobierno, así como formular y fortalecer las estrategias nacionales de Ciberseguridad.

El Informe Ciberseguridad 2016 es la primera radiografía profunda del nivel de preparación de América Latina y el Caribe ante la creciente amenaza del cibercrimen, para lo cual se estudiaron 49 indicadores distribuidos en cinco áreas: política y estrategia, cultura y sociedad, educación, marco legal y tecnología.

El análisis de la situación de 32 países de la región revela que cuatro de cada cinco países no tienen estrategias de Ciberseguridad o planes de protección de la infraestructura crítica. En la mitad de los casos, los países carecen de un mecanismo coordinado de respuesta a incidentes cibernéticos, y dos de cada tres no cuentan con un centro de comando y control para una acción coordinada en la prevención, detección y atención de incidentes de seguridad cibernética.

Asimismo, en la gran mayoría de los países, las fiscalías carecen de capacidad para perseguir los delitos cibernéticos, entre otras necesidades.

Uruguay, Brasil, México, Argentina, Chile, Colombia y Trinidad y Tobago se encuentran en un nivel intermedio de madurez, pero lejos de países avanzados como Estados Unidos, Israel, Estonia, Rusia y la República de Corea.

Dado lo anterior, durante los últimos años el gobierno ha venido fortaleciéndose por medio de estrategias generadas para la protección del ciberespacio, este trabajo comprende el desarrollo de políticas tales como el Conpes 3701 en el cual se aborda una estrategia para afrontar las diferentes amenazas, a las que se encuentran significativamente expuestas las entidades del país, mediante la inclusión del tema "Ciberdefensa y Ciberseguridad" en el Plan Nacional de Desarrollo, que busca fortalecer las capacidades del Estado y mitigar el impacto de dichos ataques. Además, menciona las leyes y organismos con los cuales se debe apoyar la Nación, para realizar la gestión del manejo de respuesta a incidentes. (Wilson Bernardo Guerrero Romero). (Departamento Nacional de

Planeación, 2011).

El objetivo principal del documento Conpes es el fortalecimiento de la capacidad del estado para enfrentar las amenazas que atentan contra su seguridad y defensa, basado en las tres problemáticas que se identificaron en el país: (Wilson Bernardo Guerrero Romero). (Departamento Nacional de Planeación, 2011).

1) Falta de coordinación en operaciones de Ciberseguridad y Ciberdefensa: se habla de una falta de concientización, transmisión y cultura en el manejo seguro de la información en sectores públicos, privados y sociedad civil.

2) Falta de personal capacitado en especialidades de Ciberseguridad y Ciberdefensa: en el momento de la presentación del documento, se evidencia un déficit en la educación de los temas descritos, por esta razón muchas de las personas interesadas se veían obligadas a obtener estos conocimientos a nivel extranjero, pero por ser un recurso más costoso, no tenía un acogimiento representativo y esto conllevaba a la perdida de casos por el mal manejo en procedimientos como la cadena de custodia.

3) Debilidad en la regulación y legislación de la protección de la información de los datos: se reflexiona a la legislación que se tenía en el momento y que a partir de esta debe ser modificada, basados en los lineamientos a nivel mundial como la de la convención del Consejo de Europa en delitos cibernéticos, que establece una cooperación judicial.

Ahora planteadas las problemáticas se definen y se llevan a cabo soluciones respectivamente, como: (Wilson Bernardo Guerrero Romero). (Departamento Nacional de Planeación, 2011).

1. Conformar tres instancias (COLCERT, CCP, CCOC) con las cuales no se contaban en la realización de dicho documento (CONPES 3701), a continuación, un gráfico referente a la implementación de dichas instancias.

Ilustración 1. Modelo de Coordinación Ministerio de Defensa, 2011, Fuente: Conpes 3701.Figura No. 01

Esquematizado de diferente manera:

Ilustración 2. Modelo de Coordinación Ministerio de Defensa, 2011, Fuente:(Mayor MILENA ELIZABETH REALPE DIAZ - Jefe de Prospectiva y Cooperación del Comando Conjunto Cibernético - CCOC , 2017)

Destacándose la orden de fortalecer las capacidades investigativas y operativas ante delitos cibernéticos de la Policía Nacional, dando pasó a la creación del Centro Cibernético Policial (CCP) y el Grupo de respuesta a incidentes Informáticos de la Oficina de Telemática (CSIRT). (Wilson Bernardo Guerrero Romero). (Departamento Nacional de Planeación, 2011).

2. Capacitación especializada a funcionarios que estén relacionados actualmente con la Ciberseguridad y Ciberdefensa y básicamente con el manejo y atención a incidentes de seguridad. El COLCERT cuenta con el apoyo del Comité Internacional Contra el Terrorismo (CICTE). En la actualidad a parte de la gran cantidad de esfuerzos de la Nación, también están un sin número de entidades que se preocupan por las mismas problemáticas y de esta manera universidades y organizaciones prestan el servicio de

capacitación y socialización de los mismos temas, tales como la Cámara Colombiana de Informática y Telecomunicaciones, La Escuela de Guerra con la primera Maestría en Ciberseguridad y Ciberdefensa, la OEA con programas de Seguridad Cibernética y cooperación en materia de Delitos Cibernéticos, entre otros.

3. Para la solución de la tercera problemática se encaminaron esfuerzos en la búsqueda de herramientas judiciales para la efectiva prevención, investigación y judicialización de los delitos cibernéticos, para lo cual el documento hace referencia al siguiente marco legal.

- Ley 527 de 1999 comercio electrónico: donde se reglamenta el uso y acceso de mensajes de datos, comercio electrónico y firmas digitales, además de establecer cuáles son aquellas organizaciones que pueden certificar dichos procesos.
- Ley 599 de 2000: en el capítulo VII, articulo 192 violación ilícita de comunicaciones. menciona que el que ilícitamente substraiga, oculte, extravié, destruya, intercepte, controle o impida una comunicación privada dirigida hacia otras personas o entidades, serán privados de la libertad y si además se revela el contenido, o lo emplea en provecho propio este tiempo se duplicara
- Ley 962 de 2005 denominada ley anti tramites: esta ley se caracteriza por incentivar el uso de la tecnología para aquellas organizaciones del estado o similares que realizan procedimientos de servicios públicos.
- Ley 1150 de 2007: en esta ley se establece que para la contratación con los recursos públicos se deben realizar mediante el sistema electrónico de contratación pública (SECOP).

- Ley 1273 de 2009: quizás la más importante hasta el momento en cuanto a sistemas informáticos se refiere, ya que con esta se modifica el código penal por el concepto de ley de la protección de la información y de los datos. En los cuales se tipifican los siguientes casos; acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicación, interceptación de datos, informáticos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales. Ministerio de Interior y de Justicia, Ley 1273 de 2009, Bogotá, 2009.
- Ley 1341 de 2009: se definen conceptos y principios sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC). (Ministerio de las Tecnologias de la Información y las Comunicaciones, 2018)
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009: establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet, de implementar modelos de seguridad que cumplan con los principios de confidencialidad, integridad y disponibilidad de los datos y elementos de red, así como medidas para autenticación y no repudio. (Comision de Regulacion de Comunicaciones , 2018)
- Circular 052 de 2007 (Superintendencia Financiera de Colombia): establece los estándares mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. (Departamento Nacional de Planeación, 2011).

Todo lo anterior trajo consigo que la conciencia social sobre la importancia de la

privacidad y la seguridad en Internet y la confianza en los sistemas digitales del país haya crecido notablemente, en parte debido a las campañas nacionales, como en la campaña "en TIC Confío" del MinTIC. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

De igual forma el desarrollo de educación de seguridad cibernética nacional ha experimentado un crecimiento notable y los foros público-privados y centros de excelencia financiados por el gobierno han comenzado a gestarse en el país. Numerosas universidades, organismos policiales y de defensa y las empresas privadas ofrecen cursos y capacitaciones, incluyendo maestrías y programas de acreditación. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

En esta evolución el Conpes 3854, propone como objetivo general que los ciudadanos, las entidades del Gobierno y los empresarios conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

La idea es educar y fomentar una cultura en todos sea conscientes de que el manejo del riesgo es responsabilidad de todos. En este sentido los mayores logros de esta política han sido.

- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

- 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.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Y de manera específica y de forma sobresaliente se evidencian los siguientes logros, entre otros:

- Adhesión de Colombia al convenio Budapest (20-06-2018), el Congreso de la República aprobó de manera unánime la ley de adhesión al Convención de Budapest, la cual deberá contar con la sanción presidencial. El Convenio del Consejo de Europa sobre la ciberdelincuencia, también conocido como Convenio de Budapest, es el primer tratado internacional que hace frente a los delitos informáticos y en internet, y que se enfoca en dos frentes: fortalecer o dar un marco de regulación a los delitos cibernéticos, y la cooperación internacional.

- La importancia de que Colombia se encuentre en este Convenio es que facilitará la adopción de medidas para detectar y perseguir, tanto en territorio nacional como internacional, a los posibles ciberdelincuentes. (Ministerio de Relaciones Exteriores, 2018).

- Policía Nacional inaugura el Centro de Capacidades para la Ciberseguridad de Colombia 'C4'. El 'C4' se creó con apoyo del Ministerio de las

Tecnologías de la Información y las Comunicaciones, el cual desarrolla cuatro enfoques principales para contrarrestar el delito: (Policia Nacioanal-Centro-Capacidades-Ciberseguridad, 2018).

1. Prevención: a través del 'CAI Virtual', se busca la interacción con ciberusuarios y la gestión de más de incidentes informáticos, así como realizar el ciberpatrullaje en la red y en la 'Deep Web' o red oculta, difundiendo alertas de ciberseguridad mediante las redes sociales Twitter y Facebook, que son las más usadas por los cibernautas.

2. Ciberinvestigación: se implementarán las actividades de prevención y articulación con la Fiscalía General de la Nación. Además, busca generar investigaciones, que arrojen la materialización de capturas.

3. Informática Forense: para apoyar las investigaciones forenses, este laboratorio se implementará con herramientas especializadas que extraen evidencias digitales de los dispositivos de almacenamiento de datos para la investigación criminal.

4. Relacionamiento Estratégico: a través de la propuesta del relacionamiento interinstitucional busca establecer alianzas con 26 entidades en el ámbito nacional, con el sector financiero, con organismos internacionales como Europol e Interpol y redes sociales como Google, Facebook y Twitter.

Las capacidades dispuestas en el Centro de Capacidades para la Ciberseguridad de Colombia 'C4' hacen parte del componente estratégico de la Policía Nacional para la reducción del delito. (Policia Nacioanal-Centro-Capacidades-Ciberseguridad, 2018).

- La Escuela de Guerra gradúa a la primera promoción de la Maestría en Ciberseguridad y Ciberdefensa del país. Este programa hace parte de los acuerdos de colaboración entre esta entidad académica y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con los cuales se busca fortalecer las capacidades en materia de seguridad digital. (www.gobiernoellinea.gov.co, 2018).

- Conformación de "Reunión de Infraestructura Critica Cibernética, Riesgo Operacional y Ciberdefensa. El Plan Nacional de Protección y Defensa de la Infraestructura Crítica Cibernética del Sector Gobierno es un instrumento que en desarrollo de la Política Nacional de Seguridad Digital, establece el marco de actuación y de operaciones para la protección y defensa de la Infraestructura Crítica Cibernética de Colombia en todas las Entidades que hacen parte del Sector, con el objeto de garantizar los servicios esenciales del Estado y contribuir a la paz, la prosperidad económica y social del país, la protección de la ciudadanía y del entorno digital. (Comando Conjunto Cibernético, 2018).

Conformación de Cibercomandos y Creación de Unidades Cibernéticas: Fuerzas espaciales de guerreros ciberespaciales, capaces de reaccionar ante lo que consideren una amenaza cibernética. Y entre sus funciones se encuentran: (Mayor MILENA ELIZABETH

REALPE DIAZ - Jefe de Prospectiva y Cooperación del Comando Conjunto Cibernético - CCOC , 2017) (Ciberoperaciones - Héctor Gómez Arriagada, 2013)

- Integración de capacidades de Ciberdefensa
- Operaciones Conjuntas en el Ciberespacio
- Investigación, Innovación y desarrollo en Ciberseguridad y Ciberdefensa
- Ciberdefensa de la infraestructura critica.

Ilustración 3. Unidades Cibernéticas en Colombia. Fuente: (Mayor MILENA ELIZABETH REALPE DIAZ - Jefe de Prospectiva y Cooperación del Comando Conjunto Cibernético - CCOC , 2017)

Finalmente, teniendo en cuenta los avances Tecnológicos y la incorporación de estos en la sociedad, es ineludible que Colombia continúe su actuar para proteger las múltiples partes interesadas - multi-stakeholder (Gobierno nacional y los territoriales, Organizaciones, públicas y privadas, Fuerza Pública, Los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, Academia, Sociedad civil) (Departamento Nacional de Planeación, 2016), en el ciberespacio, y la cooperación con aquellos países que se encuentren a la vanguardia frente este fenómeno, así como con organismos internacionales como la OEA, OTAN, BID, entre otros, para que como país y región cada vez estemos más preparados.

Evolución en Ciberseguridad en la Policía Nacional de Colombia

Historia y Misión La Policía Nacional (PNC) fue creada el 5 de noviembre de 1891. Esta Fuerza es un cuerpo armado permanente de naturaleza civil a cargo de la Nación, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz. (Ministerio de Defensa Nacional, 2016)

La Policía Nacional soportará su servicio sobre dos áreas misionales: Convivencia y Seguridad Ciudadana y Seguridad Pública, orientando sus esfuerzos a disminuir de manera significativa los delitos, factores de violencia y problemáticas que afectan la seguridad de los ciudadanos tanto en el ámbito urbano como rural, contribuyendo al fortalecimiento del control territorial y la acción integrada del Estado; igualmente, en la prevención de la atomización y mutación de los fenómenos delincuenciales, la lucha contra el crimen organizado y transnacional, además, de la desarticulación de economías ilícitas como el narcotráfico, el terrorismo y la minería ilegal. (Ministerio de Defensa Nacional, 2016)

> Al mismo tiempo, incrementará sus actividades de cooperación internacional y consolidará las relaciones policiales con organismos de seguridad homólogos, manteniendo el liderazgo policial en la Región. El desarrollo institucional requerirá de un incremento de capacidades relacionadas con el crecimiento del talento humano, la ampliación y modernización de su infraestructura, la adquisición de sistemas de información, así como de medios logísticos, técnicos y tecnológicos, con miras a

garantizar una mejor cobertura territorial, un servicio de policía efectivo y una atención más próxima al ciudadano. (Ministerio de Defensa Nacional, 2016)

Adicionalmente, será necesario continuar con el fortalecimiento del Modelo Nacional de Vigilancia Comunitaria por Cuadrantes y los medios de inteligencia e investigación criminal, con el fin de optimizar la acción preventiva, de control e investigación de la totalidad de las especialidades policiales –infancia y adolescencia, seguridad vial, seguridad rural, protección al medio ambiente, antinarcóticos, secuestro y antiextorsión, cibercrimen y Ciberseguridad. (Ministerio de Defensa Nacional, 2016)

Esta sección refleja una contextualización cronológica sobre los procesos y alcances relacionados con la Ciberseguridad en la Policía Nacional de Colombia, iniciando con los estándares instaurados al interior de la institución y el desarrollo de la misionalidad en la sociedad. Se mencionan estrategias frente a la administración del talento humano de la institución como principal actor de riesgo en el tratamiento de la información; de igual manera se señalan las acciones normativas y estructurales para la formación de los policías y el control efectivo de la información, así como la creación de organismos en pro de garantizar la seguridad en ciberespacio.

La Policía Nacional comprende el concepto de Ciberseguridad y lo incorpora en sus objetivos estratégicos, así como alineada a las mejores prácticas internacionales y exigencias dadas, evoluciona a: (POLICIA NACIONAL - DIPON - OFITE -ARADI, 2011).

Los importantes avances logrados por la Policía Nacional de Colombia en materia de seguridad de la información, se ven reflejados en la certificación otorgada por Instituto Colombiano de Normas Técnicas (ICONTEC) para el Sistema de Gestión de Seguridad de la Información (SGSI) en siete unidades policiales, acorde a la norma ISO/IEC 27001:2013; lo que ha permitido extender a todo nivel la implementación de políticas y controles a la información producida y utilizada por cada una de las actividades misionales desarrolladas por los funcionarios que laboran en las unidades de la Policía Nacional. (Rodríguez, 2017)

A nivel Interno y externo.

- La organización comprende que el conocimiento es producto del tratamiento y transformación de la información por ende se convierte en el activo sobre el cual se fundamentan sus objetivos estratégicos.
- Conforma un equipo altamente capacitado y calificado para diseñar, implementar, medir y monitorear el SGSI.
- Conciencia de la necesidad de Inversión en herramientas y capacitación para el equipo de trabajo del SGSI.
- Establece una política en materia de seguridad de la información, apoyada por la Alta Dirección.
- Establece un modelo maduro de continuidad y recuperación ante eventos e incidentes de seguridad.

Donde se asume la política nacional de seguridad digital, un enfoque a riesgos.

Seguridad = Gestión del Riesgo

- Identificar los activos de información más valiosos para la organización.
- Los dueños de la información son quienes la producen, NO la Dirección de Tecnología.
- Análisis de riesgo sobre activos de información.
- Decisiones gerenciales sobre el riesgo.
- Planes de mejora, sobre riesgos materializados.

Problemática

- Incremento de eventos registrados
- Evolución de técnicas de hacking.
- Pérdidas millonarias en organizaciones.
- Aumento de incidentes relacionados con alteración de sitios públicos en el sector público y privado y denegación de servicio.
- En 2011 se tienen registrados más de 1000 casos de cibercrimen. (Acceso abusivo a sistema informático, Interceptación de datos informáticos, daño informático, uso software malicioso, violación de datos personales, suplantación de sitios web).

Una vez identificada la problemática se plantean objetivos generales, teniendo en cuela misión de la entidad y su compromiso en el Conpes 3701 de 2011.

- Fortalecer la capacidad del Estado para hacer frente a las amenazas que atentan contra su seguridad y defensa cibernética.
- Crear un ambiente y las condiciones necesarias para brindar protección en el ciberespacio.
- Creación de directrices para el desarrollo y la promoción de la seguridad y defensa cibernética.
- Articular las capacidades y los mecanismos para identificar y establecer las acciones y responsabilidades para prevenir, preparar, servir, gestionar, recuperar y responder a cualquier amenaza.
- Crear conciencia y sensibilizar a la ciudadanía sobre todos los asuntos relacionados con la seguridad de la información.

Una vez definidos los objetivos el primer compromiso es con la Institución, consistente el lograr concientización o cultura organizacional tendiente a la salvaguarda de la información y los datos.

Siendo la empresa más grande del país.

- 186.000 empleados
- Incorporación anual de 10.200 funcionarios
- Retiro anual de 4.500 funcionarios
- Población flotante de 27.000 auxiliares de policía
- Presencia en 8368 sitios en el territorio nacional

Múltiples fuentes de información

- + 25.000 equipos de cómputo.

- + 50.000 radios de comunicación.
- + 74 sistemas de información.
- Intercambio de información con diferentes entidades nacionales e internacionales.

- **Centro Cibernético Policial – C.C.P.**

Ahora basado en lo anterior, y fortaleciendo las capacidades de la Policía Nacional, y acogiendo el Conpes 3701 de 2011, se establece el C.C.P Centro Cibernético Policial. 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.

Ilustración 4. Interfaz Gráfica Centro Cibernético Policial, fuente: Policía Nacional de Colombia –Centro Cibernético Policial.

Modelo de coordinación, con las entidades u organizamos que se crean bajo el Conpes 3701 de 2011.

Ilustración 5. Modelo de coordinación, Fuente. Policía Nacional.

- **Equipo de Respuesta a Incidentes CSIRT-PONAL** (CC-CSIRT POLICIA , 2018)

Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la 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.

Cuya misión es garantizar las condiciones necesarias para el aseguramiento de la plataforma tecnológica de la Policía Nacional, como apoyo a la estrategia de ciberseguridad y Ciberdefensa de la Nación y sus objetivos son:

- Proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones en general, en la protección de amenazas y/o incidentes informáticos.
- Consolidar los procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas.
- Activar los mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.
- Establecer alianzas estratégicas con organismos nacionales e internacionales, entidades públicas y privadas, para afianzar los mecanismos de ayuda mutua en materia de seguridad de la información.
- Fomentar la concienciación en el manejo de la información y la implementación de las políticas de seguridad de la información.
- Generar estrategias de divulgación para suministrar un sistema de alertas tempranas, anuncios y comunicados que permitan prevenir los riesgos asociados a la seguridad de la información.
- Promover en las organizaciones públicas y privadas la creación e integración de esquemas de atención de incidentes de seguridad CSIRT.

- **CAI Virtual**

Luego, para dar respuesta a los incidentes de ciberseguridad, la Policía Nacional implementó el "@caivirtual", (Policia Nacional - Informe 'Amenazas del Cibercrimen en Colombia 2016-2017', 2017) que nace en el año 2007 como primera iniciativa online de

atención policial contra el delito cibernético en Latinoamérica, y garantiza una respuesta inmediata a los requerimientos de los ciudadanos 24/7, ello como respuesta a los nuevos retos y metas ambiciosas para convertir a la Policía Nacional en el referente frente a las policías de América, con el fin de tener un ente controlador del ciberespacio en la institución, la Policía Nacional dispondrá de un equipo dedicado a la seguridad de las TICs ayudando a las organizaciones a mitigar y a evitar los incidentes graves de seguridad de la información. Estableciendo las siguientes funciones:

- Identificación de actividades que generan riesgos o amenazas a los sistemas de información.
- Desarrollar estrategias de mitigación y respuesta.
- Establecer canales de comunicación de confianza.
- Proporcionar una alerta temprana a las poblaciones de posible afectación.
- Notificar a otros entes dentro de la Internet, de los posibles problemas de seguridad.
- Seguimiento y control de esta información para determinar las tendencias y estrategias a seguir.
-

Para ello define la siguiente estructura.

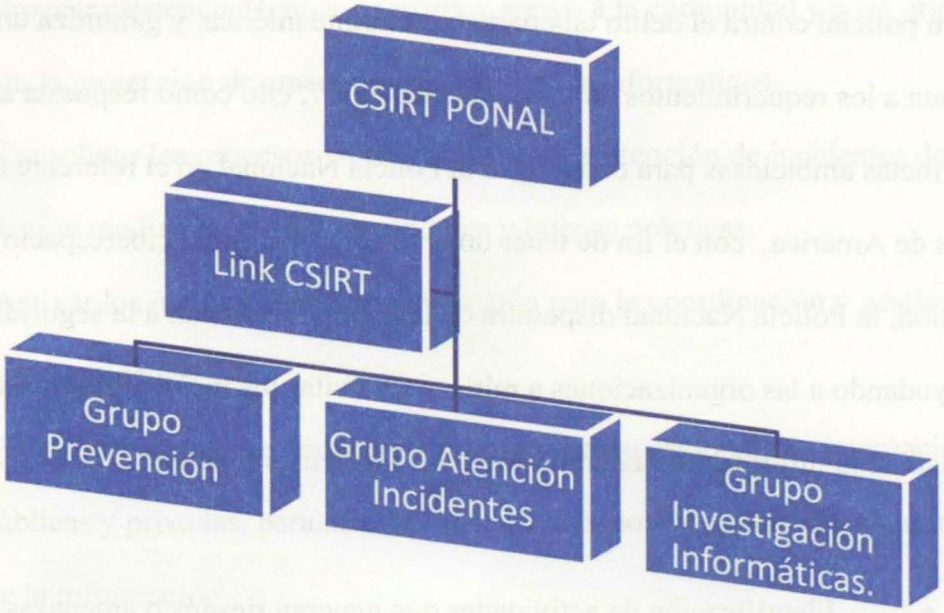


Ilustración 6. Estructura orgánica CSIR, fuente Policía Nacional.

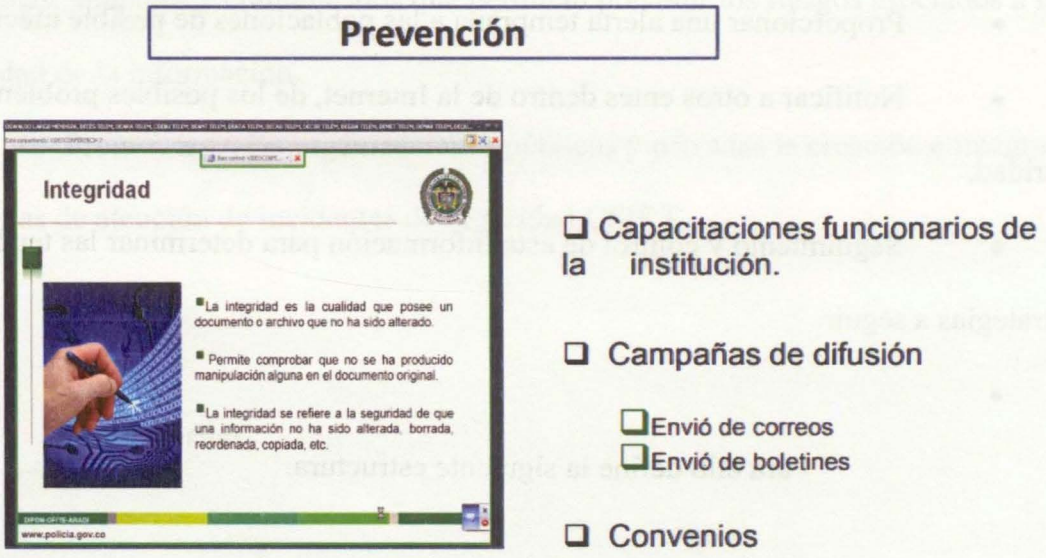
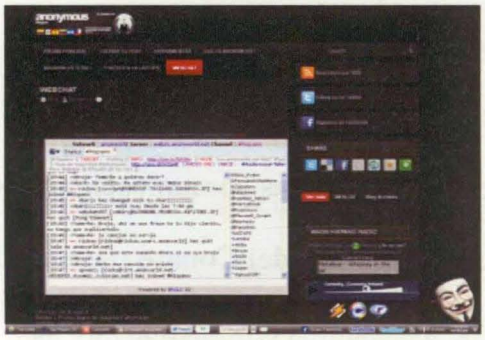
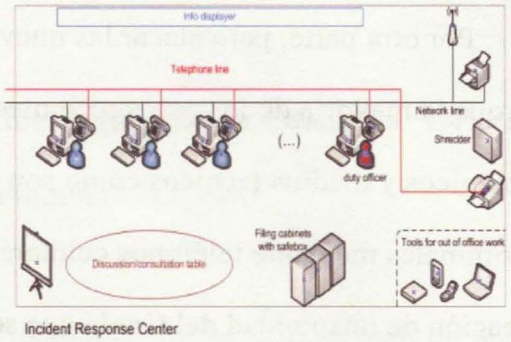


Ilustración 7. Visualización proceso Prevención, fuente: Policía Nacional.

Atención de incidentes

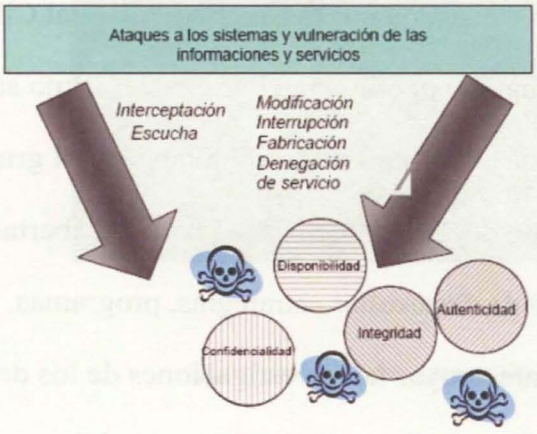




- CSIRT ponal.csirt@policia.gov.co
- Atención a Incidentes

Ilustración 8. Visualización proceso Atención Incidentes, fuente: Policía Nacional

Grupo de Investigación



- Investigación y desarrollo de Gestión de Incidentes.
- Monitoreo

Ilustración 9. Visualización proceso Grupo de Investigación, fuente: Policía Nacional.

- **Cibergaula**

Por otra parte, para atacar las nuevas modalidades en el delito del secuestro, y dado que la mayoría de los casos recientes se han resuelto con el apoyo de equipos tecnológicos y medios técnicos como son las interceptaciones de las comunicaciones de los criminales mediante teléfonos celulares, la Secretaría Técnica del Conase recomendó la creación de una unidad del Gaula que se ocupará de los asuntos cibernéticos de las investigaciones. Esto se oficializo, en la apertura del primer congreso de Grupo de Acción Unificada por la libertad Personal (Gaula) 2013, la creación y puesta en funcionamiento del Cibergaula de la Policía Nacional. Los cibergaulas implementan la tecnología para combatir los delitos informáticos y la extorsión cibernética que emplean los criminales, aprovechando y robando información detallada de los usuarios. (www.webinfomil.com, 2015).

Para ello se expidió la resolución Número 2040 del 20 de marzo del 2015, por medio de la cual se crea el Grupo de Acción Unificada por la Libertad Personal Ciber Gaula. Con esta resolución se dio la conformación operativa del grupo, así como sus características y los bienes e insumos que esta unidad manejaría. La misión del grupo está determinada de la siguiente manera: El Grupo de Acción Unificada para la Libertad Personal "CIBER GAULA" es el encargado de desarrollar estrategias, programas, proyectos y demás actividades requeridas para apoyar las investigaciones de los delitos de secuestro y extorsión, en los cuales se utilice el ciberespacio como canal de comunicación. Asimismo, como la realización de acciones de prevención, inteligencia e investigación criminalística que permita identificar, recolectar, preservar y analizar la

evidencia digital y fortalecer la atención a las víctimas y sus familias. (Resolución 2040 del 20 de marzo del 2015).

- **Centro de Capacidades para la Ciberseguridad de Colombia 'C4',** (Policia Nacional - Centro-Capacidades-Ciberseguridad-Colombia-C4, 2018)

Complejo de más de 5.000 metros cuadrados, donde se enfocarán los esfuerzos para luchar contra los fraudes informáticos, el ciberterrorismo y la pornografía infantil en Internet, entre otros delitos que utilizan la red como escenario, y que se constituye en el complejo más grande de Latinoamérica para combatir crímenes cibernéticos.

Ilustración 10. Inauguración 'C4', Fuente: Policía Nacional.

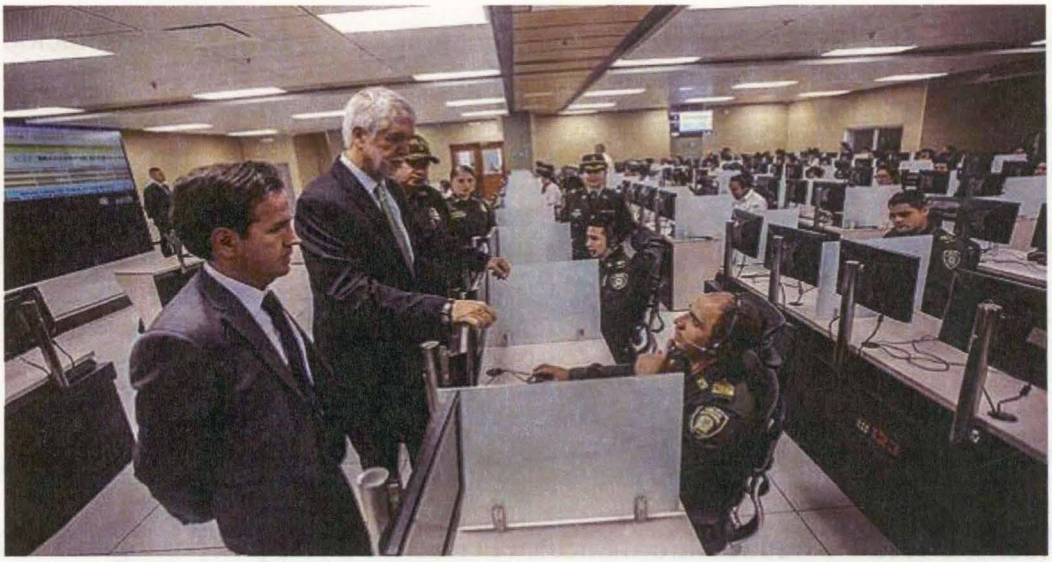


Ilustración 11. Inauguración 'C4', Fuente: Alcaldía Mayor de Bogotá.

El objetivo del 'C4' es robustecer la seguridad de los colombianos y del Estado en el entorno digital y optimizar la lucha tendiente a erradicar los fraudes informáticos, el ciberterrorismo a infraestructuras, la pornografía infantil en Internet, entre otros.

El 'C4' se creó con apoyo del Ministerio de las Tecnologías de la Información y las Comunicaciones, el cual desarrolla cuatro enfoques principales para contrarrestar el delito:

1. Prevención: a través del 'CAI Virtual', se busca la interacción con 453.000 ciberusuarios y la gestión de más de 26.000 incidentes informáticos, así como realizar el ciberpatrullaje en la red y en la 'Deep Web' o red oculta, difundiendo 15.767 alertas de Ciberseguridad mediante las redes sociales Twitter y Facebook, que son las más usadas por los cibernautas.

2. Ciberinvestigación: se implementarán las actividades de prevención y articulación con la Fiscalía General de la Nación. Además, se busca generar más de 100 investigaciones, que arrojen la materialización de capturas. Este tipo de control, que ya se ha venido realizando, ha dejado cerca de 56 capturas por abuso infantil, logrando también el bloqueo de 15.767 páginas con contenido de pornografía infantil.

3. Informática Forense: para apoyar las investigaciones forenses, este laboratorio se implementará con herramientas especializadas que extraen evidencias digitales de los dispositivos de almacenamiento de datos para la investigación criminal. Como antecedente de esta práctica, se destaca el apoyo a las operaciones 'Albania' y 'Tormenta' donde se analizaron más de 15 Terabytes de información.

4. Relacionamiento Estratégico: a través de la propuesta del relacionamiento interinstitucional busca establecer alianzas con 26 entidades en el ámbito nacional, con el sector financiero, con organismos internacionales como Europol e Interpol y redes sociales como Google, Facebook y Twitter.

> Las capacidades dispuestas en el Centro de Capacidades para la Ciberseguridad de Colombia 'C4' hacen parte del componente estratégico de la Policía Nacional para la reducción del delito. (Policia Nacional - Centro-Capacidades-Ciberseguridad-Colombia-C4, 2018)

- **Despliegue Interagencial** (Policia Nacional - Informe 'Amenazas del Cibercrimen en Colombia 2016-2017', 2017)

- Centro Europeo Contra el Cibercrimen EC3 Europol La Policía Nacional de Colombia se ha vinculado a los diferentes grupos de expertos (Focal Point) del EC3 desde el año 2014, participando en operaciones contra la ciberdelincuencia transnacional y el crimen organizado en sus diferentes blancos. Permitiendo un despliegue de capacidades técnicas y humanas para enfrentar estas amenazas globales, fortaleciendo la cooperación policial internacional.

- Joint Cybercrime Action Taskforce "J-CAT" del EC3 Europol: El grupo de tarea conjunta contra el Cibercrimen es una iniciativa del EC3 de Europol, que consta de (13) oficiales de enlace expertos en Cibercrimen, cuya responsabilidad, es liderar y articular acciones conjuntas contra redes cibercriminales transnacionales. La participación de Colombia data desde el año 2015 siendo nuestro país el único representante de Latinoamérica en esta mesa de expertos en Europol.

- INTERPOL La presidencia del Grupo de jefes de unidades para la lucha contra la ciberdelincuencia en la región de América Latina, ha permitido, a la Policía Nacional de Colombia, liderar acciones conjuntas de prevención y articulación operacional con los homólogos policiales en la región, asimismo el uso eficiente de los canales de cooperación policiales con esta agencia nos ha permitido mejorar los tiempos de respuesta ante solicitudes de apoyo investigativo en la región.

- AMERIPOL A través de la unidad nacional de Ameripol en Colombia, se está articulando las capacidades tecnológicas para enfrentar la amenaza del Cibercrimen a nivel continental, siendo Colombia, un referente en el despliegue de acciones operativas contra el fraude por medios informáticos, la lucha contra el contenido de abuso sexual infantil en línea y otras amenazas de carácter informático como el Ransomware y Botnets en la región.

- **ACADEMIA** (Policia Nacional - Escuela de Telematica, 2018)

Finalmente, sin dejar al lado la academia la Policía Nacional a través de la Escuela de Tecnologías de la Información y las Comunicaciones "Teniente Coronel Jorge Luis Mauledoux Barón", y quien tiene como misión capacitar y especializar mediante programas de pregrado y posgrado en telemática al talento humano de la Institución, para satisfacer las exigencias tecnológicas y soporte en los sistemas de comunicación que presentan las unidades policiales en todo el territorio Nacional, realiza lanzamiento y convocatoria de la Maestría en Ciberseguridad e Informática Forense abierta el 08 de julio de 2018. (Policia Nacional - Dirección Nacional de Escuelas , 2018)

- **Unidad De Investigación Criminal De Infancia Y Adolescencia** (Policia Nacional - Infancia -Adolecencia, 2018).

Unidad de Investigación Criminal de Infancia y Adolescencia, fue creada el día 24/08/2011 Bajo la resolución 02980 del SUDIR-DIPRO, y nace de la necesidad de

enfrentar las nuevas modalidades y evolución que tuvo la criminalidad y más para el Delito de pornografía con persona menor de 18 años Art 218 C.P

- **Propuesta de la Creación de la Dirección de Ciberseguridad - DICIS.**

Propuesta de Unificación de todos los Grupos que realizan anticipación, prevención, atención e investigación de todo tipo de conductas delictivas en el entorno Ciber. Y de manera específica para este documento una definición de funciones, grupos y procesos del personal de la DICIS y los cargos, perfiles de la Dirección de Ciberseguridad. Cada una de estas secciones corresponde a los objetivos planteados para dar respuesta a la pregunta de investigación definida. El actual documento reafirmó el hecho que la mayoría de las funciones ya se realizan en la institución, pero no existe una integración entre ellas, lo que lleva a que se presente duplicidad de funciones y limitaciones en la definición de estrategias que abarquen todas las conductas que puedan afectar al ciudadano en el ciberespacio.

Planeación por capacidades en el dominio del ciberespacio en la Policía Nacional.

Surge un nuevo concepto, 'Planeación por capacidades' en el cual se basa la Visión del Futuro de las Fuerzas Armadas (Ministerio de Defensa Nacional, 2016), el Plan Estratégico del Sector Defensa y Seguridad – Guía de planeamiento estratégico 2016-2018 (Ministerio de Defensa , 2016) y se alinea con el Plan Nacional de Desarrollo

PND 2.014 – 2.018 (Departamento Nacional de Planeación , 2014), en su estrategia de Seguridad, Justicia y Democracia para la construcción de la paz, lineamiento de modernización y fortalecimiento de las instituciones de Seguridad y Defensa, y en el cual la Policía Nacional estructura sus posibles desarrollos basados en este.

Para un mejor entendimiento se detalla a continuación, y se resalta que sobre la aplicación de este concepto se estructura la propuesta del dimensionamiento del personal (cantidad y perfiles) necesarios para la conformación de la Dirección (Dirección de Ciberseguridad- DICIS) que articulara todas las capacidades existentes en la investigación criminal en el ciberespacio y delitos que afecten la salvaguarda de la protección y datos.

Transformar de acuerdo con las Capacidades

Un elemento fundamental del ejercicio de Transformación y Futuro de la Fuerza Pública 2030 es la introducción del concepto de capacidad para la planeación estratégica. Una capacidad está definida como la habilidad para desarrollar una tarea bajo ciertos estándares (como tiempo, ambiente y nivel de alistamiento específicos), a través de la combinación de diferentes medios y modos. Una capacidad está en función de cinco componentes (Doctrina, Material y Equipo, Personal, Infraestructura y Organización) y requiere de todos ellos para ser efectiva. (Ministerio de Defensa Nacional, 2016)

Ilustración 12. Componentes de una capacidad. Fuente: Ministerio de Defensa Nacional.

La metodología de planeación por capacidades lanzada por el Misterio de Defensa Nacional, da fuerza y piso a la propuesta de este trabajo donde se plantea integrar las capacidades cibernéticas en la PONAL, esto teniendo en cuenta que esta metodología articula la estrategia con la planeación de presupuesto y adquisiciones, lo anterior teniendo en cuenta todos los procesos internos de la institución, permitiendo de tal manera una respuesta por parte de la Fuerza Pública acorde a las características del entorno estratégico. Además, la articulación entre estrategia y adquisiciones permite hacer un seguimiento de como los proyectos de la Fuerza Pública aportan al cumplimiento de la estrategia del sector. (Ministerio de Defensa Nacional, 2016)

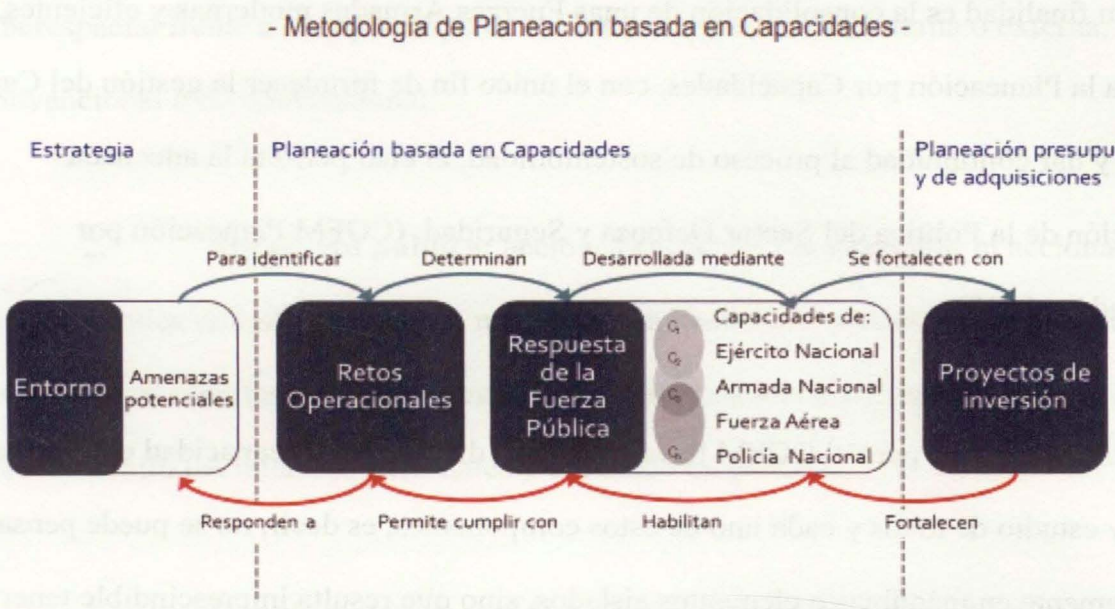


Ilustración 13. Metodología de Planeación basada en Capacidades. Fuente CGFM.

Este es un ejercicio realizado en las entidades de maneras diferentes, y está basado en el entendimiento de las fortalezas, herramientas y perfiles con los que se cuentan, para de esta manera proyectar metas a mediano y largo plazo, las cuales sean alcanzables, permitiendo a las entidades planear y desarrollar actividades de acuerdo a las capacidades que se tengan para este fin, y no planificar de manera dimensionada con referencia a las capacidades con las que se cuenta. (CGFM Planeación por Capacidades., 2017).

Este planear que básicamente es la elaboración y establecimiento de un plan conforme a la búsqueda del poder desarrollar alguna actividad. De igual forma este desarrollo de actividades debe estar ligado a el conjunto de capacidades con las que se cuentan, que se basan en herramientas tecnológicas, talento humano (personal) con sus diferentes perfiles y proyecciones, logrando de esta manera establecer una planeación de acuerdo a las capacidades con las que cuenta. (CGFM Planeación por Capacidades., 2017)

Su finalidad es la consolidación de unas Fuerzas Armadas modernas y eficientes, se consolida la Planeación por Capacidades, con el único fin de fortalecer la gestión del Capital Humano y dar continuidad al proceso de sostenibilidad, el cual permita la adecuada financiación de la Política del Sector Defensa y Seguridad. (CGFM Planeación por Capacidades., 2017)

Es por eso que para el CGFM llevar a cabo el diseño de una capacidad es necesario el análisis y estudio de todos y cada uno de estos componentes, es decir, no se puede pensar exclusivamente en máquinas o elementos aislados, sino que resulta imprescindible tener una visión integral de los medios y recursos que incluya la educación, el entrenamiento, la infraestructura, la actualización de la doctrina, y la organización, entre otros.

En este proceso del Ministerio de Defensa Nacional, la Planeación por Capacidades, definió ocho áreas misionales las cuales serán el fundamento de verificación de cada uno de los grupos y sus respectivas capacidades, que permitan establecer cuál será la tarea específica de acuerdo a sus capacidades tácticas, operacionales y de talento humano. (CGFM Planeación por Capacidades., 2017)

Las definiciones de estas áreas misionales son:

1. **Defensa Nacional:** acciones encaminadas a proteger la soberanía e integridad territorial en los dominios terrestre, marítima, fluvial, aérea, espacial y

ciberespacial frente a cualquier tipo de amenaza o agresión sea interna o externa, convencional o no convencional.

2. **Seguridad pública:** acciones encaminadas a asegurar el accionar de la Fuerza Pública en todo el territorio nacional para neutralizar y desarticular los actores ilegales y sus manifestaciones conexas organizadas nacionales y transnacionales que atenten contra los intereses nacionales y el Estado en general.

3. **Convivencia y seguridad ciudadana:** acciones encaminadas a garantizar los derechos, libertades, desarrollo social y proyección humana, con esfuerzos coordinados con las autoridades político-administrativas, que satisfagan las necesidades de los habitantes.

4. **Gestión del riesgo:** acciones en apoyo a la prevención, atención y mitigación del riesgo de desastres a nivel nacional e internacional.

5. **Cooperación internacional:** participación de las FF.MM. en organismos multilaterales y de cooperación internacional.

6. **Protección de los recursos naturales y del medio ambiente:** acciones propias y para prestar apoyo a las autoridades ambientales, a los entes territoriales y a la comunidad, en la defensa y protección del medio ambiente y los recursos naturales

renovables y no renovables, en las funciones y acciones de control y vigilancia previstas por la ley.

7. **Contribución al desarrollo del país:** acciones en campos como el transporte, la construcción, las telecomunicaciones y la tecnología e innovación, que permitan promover el papel de las Fuerzas Militares en el desarrollo económico y social de la Nación.

8. **Gestión, apoyo y desarrollo proyectivo:** proveer funciones comunes de dirección, administración y gestión en el Sector Seguridad y Defensa para el desarrollo de la infraestructura logística, desarrollo tecnológico, gestión del talento humano y potenciación del conocimiento, así como garantizar la legitimidad de las acciones de las Fuerzas Militares.

Ilustración 14. Definición de áreas misionales. Fuente: Ministerio de Defensa.

Integración de diferentes cuerpos de Seguridad para responder a los delitos del Ciberespacio

A continuación, se exponen ejemplos de diferentes países de como integraron los diferentes cuerpos de seguridad para responder a los delitos del ciberespacio.

- **Centro para la Ciberseguridad e Investigación del Cibercrimen -CIC:** Institución dedicada a la investigación científica de las tendencias cibercriminales con el fin de coadyuvar a las autoridades a contrarrestar el cibercrimen y los delitos informáticos.

- **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 de España**, responsables de combatir la ciberdelincuencia. (Grupo de Delitos Telemáticos Unidad Central Operativa, 2011)

- **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).

- **CTIIC (*Cyber Threat Intelligence Integration Center*,** traducido "Centro de Integración de Inteligencia contra la Amenaza Cibernética") EEUU. 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.

- **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.). 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).

- **IGCI / Singapur.** 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.).

- **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).

- **AMERIPOL:** Se encuentra conformada por 33 cuerpos de Policía e Instituciones homólogas y 26 Organismos Observadores, quienes aportan conceptos trascendentales en forma permanente. (AMERIPOL -Comunidad de Policias de America, s.f.)

- **G.A.T. / Guardia di Finanza / Italia**: **Grupo Anticrimen Tecnológico — hacker y cracker):** La Guardia di Finanza es una fuerza especial de policía que forma parte de las Fuerzas Armadas de Italia. Es un cuerpo militar dependiente directamente del Ministro de Economía y de Finanzas y del servicio de seguridad pública del Ministerio del Interior.

Desarrolla tareas de policía judicial y seguridad pública en el ámbito económico y financiero. Con su Grupo G.AT. desarrolla investigaciones contra crimen tecnológico – hacker y cracker. (Guardia Di Finance, s.f.)

- **Fiscalía General de la Nación/Colombia:** Entidad que 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 el Grupo pericial e investigativo de Informática Forense a nivel central que tiene por competencia, conocer investigaciones y casos adelantados por la ley 1273 de 2009 y 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. (Fiscalía General de la Nación, 2018)

6. Propuesta de Solución a la Problemática Planteada

6.1. Implementar para la Dirección de Ciberseguridad – DICIS, Tablas TOP Como Herramienta de Solución a la problemática planteadas

Basado en los capítulos o secciones anteriormente expuestas, finalmente se plantea la estructuración de las tablas TOP, en pro de garantizar el personal idóneo y suficiente en el cubrimiento del talento humano en la creación de la Dirección de Ciberseguridad – DICIS.

Para el año 2008 la PONAL inicia un fuerte trabajo alineado a la optimización del talento humano, tarea que buscaba la ubicación del personal de acuerdo a necesidades reales establecidas por los cargos que cada unidad debería tener de acuerdo a sus funciones y misionalidad. De acuerdo a esta estrategia, se crean para la Policía las Tablas de Organización Policial (TOP) cuya misión sería la de estandarizar las cantidades mínimas requeridas de personal en cada cargo asociado a las unidades policiales, identificando la cantidad de vacantes y/o remanentes por dependencias y determinando las necesidades de personal a nivel nacional. (Policia Nacional - PONAL).

Así como contar con una distribución equitativa, eficiente del personal, que permita realizar un trabajo efectivo en cuanto a las diferentes necesidades institucionales. Con las TOP se gerencia el talento humano, se proyectan los programas educativos y de formación de la Policía en capacidades específicas, se mantiene controlados los recursos y se puede establecer que labor debe realizar cada funcionario, adicionalmente permite establecer

perfiles, lo cual da la posibilidad de enfocar de la mejor manera la tarea de cada policial cumpliendo con su perfil y competencia. (DINAE Policía Nacional de Colombia , 2018)

La aplicabilidad de estas TOP se establece por medio de cinco funciones:

Ilustración 15. Funciones de la TOP, Fuente: Policía Nacional.

El fortalecimiento de las Tablas de Organización Policial inicia para el año 2013, con la construcción de la TOP en cada unidad policial, buscando con esto el despliegue de la política a nivel nacional, igualmente con la validación de las TOP por parte de los dueños de proceso logrando con esto el empoderamiento de cada comandante de unidad para mostrar sus necesidades reales en cuestión de personal y de esta manera tener claridad en la cantidad de funcionarios por proceso.

Durante los años 2014 a 2016, se realiza la reestructuración del módulo de perfiles y cargos por competencias generando la segunda versión del manual de funciones alineando la TOP de cada unidad, la implementación del Manual de Funciones establecida mediante la (Resolución No. 00937), la sistematización de las TOP en el Módulo de perfiles de cargos por competencias, se formaliza la resolución No. 05309 por la cual se establecen las TOP, se diseña y formaliza el formato de la Tabla de Organización Policial (2PP-FR-0010), se procede al bloqueo por Orden Interna para que el nombramiento de personal no exceda el mínimo requerido de TOP y se implementa y verifica el personal que no se encuentra parametrizado y esta como remanente.

Como apoyo integral a la estrategia organizacional del talento humano en la policía mediante las TOP, se trabajaron dos líneas estratégicas, la primera de ellas el Plan de Desarrollo Individual PDI y la segunda el Plan de Carrera.

El Plan de Desarrollo Individual, es la herramienta que le permite al funcionario potenciar los aspectos susceptibles de mejora, demandados por el perfil del cargo, logrando identificar las debilidades de cada funcionario, las cuales son entregados a la Dirección Nacional de Escuelas como insumo para el Plan Institucional de Capacitación (PIC).

El Plan de Carrera permite dinamizar el Modelo de Gestión del Talento Humano y Cultura Institucional, articulando sus componentes de tal forma que es posible definir rutas de desempeño a las que puede acceder un profesional de policía a lo largo de su vida institucional, logrando un engranaje armónico entre las políticas y objetivos de la Policía

Nacional y el proyecto de vida profesional de cada uno de los funcionarios.

Su objetivo primordial es permitir un mejor gerenciamiento del talento humano, con el fin de brindar una guía clara y sencilla respecto a las rutas de desempeño laboral que puede seguir un policía a través de su vida profesional en la institución; teniendo en cuenta la formación, capacitación, habilidades y experiencia, en concordancia con la misionalidad del servicio de policía

Teoría Organizacional

Hablar de clima organizacional en una empresa, entidad o institución es el valor principal que existe para las mismas, las organizaciones como simples organizaciones carecen de sentido pues el solo entorno físico sin el talento humano que permita generar ese clima organizacional no funcionaria. En este contexto la Policía Nacional, desde el año 2009 ha volcado un gran esfuerzo por darle una organización a su talento humano, organización que permita además de capacitar su personal, ubicarlo por cargos y perfiles en los puestos a fin con sus capacidades

Según Richard L Daft en su libro *Teoría y Diseño Organizacional* (Daft, 2015), asegura que el manejo de las teorías organizacionales en las empresas, permiten generar tendencias en las administraciones reconociendo la importancia del personal, dando paso a nuevos enfoques, nuevas ideas que den oportunidades a contribuir en el logro de grandes objetivos con un trabajo en equipo realizado por personas capacitadas, y para esta labor es responsabilidad de la

administración de las organizaciones, que se realicen las estrategias que permitan generar tendencia a la importancia del talento humano y a su vez el que esté ubicado donde corresponde de acuerdo a sus perfiles y competencias.

Para Richard L Daft, deben existir tres componentes fundamentales organizacionalmente en una empresa o institución: (Daft, 2015).

1. Una estructura organizacional designa relaciones formales de subordinación, como son la jerarquía y el tramo de control de los gerentes y supervisores. Para el caso de la PONAL, este se define claramente, entendiendo que la institución está estructurada jerárquicamente por grados y de acuerdo a este se definen las áreas y cargo a ocupar para su dirección.

2. La estructura organizacional identifica el agrupamiento de individuos en departamentos y el de departamentos en la organización total. En la PONAL esta clave se ve desarrollada en la estructura orgánica que se maneja, encontrando que existen las Direcciones, Los Comandos de Departamentos de Policía, Las Metropolitanas de Policía y las Oficinas Asesora, y cada una de ellas maneja internamente su estructura orgánica la cual permite tener en un segundo plano las áreas, las oficinas asesoras y los diferentes grupos operativos de acuerdo a la especialidad, cada uno de estas con su jefe, comandante o coordinador los cuales despliegan igualmente responsabilidades de acuerdo al grado, perfil y conocimiento de cada funcionario.

3. Según Gareth R. Jones los cargos por perfiles que permiten establecer la teoría organizacional establecen para este fin el desarrollo de cuatro líneas estructurales necesarias para

la proyección del cargo de cada empleado de acuerdo a sus competencias y el perfil.

En primer lugar, realizar un diagnóstico que permita determinar con que personas se cuentan para ocupar los cargos existentes en la organización, así como quienes quieren y tienen la motivación para ocuparlos. Este diagnóstico debe permitir estar revisando los procesos y su desarrollo con el fin de hacer las nivelaciones correspondientes a los cargos y quienes los ocupan.

Realizado el diagnóstico, la segunda línea estaría basada en la estructuración formal de los perfiles y las responsabilidades que se le asignarán a cada uno luego de ocupar el cargo, esta estructuración debe ir paralela a la claridad que se debe tener sobre cuáles son los objetivos de la organización y a donde se quiere llegar de tal manera que se engranen cargos con perfiles logrando con esto una cohesión entre el funcionario y la organización.

Posterior al diagnóstico viene el ajuste con el cual se lleva a cabo la nivelación de la totalidad de los empleados y sobre la repercusión del nuevo cambio. También se incluirán entrenamientos acelerados para aquellos trabajadores que ocupen cargos que sufran cambios importantes y se finaliza implantando los nuevos cargos que se hayan hecho necesarios de acuerdo a las metas trazadas y objetivos planteados.

Finalmente, la última etapa establece la aplicación del proceso de mejora continua, permitiendo con esta realizar una retroalimentación sobre la eficiencia y la eficacia lograda con la aplicación de cargos por perfiles y competencias, así como los requerimientos que se le podrán

disponer al funcionario una vez asignada su responsabilidad y si se requiere hacer medición a los resultados obtenidos durante sus procesos laboral.

Basado en lo anteriormente descrito, se inicia con el análisis de las capacidades en el talento humano de los grupos existentes con relación directa en la prevención, investigación y judicialización de los delitos que atenten contra los datos y la información, o cometidos en el ciberespacio.

Análisis de las capacidades actuales en el talento humano del Centro Cibernético Policial - CCP, CSIRT, CiberGaula, Seccion de CiberInteligencia y Criptoanálisis –SECYC, Grupo contra la Pornografía Infantil DIPRO.

El alcance de este análisis es evidenciar que grupos o áreas existen, que funciones desempeñan y cuales capacidades académicas e investigativas ostentan los funcionarios de policía que se desenvuelven en la actualidad en los roles de seguridad de la información, por tal razón se va a realizar un análisis en cada una de las áreas y grupos, como lo son Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL (CCP), Grupo de respuesta a incidentes Informáticos de la Oficina de Telemática (CSIRTPONAL), Grupo CiberGaula de la Dirección de Antisecuestro y Extorsión (CIBERGAULA), Sección de CiberInteligencia y Criptoanálisis de la Dirección de Inteligencia Policial, (SECYC) y el Grupo Contra la Pornografía Infantil de la DIPRO.

- **Centro Cibernético Policial – CCP**

El CCP "Es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada de desarrollar estrategias, programas y proyectos para la Ciberseguridad, Ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal." (Ministerio de Defensa Nacional, Policía Nacional-Dirección General, 2015), a la cual le fueron asignadas funciones relacionadas con:

1. Contar con la capacidad de detección (Ciberpatrullaje 24/7 en la web), prevención, investigación, análisis, correlación, frente a crisis informática y planes de contingencia.
2. Judicialización de las amenazas que afecten la ciberseguridad en el ámbito nacional.
3. Liderar procesos investigativos de carácter nacional e internacional contra organizaciones cibercriminales que afecten ciudadanos, patrimonio, infraestructura digital, etc.
4. Administrar el Observatorio Nacional del Cibercrimen realizando análisis de tendencias, alertas tempranas, georreferenciación y focalización.
5. Generar alianzas que fortalezcan la investigación del cibercrimen cumpliendo con la Estrategia de Ciberseguridad en Colombia (Consejo Nacional de Política Económica y Social, 2016).
6. Atender incidentes cibernéticos que afecten a los ciudadanos que utilizan el

ciberespacio en Colombia.

Para la ejecución de estas funciones cuenta con una estructura interna de líneas de investigación así: (1. Centro de Capacidades para la Ciberseguridad. - 2. Unidad Investigativa. - 3. Informática Forense. - y 4. Observatorio del Crimen) al igual que desarrollan investigación a las actividades que desestabilizan al Estado, renombre nacional y temas relacionados con la prevención ante delitos informáticos en todos sus aspectos.

La fuerza efectiva del CCP es de sesenta y cuatro (64) funcionarios, de los cuales son ocho (8) oficiales, trece (13) personal del nivel ejecutivo, y cuarenta y tres (43) patrulleros.

La formación académica está distribuida en: dos (2) con título de maestría en temas relacionados con ciberseguridad, cuatro (4) con especialización en informática forense, cinco (5) ingenieros de sistemas, veinte (20) tecnólogos y técnicos en sistemas, los restantes treinta y tres (33) funcionarios cuentan con el curso básico de policía judicial dictado por la escuela de investigación criminal de la Policía Nacional.

- **CSIRTPONAL**

El CSIRTPONAL está compuesto por tres grupos, Grupo Continuidad de la Información (GUCIN), Grupo Seguridad de la Información (GUSIN), y el Grupo Respuesta a Incidentes de Seguridad (CSIRT), dependencias encargadas de supervisar el desarrollo, implementación,

mantenimiento, calidad, ciclo de vida, continuidad, disponibilidad, confidencialidad, integridad y la atención a incidentes informáticos que puedan o afecten las tecnologías de la información y la información en sí mismo de la Policía Nacional, (Ministerio de Defensa, Policía Nacional-Dirección General, 2013), a los cuales les fueron asignados las siguientes funciones en general :

1. Definir metodología y controles para contar con las mejores prácticas de ciclo de vida y clasificación de la información, con el fin de conservar la memoria digital de la institución.

2. Realizar el monitoreo de herramientas de disponibilidad de red, servidores y canales de datos.

3. Realizar pruebas de calidad con el fin de verificar que el software adquirido o desarrollado no cuente con vulnerabilidades.

4. Liderar el análisis del impacto en el negocio, plan de continuidad del negocio y el plan de recuperación ante desastres.

5. Implementar, configurar, aplicar, operar y hacer seguimiento a los controles de seguridad y el Sistema de Gestión de Seguridad en la Policía Nacional.

6. Asesorar, adquirir y administrar los proyectos tecnológicos relacionados con seguridad de la información.

7. Detectar, reportar y solucionar, vulnerabilidades y amenazas a incidentes informáticos que afecten la disponibilidad, confidencialidad e integridad de la plataforma de la Policía Nacional.

8. Realizar la difusión, concientización y prevención de las políticas de seguridad de la información.

9. Apoyar y dar respuesta a los incidentes de seguridad de la información que se presenten en la institución.

10. Realizar acuerdos de colaboración y convenios con diferentes organismos nacionales e internacionales, que permita construir una red mundial de apoyo en Ciberseguridad.

11. Implementar y hacer seguimiento a la "Estrategia Nacional para la protección del Ciberespacio" (Consejo Nacional de Política Económica y Social, 2016), a fin de contribuir a la sensibilización del ciberciudadano sobre la importancia de la seguridad de la información.

El CSIRTPONAL está organizado y conformado por 3 grupos operativos así: Grupo de Seguridad de la Información, Continuidad en el Negocio y Grupo CSIRT.

La fuerza efectiva del CSIRTPONAL es de dieciséis (16) funcionarios, de los cuales son tres (3) oficiales, ocho (8) personal del nivel ejecutivo, cuatro (4) patrulleros y un (1) personal no uniformado. La formación académica se distribuye en: cinco (5) con título de maestría en seguridad de la información, ciberseguridad y ciberdefensa y gestión de proyectos, cuatro (4) cuentan con especializaciones en seguridad de la información e informática forense, cuatro (4) ingenieros de sistemas y tres (3) tecnólogos en telemática de la escuela de tecnologías de la información y las comunicaciones de la Policía Nacional.

- **Grupo de Inteligencia de Señales y Geoespacial – SECYC**

El Grupo de Inteligencia de Señales y Geoespacial tiene uno de sus procesos orientado a la SECYC, dentro de las funciones del grupo se destaca lo siguiente, "Es una dependencia

del Área de Producción de Inteligencia, encargada de recolectar información a través de medios técnicos con el fin de aportar a la producción de inteligencia estratégica, operacional y para el Servicio de Policía, que permita prevenir las amenazas y riesgos que puedan atentar contra la seguridad y defensa de la Nación" (Ministerio de Defensa, Policía Nacional-Dirección General, 2015), a la cual le fueron asignadas las siguientes funciones que aplican al ciberespacio, así:

1. Coordinar con las autoridades del sector de las tecnologías de la información y las comunicaciones en el país, las medidas disuasivas y de control para el correcto uso del espectro electromagnético.
2. Evaluar que la información recolectada a través de la inteligencia de señales cumpla los límites, fines y principios establecidos en la normatividad vigente y que esta permita aportar a la producción de inteligencia.

El SECYC está conformado por cuatro grupos que abarcan la línea de análisis e investigativo así: Criptoanálisis, Minería de Datos, Análisis de Fuentes Abiertas y Monitoreo de Redes.

La fuerza efectiva del SECYC es de nueve (9) funcionarios, de los cuales son un (1) oficial, cuatro (4) personal del nivel ejecutivo y cuatro (4) patrulleros. La formación académica se distribuye en: una (1) con título de maestría en seguridad de la información, tres (3) ingenieros de sistemas y cinco (5) cuentan con el curso de análisis de información en inteligencia de la Escuela de Inteligencia y Contrainteligencia de la Policía Nacional.

- **Cibergaula**

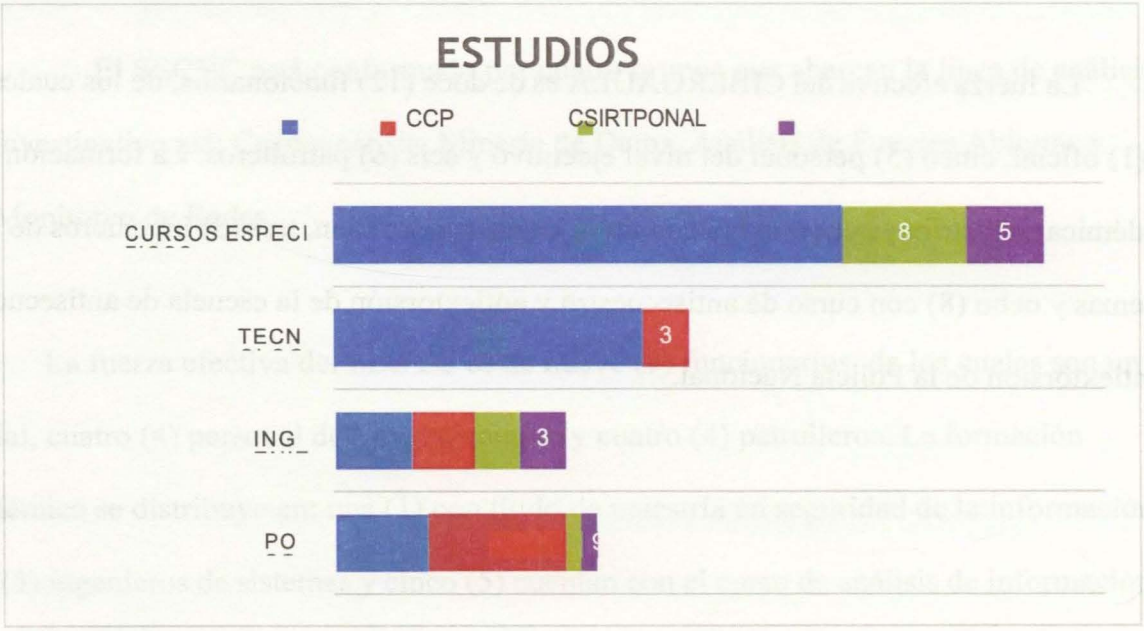
Por último, el CIBERGAULA actualmente no hace parte de la estructura orgánica de la Dirección de Antisecuestro y Antiextorsión; sin embargo, este grupo tiene como función apoyar investigaciones de secuestro y extorsión donde se hayan empleado medios tecnológicos o se utilice el ciberespacio como canal de comunicación, además realizar el seguimiento a flagelos de extorsión a través de medios tecnológicos (correos electrónicos, redes sociales, mensajería instantánea etc.).

El CIBERGAULA está conformado por tres grupos los cuales trabajan líneas de acción diferentes pero engranadas para generar un producto operativo, estos grupos son: Grupo de Laboratorio de Informática, Grupo Investigativo y el Grupo de Prevención.

La fuerza efectiva del CIBERGAULA es de doce (12) funcionarios, de los cuales son un (1) oficial, cinco (5) personal del nivel ejecutivo y seis (6) patrulleros. La formación académica se distribuye en: uno (1) con título de especialización, tres (3) ingenieros de sistemas y ocho (8) con curso de antisecuestro y antiextorsión de la escuela de antisecuestro y antiextorsión de la Policía Nacional.

CATEGORIA	DIJIN CCP	DIASE CIBERGAULA	OFITE CSIRT	DIPOL SECYC	DISEC GRUPO CONTRA PORNOGRAFÍA INFANTÍL	EXISTENTE ACTUAL	IDEAL DICIS	DIFERENCIA
OFICIALES	8	2	3	2	1	16	23	7
NIVEL EJECUTIVO	13	5	8	6	5	37	56	19
PATRULLERO	43	8	4	8	7	70	103	33
NO UNIFORMADOS	-	-	-	-	-	1	-	-1
TOTAL PERSONAL	64	15	16	16	7	124	182	58
MAESTRÍA	2	1	5	1	-	9		
ESPECIALIZACIÓN	4	1	4	2	2	13		
INGENIERO SISTEMAS	5	5	4	4	2	20		
TECNÓLOGOS	20	-	3	-	1	24		
CURSOS BÁSICOS	33	8	-	9	-	50		

Gráfica 6. Cantidad de personal de cada grupo. Fuente: Elaboración propia, 2018



Gráfica 7. Fuente: Distribución académica de los grupos. Elaboración propia, 2018

Una vez revisada cada una de las unidades policiales que tienen relación con las conductas que afectan la seguridad y convivencia de los ciudadanos en el ciberespacio, en sus procesos misionales de investigación criminal, inteligencia y direccionamiento tecnológico, se observa que algunas de las tareas son transversales en los grupos, entre ellas:

- Generación y aplicación de Estrategia Nacionales de Ciberseguridad
- Realización de convenios, alianzas con las entidades pioneras y líderes en temas de prevención e investigación de este tipo de conductas.

Las funciones listadas no son un indicador de cumplimiento frente a las tareas que debe ejecutar la Policía Nacional en materia de Ciberseguridad, dado que al momento no han sido comparadas con estándares o buenas prácticas existentes. Es por esta razón que en el proceso de investigación se tomó como línea base el documento emitido por el Observatorio de la Ciberseguridad en América Latina y el Caribe, el cual analiza el nivel en las capacidades y preparación de la Región en materia cibernética (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016). Cabe mencionar que este estudio empleó como fundamento el Modelo de Madurez de Capacidad de Seguridad Cibernética (MMCSC).

El Modelo de Madurez de Capacidad de Seguridad Cibernética y el estudio del Observatorio definen cinco (5) dimensiones para determinar el nivel de madurez en Ciberseguridad de un Estado, la primera dimensión se denomina política y estrategia, busca establecer si un estado cuenta con una estrategia nacional de seguridad cibernética oficial o

documentada, en que proceso de desarrollo o implementación se encuentra, a quien involucra y por otra parte verifica si el estado tiene una estrategia de defensa cibernética, quien es el responsable y que procedimientos de coordinación existen ante un ataque informático. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016)

La segunda dimensión se denomina cultura y sociedad, esta mide cuatro factores, mentalidad de seguridad cibernética (como está el estado en los diferentes sectores gobierno, Sector privado y sociedad), conciencia en seguridad cibernética, confianza en el uso de internet (servicios en línea, gobierno y comercio electrónicos) y privacidad en línea. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

La tercera dimensión se denomina educación, esta mide cuatro factores, disponibilidad nacional de la educación y formación cibernética, desarrollo nacional de la educación de seguridad cibernética, formación e iniciativas educativas públicas y privadas y la comprensión de la seguridad cibernética por parte de empresas. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

La cuarta dimensión se denomina marcos legales, mide tres factores, marcos jurídicos de seguridad cibernética (en el uso de las TIC, privacidad de datos, derecho procesal y sustantivo de la delincuencia cibernética), investigación jurídica (Fiscalía, cumplimiento de la ley) y divulgación responsable de la información. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

La quinta dimensión agrupa las tecnologías, esta dime ocho factores, adhesión a las

normas (desarrollo de software y cumplimiento de estándares), organizaciones de coordinación de seguridad cibernética (centros de operaciones de seguridad, comando y control), respuesta a incidentes, resiliencia de la infraestructura critica, protección de la infraestructura critica, gestión de crisis y redundancia digital. (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016).

Para el caso particular de este documento, se compararon estas dimensiones con los procesos actuales de la PONAL con el objetivo de determinar aquellos que deben ser incluidos en la conformación de la DICIS. De esta forma se obtuvieron los siguientes resultados:

1. La primera dimensión hace referencia a Políticas y Estrategia. En el caso de la PONAL, aunque la institución tiene cinco (5) grupos que atienden en algún sentido la necesidad de Ciberseguridad del Estado Colombiano, no existe una estrategia que los coordine, indicadores de seguimiento, cumplimiento y lineamientos claros que permitan la suma de esfuerzos orientados a operacionalizar la Política en la PONAL. Es por esta razón que deben ser unificados en la Dirección de Ciberseguridad - DICIS.

2. La segunda dimensión contempla la cultura cibernética y sociedad. En la revisión realizada cuatro (4) de los cinco (5) grupos desarrollan esta tarea, sin embargo, la orientan a concientizar a los ciudadanos en sus problemáticas específicas, lo que lleva a desperdiciar esfuerzos, ya que, en la mayoría de los casos, estas jornadas de concientización atacan una misma causa raíz y un mismo objetivo, la DICIS debe contar con una área o grupo que se dedique específicamente a esta tarea.

3. La tercera dimensión busca que exista educación, formación y competencias en seguridad informática, al realizar una sumatoria del personal que en la actualidad tiene relación con la prevención, anticipación e investigación de conductas delictivas en el ciberespacio, la Policía Nacional tiene un total de: ciento un (124) funcionarios, distribuidos en trece (16) oficiales, treinta (37) personal del nivel ejecutivo, cincuenta y siete (70) patrulleros y un (1) personal no uniformado, en lo relacionado con la preparación académica se observa un nivel académico importante al contar con, ocho (8) con título de maestría en temas relacionados con Ciberseguridad, nueve (9) con especialización en seguridad de la información e informática forense, quince (15) ingenieros de sistemas y electrónicos, los restantes sesenta y nueve (69) son tecnólogos y técnicos en sistemas, investigación criminal y análisis de información, en las diferentes escuelas de formación de la Policía Nacional.

4. La cuarta dimensión se enfoca a que la institución cuente con un marco reglamentario que oriente el actuar en cuanto a Ciberseguridad y seguridad de la información, al compararlo con lo que actualmente realiza la Policía Nacional, se observa que los grupos según su proceso misional lo realizan, CCP con el cumplimiento de la ley 1273 de 2009, el GUSIN verifica el cumplimiento del Sistema de Gestión de Seguridad de la Información ISO 27001:2013, sin embargo se deberían incluir las mismas funciones con un alcance a entidades públicas y privadas en la DICIS.

5. La quinta dimensión está relacionada con los procedimientos necesarios para que la tecnología cuente con gestión de incidentes, resiliencia de infraestructuras críticas, gestión

de crisis, redundancia, ciclo de vida del desarrollo y coordinación interinstitucional, la institución lo realiza con: CSIRTPONAL, CCP y GUSIN, sin embargo se orientan en su mayoría a blindar la institución, dado que la DICIS está enfocada a brindar servicios al Estado y la ciudadanía por tal razón estas funciones deben ser incluidas, con el fin de mejorar la operación y uso de la tecnología en el Estado Colombiano.

6.2. Estructura orgánica proyectada para la Dirección de Ciberseguridad

Una vez realizada la comparación de los procesos existentes con el estudio del Organismo de los Estados Americanos (Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID), 2016)se identificó una estructura orgánica que esta alienada a los requerimientos de la Institución y que a su vez pueda mejorar el nivel de madurez del Estado Colombiano según el MMCSC.

Por tal razón es importante mencionar que la Policía Nacional cuenta con unos lineamientos que orientan el proceso de creación de grupos, áreas, oficinas asesoras, metropolitanas y direcciones, según estos lineamientos una dirección debe contar con una misión que defina el que hacer, un tren administrativo y logístico que facilite las herramientas, bienes y servicios que permitan a los grupos misionales realizar sus funciones, dado que el alcance de este documento busca definir los procesos y funciones de la DICIS, el alcance se orienta en los grupos misionales y no administrativos y logísticos, ya que estos son un estándar para todas las unidades de la Policía.

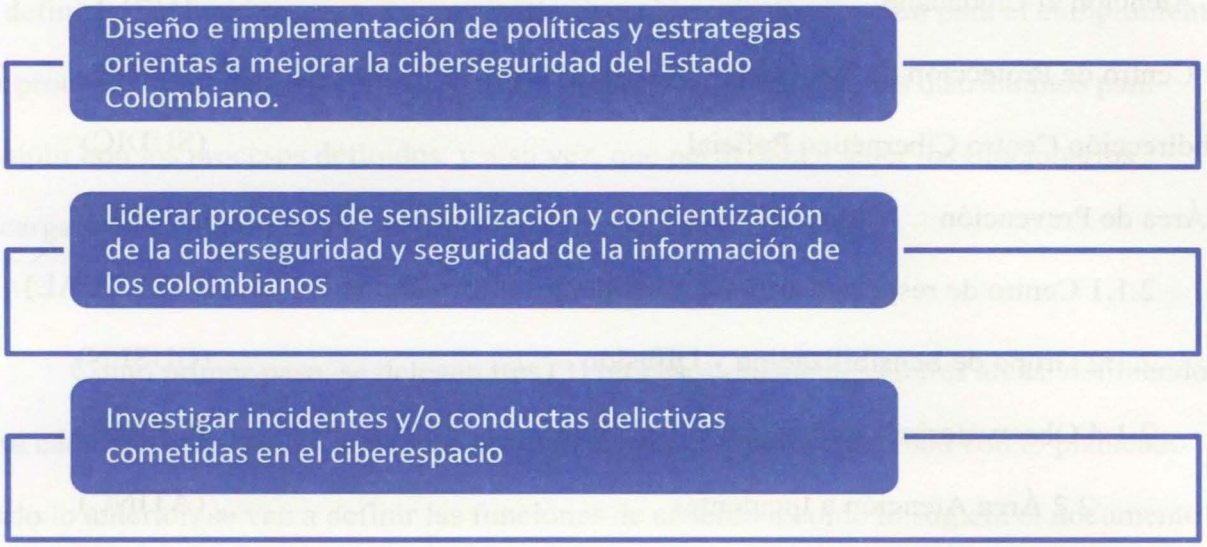
Según lo revisado anteriormente el país necesita de una Dirección dedicada a la anticipación, prevención, atención de incidentes e investigación de los delitos cibernéticos que afectan la confidencialidad, integridad y disponibilidad de los activos críticos de la nación, la institución debe buscar contar con una estructura dotada de herramientas tecnológicas, metodologías basadas en estándares internacionales, laboratorios y un equipo dedicado a la seguridad de las TI, enfrentando y combatiendo los delitos que se generen con el uso de las Tecnologías de la Información apoyando a la ciudadanía y organizaciones a mitigar sus riesgos y la gestión adecuadamente de incidentes cibernéticos.

Por tal razón se plantea como misión la siguiente: la Dirección de Ciberseguridad tiene como misión velar por la Ciberseguridad de los ciudadanos a través de la anticipación, prevención, atención de incidentes e investigación de los delitos cometidos en el ciberespacio dentro del ámbito nacional, apoyando al gobierno nacional en la Política de seguridad digital

mediante la sensibilización, concientización, análisis criminal, logrando de esta un uso responsable de las tecnologías de la Información y las comunicaciones al servicio de la ciudadanía.

La estructura de áreas y grupos se plantea de la siguiente forma:

La Dirección de Ciberseguridad dependerá de la Subdirección General de la Policía Nacional, y será la encargada de liderar los procesos de:



Una vez definidos los procesos misionales de la DICIS, se propone definir la estructura con base en la siguiente nomenclatura y estructura orgánica, la cual es utilizada por la Policía Nacional para definir grupos y áreas, consta de una sigla compuesta por cinco (5) letras.

1. Dirección de Ciberseguridad (DICIS)

1.1. Secretaria Privada (SEPRI)

1.2. Comunicaciones Estratégicas (COEST)

1.3. Asuntos Jurídicos y DDHH (ASJUD)

1.4. Planeación (PLANE)

1.5. Gestión Documental (GEDOC)

1.6. Asuntos Internacionales (ASINT)

1.7. Telemática (TELEM)

1.8. Atención al Ciudadano (OAC)

1.9. Centro de Protección de Datos (CPDI)

2. Subdirección Centro Cibernético Policial (SUDIC)

2.1 Área de Prevención (ARPRE)

2.1.1 Centro de respuesta en línea a incidentes informáticos (CAI VIRTUAL)

2.1.2 Grupo de Sensibilización y Difusión (GUSEN)

2.1.4 Observatorio Nacional del Cibercrimen (OBNCI)

2.2 Área Atención a Incidentes (ATINC)

2.2.1 Administración del SGSI (ASGSI)

2.2.2 CSIRT-PONAL (CSIRT)

2.3 Área de investigaciones tecnológicas. (ARINV)

2.3.1 Grupo de protección a la información y a los datos. (GUPID)

2.3.2 Grupo contra la pornografía infantil. (GUPME)

2.3.3 Grupo contra la extorsión y el fraude. (GUCNA)

2.3.4 Grupo de Ciberterrorismo. (GCITE)

2.4 Laboratorios (GULAB)

6.3. Definición de funciones, grupos y procesos del personal de la DICIS

Los anteriores títulos tenían como objetivo, encontrar en la Institución los grupos dedicados a la Ciberseguridad, comparar estas funciones con estándares y buenas prácticas internacionales y con base en esto, definir los procesos que debe tener la DICIS. A partir de allí

se definirán las funciones que son necesarias, su adecuada distribución para el cumplimiento de los procesos definidos, así como el perfil y los cargos, igualmente las distribuimos para cumplir con los procesos definidos, y a su vez, que perfil deben tener los funcionarios encargados de cumplir con la misión planteada para esta dirección.

Como primer paso, se delegan tres (3) procesos misionales en tres áreas, definiendo para cada una de ellas, las funciones necesarias para cumplir a cabalidad con lo planteado. Dado lo anterior, se van a definir las funciones de acuerdo a como lo sugiere el documento de la Oficina de Planeación de la Policía Nacional, así:

Dirección de Ciberseguridad: esta Dirección de la Policía Nacional será la encargada de liderar los siguientes procesos:

1 Diseño e implementación de políticas y estrategias orientas a mejorar la Ciberseguridad del Estado Colombiano.

2 Liderar procesos de sensibilización y concientización de la Ciberseguridad y seguridad de la información de los colombianos.

3 Investigar incidentes y/o conductas delictivas cometidas en el ciberespacio.

Realizando las siguientes funciones, propender por la seguridad de los colombianos en el ciberespacio, a través de sus programas de difusión y observatorio nacional del crimen e investigaciones tecnológicas; En la parte de difusión cumplirá labores de concientización de los ciudadanos y usuarios finales, con el fin de minimizar el riesgo de mal uso o uso

irresponsable de algún tipo de medio tecnológico, así mismo, realizará la divulgación de planes, programas, campañas, informes de situaciones en el ciberespacio, comportamientos más frecuentes, perfiles de ciberdelincuentes y sus modus operandi, principales amenazas y recomendaciones para mitigar los impactos de la materialización de eventos e incidentes informáticos; En cuanto a la función de análisis, realizará un monitoreo de la red soportando a las diferentes instituciones y organismos del Estado, sector público y privado en la Internet, en cuanto a reportes de comportamiento y salud del ciberespacio; Finalmente en el área de investigación criminal, realizará los procesos de investigación y judicialización de los ciberdelitos y comportamientos que atenten contra las libertades y derechos de los ciberciudadano, adicionalmente dispondrá de un equipo dedicado a la seguridad de las TI, ayudando a las organizaciones a mitigar y a evitar los incidentes graves de seguridad de la información.

Es de aclarar que, al referirse a los procedimientos y funciones de la DICIS, se hace referencia a que estos deben ser liderados por el director.

A continuación, se distribuyen en cada una de ellas, delegando a los jefes de área para liderar el proceso definido, los jefes de grupos deberán liderar las funciones y el personal operativo realizar las funciones, los cargos y funciones para cada uno de los integrantes de la dirección se encuentran definidos en el apéndice 2 de este documento, del cual se va a hablar en más detalle en el siguiente título, así:

Área de Prevención: Es la dependencia de la DICIS que tiene como función liderar el proceso de sensibilización y concientización de la Ciberseguridad y seguridad de la información de los colombianos, y la de gerenciar las funciones de recolección, atención, difusión y prevención, en la recolección se deberá ejecutar y orientar el tratamiento de la información a través de la organización, clasificación, valoración preliminar, registro y análisis de la información a partir de la aplicación de metodologías, técnicas y herramientas que lleven a anticiparse a conductas delictivas. En la atención deberá garantizar que la respuesta sea oportuna y acertada hacia los ciudadanos afectados, en la difusión se deberá fomentar el cumplimiento a la ley y la implementación de las políticas de seguridad digital del estado colombiano y la prevención debe estar de la mano con el observatorio nacional del cibercrimen con el fin de orientar las campañas de acuerdo a las amenazas que se estén presentado, para esto se deberán diseñar cursos, charlas y guías, buscar alianzas, convenios e intercambios con instituciones referentes orientados a la toma de conciencia y el cuidado que se debe tener con la seguridad de la información.

Centro de respuesta en línea a incidentes informáticos: Es la dependencia del área de prevención que será el punto de contacto entre el ciudadano y la Policía Nacional, recibiendo todo tipo de información, requerimiento, denuncias o reportes de incidentes que tengan relación con la Ciberseguridad. Estos deberán ser filtrados, organizados y clasificados, realizando el *triage* que consta de asignarles en una escala de prioridad y un investigador para luego ser asignados al grupo CSIRT para su análisis.

Grupo de Sensibilización y Difusión: Es la dependencia del área de prevención que

tendrá como función primordial, implantar una estrategia que aterrice la Política de seguridad digital ((Económica, 2016)), en lo referente a las obligaciones de la Policía Nacional, la estrategia debe incluir; priorizar el contacto con los equipos de respuesta a incidentes informáticos, casas de antivirus, comunidades dedicadas a la Ciberseguridad, entidades educativas, organismos nacionales e internacionales con el fin

de crear una red de colaboración que permita tener de primera mano nuevas modalidades, estrategias, ataques cibernéticos y técnicas de mitigación de amenazas en el ciberespacio.

Observatorio Nacional del Cibercrimen: Es la dependencia del área de prevención que tendrá como función primordial ejecutar y orientar el tratamiento de la información a través de la organización, clasificación, valoración preliminar, registro y análisis de la información a partir de la aplicación de metodologías, técnicas y herramientas que lleven a anticiparse a conductas delictivas, generar productos frente a los diferentes factores y dinámicas que afecten el ciberespacio que permita orientar la toma de decisiones. Adicionalmente deberá hacer la identificación y medición del impacto de los análisis criminológicos realizados, la satisfacción de las necesidades y las expectativas de los ciudadanos.

Área Atención a Incidentes: es la dependencia de la DICIS que tendrá como función liderar el proceso de diseño e implementación de políticas y estrategias orientadas a mejorar la Ciberseguridad del Estado Colombiano y gerenciar las funciones relacionadas con el Sistemas de Gestión de Seguridad de la Información en la Policía Nacional, la asesoría en la

implementación de controles de seguridad a las entidades del Estado y la atención a incidentes informáticos tanto para la Policía Nacional como para las entidades públicas y privadas que soliciten su asesoría o apoyo, garantizar que la información de nuestro talento humano, instalaciones policiales y el hardware y software que soporta el servicio de policía cuente con los más altos niveles de seguridad que permita garantizar la confidencialidad, disponibilidad e integridad de los mismos, mitigando con esto riesgos como fuga, perdida o daño de la información.

Administración del SGSI: Es el grupo del Área Atención de incidentes que tiene como función realizar el análisis, verificar el cumplimiento del SGSI (Sistema de Gestión de Seguridad de la Información) en la Policía Nacional con responsabilidad sobre los siguientes procesos:

- Levantamiento de activos
- Análisis de riesgos.
- Tratamiento de riesgos
- Ciclo de vida de la información
- Auditorías de seguridad de la información
- Análisis de la vulnerabilidad
- Continuidad del negocio.

CSIRT-PONAL: Es la dependencia del Área Atención de incidentes que se encargará de la gestión a incidentes informáticos de la Policía Nacional y las entidades públicas y privadas que soliciten su asesoría o apoyo, enfocando sus servicios a incidentes que afecten la

confidencialidad, integridad o disponibilidad, realizando las acciones necesarias para recuperar la funcionalidad del sistema o activo afectado, evidenciando causas, vulnerabilidades y las lecciones aprendidas que garanticen la no reincidencia de incidentes asociados a la misma causa raíz.

Área de investigación Tecnológica: Es la dependencia de la DICIS que tiene como función liderar el proceso de investigación de incidentes o conductas delictivas cometidas en el ciberespacio, y realizar las siguientes funciones:

1. Asesorar e investigar las tecnologías asociadas a la anticipación, prevención y mitigación de conductas que atenten contra la Ciberseguridad de los usuarios de las tecnologías de la información en Colombia.

2. Asegurar la seguridad de la información y Ciberseguridad orientada a liderar los siguientes procesos:

- Protección a la información y a los datos.
- Protección a los menores de edad, investigación a la pornografía infantil y sistema de seguimiento a la explotación infantil (C.E.T.S).
- Protección al fraude informático, estafas virtuales, extorsión por medios informáticos y criptomonedas.
- Anticipación y protección al hacktivismo, amenazas electrónicas y ciberterrorismo.
- Investigación a las defraudaciones de derechos de autor (piratería de software).
- Anticipación e investigación a intrusiones a la infraestructura digital del estado.

- Monitoreo y vigilancia digital.

Grupo de protección a la información y a los datos: Es la dependencia del área de investigación que tendrá como función el proceso de investigar y hacer el seguimiento de la verificación y las diligencias judiciales en todos los casos que incurra en una conducta penal violando la ley 1273 del 2009 "de la protección de la información y de los datos", ley 1581 del 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales." y demás normatividad que su incumplimiento acarreara una conducta penal que deba ser judicializado. Adicionalmente coordinará con el Observatorio Nacional del Cibercrimen con el fin de actualizar y analizar las estadísticas de los delitos de su competencia, diseñando una base de datos con los delincuentes más buscados y el modo de operación de estos delincuentes, coordinará con los diferentes organismos del Estado, entidades públicas y privadas a nivel Nacional e Internacional, el apoyo necesario en procura de lograr la efectividad en la investigación criminal orientada a neutralizar los delitos informáticos.

Grupo contra la extorsión y el fraude: Es la dependencia del área de investigaciones tecnológicas que tendrá como tarea, todo lo relacionado con la investigación en temas relacionados con la extorsión y fraude informático direccionando los procesos de protección al fraude informático, estafas virtuales, extorsión por medios informáticos (ransomware, sextorsión), criptomonedas y defraudaciones de derechos de autor (piratería de software).

Grupo contra la pornografía infantil: Es la dependencia del área de investigaciones tecnológicas que tendrá como tarea todo lo relacionado con menores de edad, dirigiendo las siguientes funciones:

- Protección a los menores de edad, investigando a las estructuras que lideran la pornografía infantil.
- Anticipación a conductas (sexting).
- Liderar la implementación del sistema de seguimiento a la explotación infantil (C.E.T.S) o similares.
- Adherir nuevos patrones de análisis al coordinador del sistema de alerta para la desaparición de Menores de Edad (Cámara de representantes Secretaria General, 2016), en temas provocados por medios tecnológicos.

Grupo de Ciberterrorismo: Es la dependencia del área de investigaciones tecnológicas que tendrá como tarea, todo lo relacionado con la protección del estado en lo referente a ataques cibernéticos, ciberterroristas, amenazas cibernéticas y lo que se considere una amenaza para los ciberciudadanos colombianos. Para esto deberá direccionar los siguientes procesos, anticipación y protección al Hacktivismo, amenazas electrónicas, ciberterrorismo, anticipación e investigación a intrusiones a la infraestructura digital del Estado y monitoreo y vigilancia digital.

Área de Laboratorios: Esta dependencia es la encargada de operar los diferentes laboratorios de la DICIS con el fin de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable. Las capacidades de análisis deben ir

orientadas a las unidades forenses de dispositivos móviles, forenses en red alámbrica e inalámbricas, forenses en bases de datos, auditorias en activos de red y perímetros de seguridad (firewall, sistemas de prevención de intrusos, etc.), criptoanálisis, auditoria en sistemas de almacenamiento, audio, video, análisis de malware. Para esto deberá diseñar, implantar y administrar una cámara limpia lineada a los estándares internacionales.

6.4. Definición de cargos y perfiles de la Dirección de Ciberseguridad -DICIS

Esta fase busca definir, capacidades actuales, procesos y funciones de la DICIS, definir los cargos que deben tener la direcciones y los perfiles que deben tener cada uno de los funcionarios, para esto se toma como base la Resolución 00937 del 10 de marzo de2016 "por la cual se establece el manual de funciones para el personal uniformado de la Policía Nacional, la metodología de evaluación para el perfil de los cargos", (Ministerio de Defensa, Policía Nacional-Dirección General, 2016).

Aunado a lo anterior, la Policía Nacional con el fin de optimizar la distribución del talento humano de la institución de acuerdo a sus capacidades y necesidades, definió las TOP, para las cuales cada uno de los grupos y áreas para este caso de las direcciones tienen un mínimo de personal para su funcionamiento.

En la actualidad las unidades operativas y oficinas asesoras objeto de este estudio, tienen en promedio 862 funcionarios, siendo la más pequeña la Oficina de Telemática con 182 funcionarios y la más grande la Dirección de Investigación Criminal con 1.600, lo que

claramente nos deja ver que no existe un estándar para la cantidad de funcionarios que debe tener una Dirección en la Policía Nacional, lo que sí se puede definir y esta reglado parcialmente en la Resolución 00937 del 10/03/2016 (Ministerio de Defensa, Policía Nacional-Dirección General, 2016), es que la cantidad de funcionarios debe ser directamente proporcional a la cantidad de procesos que maneja el área y el grupo, es por esto que la distribución de personal según las funciones definidas y el personal existen es la siguiente:

Para los grupos administrativos y logísticos, se define que el personal ideal es de 20 funcionarios, este valor se obtiene de hacer una comparación con la Oficina de Telemática de la Policía Nacional, la cual cuenta con tres procesos misionales al igual que los definidos en la DICIS. Sin embargo, este es un valor tentativo, que se deberá ajustar en el momento que la DICIS entre en operación, fecha en el cual realmente se evidenciará el flujo de requerimientos administrativos y logísticos de la dirección.

En la tabla 1 se muestra la distribución de los 20 funcionarios en los siete (7) grupos estandarizados por la Policía Nacional, para la parte administrativa y logística de cualquier unidad.

Dirección de Ciberseguridad	
Personal ideal	20
Personal si se creara hoy la DICIS	0
Grupos	Personal
Planeación	3
Comunicaciones Estratégicas	2

Telemática	5
Gestión Documental	1
Centro de Protección de Datos	3
Atención al ciudadano	2
Asuntos Jurídicos y DDHH	4
Total	20
Personal de plana mayor que no hace parte del personal operativo de la DICIS	

Tabla 1. Talento humano parte administrativa DICIS, elaboración propia.

Los cargos y funciones de la parte administrativa no son alcance de este trabajo ya que estos se encuentran estandarizados en la Policía Nacional, en el caso de la creación de la DICIS solo se asignará personal que cumplan con el manual de funciones para cada una de estas labores.

En la tabla 2 se explica la distribución del personal en cada uno de las áreas y grupos. Las tres (3) áreas cuentan con funcionarios de apoyo para el control de su proceso asignado, las funciones serán las siguientes:

- Jefe de área ejercerá el liderazgo y control para las funciones definidas anteriormente, su perfil está definido en el apéndice 2.
- Cada una de las áreas tiene personal de apoyo, que deberá realizar las funciones de control, sobre las funciones de los grupos que hacen parte del área, cada uno se deberá encargar del seguimiento a los planes de acción definidos por los jefes de área, para el cumplimiento de su proceso asignado.

El personal definido en cada uno de los grupos se debe a la siguiente relación:

- Centro de respuesta en línea a incidentes informáticos: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.
- Para este grupo se definieron treinta (30) funcionarios con el cargo analista de seguridad de la información, este grupo opera 7x24, distribuido en tres turnos, cada uno de los turnos con diez (10) personas, que son los que en promedio operan un 123 de la Policía Nacional, las funciones están relacionadas con punto de contacto entre el ciudadano y la Policía Nacional, recibiendo todo tipo de información, requerimiento, denuncias y reportes de incidentes que tengan relación con la ciberseguridad, los deberán filtrar, organizar y clasificar, realizando el *triage* asignará una escala de prioridad y un investigador, el perfil se encuentra en el apéndice 2.
- Grupo de Sensibilización y Difusión: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

Para este grupo se definieron diez (10) funcionarios con el cargo analista de seguridad de la información, dado que este grupo tiene como funciones operacionalizar las obligaciones de la Policía Nacional con la estrategia de política de seguridad digital, tres (3) funcionarios se dedicarán a integrar el sector educativo. Tres (3) sector privado, tres (3) sector público y uno (1) con la comunidad internacional, el perfil se encuentra en el apéndice 2.

- Observatorio Nacional del Cibercrimen: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.
- Para este grupo se definieron diez (10) funcionarios, con el cargo analista de seguridad de la información, que se van a distribuir las tareas así, cinco (5) realizarán las funciones de organización, clasificación, valoración preliminar, registro y análisis de la información a partir de la aplicación de metodologías, técnicas y herramientas que lleven a anticiparse a conductas delictivas, entregando productos del estudio, y los otros cinco (5) deberán hacer la identificación y medición del impacto de los análisis criminológicos realizados, la satisfacción de las necesidades y expectativas de los ciudadanos.
- Grupo Administración del SGSI: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.
- Para este grupo se definieron quince (15) funcionarios con el cargo analista de seguridad de la información, que van a cumplir con las siguientes tareas, cinco (5) realizarán las funciones de levantamiento de activos, análisis de riesgos y tratamiento de riesgos, dos (2) las funciones de ciclo de vida de la información, tres (3) auditorías de seguridad de la información, tres (3) análisis de vulnerabilidades y dos (2) los funciones relacionadas con la continuidad del negocio, el perfil se encuentra definido en el apéndice 2.
- Grupo CSIRT-PONAL: Un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

- Para este grupo se definieron quince (15) funcionarios, con el cargo investigador de incidentes, este grupo opera 7x24, distribuido en tres turnos, cada uno de los turnos con cinco (5) personas y realizarán las funciones de atención a incidentes que afecten la confidencialidad, integridad o disponibilidad, realizando las acciones necesarias para recuperar la funcionalidad del sistema o activo afectado, evidenciando causas, vulnerabilidades y las lecciones aprendidas que garanticen la no reincidencia de incidentes asociados a la misma causa raíz, el perfil se encuentra definido en el apéndice 2.
- Grupo de protección a la información y a los datos: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.
- Para este grupo se definieron quince (15) funcionarios, con el cargo investigador judicial, de los cuales trece (13) realizan las funciones relacionadas con el proceso de investigación, seguimiento, verificación y diligencias judiciales, en todo caso que incurra en una conducta penal violando la ley 1273 del 2009 "de la protección de la información y de los datos", ley 1581 del 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y demás normatividad que su incumplimiento acarre a una conducta penal y deba ser judicializado, los dos (2) restantes, realizarán las labores de coordinación con el observatorio nacional del cibercrimen, con el fin de actualizar y analizar la estadística de los delitos de su competencia, diseñando una base de datos con los delincuentes más buscados y el modo de operación de estos delincuentes, el perfil se encuentra definido en el apéndice 2
- Grupo contra la pornografía infantil: un funcionario que se desempeñará como

jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

- Para este grupo se definieron quince (15) funcionarios, con el cargo investigador judicial, de los cuales diez (10) realizarán las funciones de protección a los menores de edad, investigación a las estructuras que lideran la pornografía infantil y anticipación de conductas como el *sexting*, tres (3) realizarán las funciones para la implementación del sistema de seguimiento a la explotación infantil (C.E.T.S) y los dos (2) restantes, investigarán como adherir un nuevo patrón de análisis para el sistema de alerta para la desaparición de Menores de Edad en temas provocados por medios tecnológicos, el perfil se encuentra definido en el apéndice 2.

- Grupo contra la extorsión y el fraude: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

- Para este grupo se definieron quince (15) funcionarios, con el cargo investigador judicial, de los cuales seis (6) realizarán las funciones de investigación de modalidades del fraude informático y estafas virtuales, seis

(6) investigación sobre extorsión por medios informáticos (ransomware, sextorsión) y criptomonedas y los restantes tres (3) investigaciones sobre defraudaciones de derechos de autor (piratería de software), el perfil se encuentra definido en el apéndice 2.

- Grupo de Ciberterrorismo: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

- Para este grupo se definieron quince (15) funcionarios, con el cargo investigador judicial, de los cuales dos (2) realizarán las funciones de anticipación y protección al activismo, cuatro (4) investigaciones sobre amenazas electrónicas y ciberterrorismo, cuatro (4) las funciones de anticipación e investigación a intrusiones a la infraestructura digital del estado y cinco (5) monitoreo y vigilancia digital con el fin de brindar anticipación a las entidades del estado en lo referente a ataques cibernéticos, ciberterroristas y amenazas cibernéticas.

- Grupo de Laboratorios: un funcionario que se desempeñará como jefe de grupo y deberá liderar y controlar las funciones definidas anteriormente, el perfil se encuentra definido en el apéndice 2.

- Para este grupo se definieron veinte (20) funcionarios, con el cargo de perito informático, los cuales deberán cumplir las siguientes funciones, distribuidos de la siguiente forma: tres (3) forense de dispositivos móviles, tres (3) forense en red alámbrica e inalámbrica, tres (3) forense en bases de datos, tres (3) auditorias en activos de red y perímetros de seguridad (firewall, sistemas de prevención de intrusos, etc.), tres (3) criptoanálisis, dos (2) auditoria en sistemas de almacenamiento, audio, y video, y tres (3) análisis de malware, el perfil se encuentra definido en el apéndice 2.

Dirección de Ciberseguridad		
Personal ideal		182
Personal si se creara hoy la DICIS		101
Grupos	**Cargos**	**Personal**
Área de Prevención	Jefe Área de Prevención (1) Analista de seguridad de la Información (3)	1 3

Centro de respuesta en línea a incidentes informáticos	Jefe grupo Centro de respuesta en línea a incidentes informáticos (1) Analista de seguridad de la Información (30)	31
Grupo de Sensibilización y Difusión	Jefe grupo de Sensibilización (1) Analista de seguridad de la Información (10)	11
Observatorio Nacional del Cibercrimen	Jefe Grupo Observatorio Nacional del Cibercrimen (1) Analista de seguridad de la Información (10)	11
Área Atención a Incidentes	Jefe Área Atención a Incidentes (1) Analista de seguridad de la Información (2)	3
CSIRT-PONAL	fe grupo CSIRT- PONAL (1)	16
	dor de incidentes (15)	
Área de investigaciones tecnológicas	Jefe Área de investigaciones tecnológicas (1) Investigador Judicial (4)	5
Grupo de protección a la información y a los datos	Jefe grupo protección a la información y a los datos (1) Investigador Judicial (15)	16
Grupo contra la pornografía infantil	Jefe Grupo contra la pornografía infantil (1) Investigador Judicial (15)	16
Grupo contra la extorsión y el fraude	Jefe Grupo contra la extorsión y el fraude (1) Investigador Judicial (15)	16
Grupo de Ciberterrorismo	Jefe Grupo de Ciberterrorismo (1) Investigador Judicial (15)	16
Laboratorios	o Laboratorios (1) Perito informático (20)	21
Total		182

Tabla 2. Talento humano parte operativa DICIS. Elaboración propia.

La cantidad de funcionarios definidos están de acuerdo a los procesos y funciones que van a ejercer solo para nivel central, las seccionales contarán con una estructura similar, pero en un segundo nivel de despliegue las cuales harán parte del mapa de procesos de las 8 regionales de policía, las funciones son iguales a las definidas anteriormente.

Seccionales Dirección de Ciberseguridad		
Personal ideal		25
Personal si se creara hoy la DICIS		0
Procesos		Personal
esta en línea a incidentes informáticos	Analista de seguridad de la Información	3
Sensibilización y Difusión	Analista de seguridad de la Información	3
Soporte del SGSI	Analista de seguridad de la Información	2
ínea de investigación de la información y a los datos	Investigador Judicial	3
Línea de investigación contra la pornografía infantil	Investigador Judicial	3
Línea de investigación contra la extorsión y el fraude	Investigador Judicial	3
Línea de investigación de Ciberterrorismo	Investigador Judicial	3
Laboratorios	Perito informático	5
Total		25

Tabla 3. . Talento humano seccionales DICIS. Elaboración Propia

Entendiendo que la mayor dificultad que enfrenta una dirección con el alto nivel de especialización que se espera tenga la DICIS, es contar con un talento humano

capacitado, la estrategia de creación será inicialmente dotar el nivel central con los 101 funcionarios existentes, estos funcionarios soportan actualmente las obligaciones que tiene la Policía Nacional en relación con la Ciberseguridad, como se observó anteriormente, el problema que se evidencia no es que no exista personal o funciones relacionadas con la Ciberseguridad, es que las que existen no se encuentran articuladas, adicionalmente para formar un funcionario apto para desempeñar cualquier de las cargos definidos, no toma menos de 5 años, incluyendo los que requieren un pregrado y cursos específicos de formación, lo que llevaría a iniciar operación dentro de cinco (5) años mínimo, siguiendo con los esfuerzos aislados de cada una de las direcciones.

Adicionalmente en primera medida parece ser un aceptable talento humano, ya que, según estadística de la Dirección de Talento Humano de la Policía Nacional, ninguna unidad de Policía cuenta con su personal ideal, en promedio tiene de un 60 a 70 % de sus tablas TOP.

Cargos a desempeñar por área y grupo: revisando las funciones desempeñadas actualmente en la Policía Nacional, se encontró que ya existen una serie de cargos que se podría ajustar perfectamente a los objetivos que tendrá la DICIS, estos cargos de acuerdo al manual de funciones se parametrizan con un propósito, funciones y perfil (grado policial, educación, formación para el trabajo, experiencia y habilidades comportamentales), el alcance de este entregable se enfoca en el perfil que debe tener el funcionario que quieran desempeñar algún cargo operativo.

Para el caso de habilidades comportamentales no se tendrán en cuenta dado que estas son un estándar para la Policía Nacional y se obtienen del resultado de las pruebas de diagnóstico de efectividad gerencial (en adelante: DEG).

La descripción de cada uno de los cargos queda establecida por los jefes de área, grupo y el personal operativo que lo componen; Con el fin de optimizar el talento humano, el personal que va a laborar en los grupos y áreas se va a agrupar en cuatro cargos así:

- Analista de seguridad de la información.
- Investigador de incidentes.
- Investigador judicial.
- Perito informático.

La descripción de cada uno de ellos se puede consultar en el apéndice 2- perfil de funciones.

Por último y observando que los perfil que deben desempeñar los funcionarios que harán parte de la DICIS, requieren de conocimientos que son transversales a diferentes direcciones y que en la actualidad los cursos de capacitación de cada una de las escuelas solo se centra en su misionalidad particular, se hace necesario que las escuela de investigación criminal, inteligencia policial, tecnologías de la información y las comunicaciones y la de antisecuestro y antiextorsión, lideradas por la Dirección Nacional de escuelas, diseñen un curso en el cual cada uno de ellas se articule para orientar a los estudiantes en todas las aristas que tiene el problema y no en las problemáticas

particulares que se vienen generando.

Adicionalmente deberá propender para que los docentes que brinden estas capacitaciones sean los funcionarios que en la actualidad se enfrentan a la problemática, para

que de esta manera no se quede en un conocimiento meramente académico sino, se gradúen con los conocimientos técnicos y prácticos con los que se van a encontrar en el día a día.

Conclusiones

Sin intentar realizar una recopilación de lo anteriormente expuesto y desarrollado en el presente documento, pero si como resultado se resaltan algunas precisiones que considero importantes en el contexto de la investigación contra el ciber delito y la necesidad de integrar las capacidades existentes con el fin de hacer de la Policía Nacional una entidad que responda de manera efectiva a los delitos cibernéticos.

i. El continuo avance de las Tecnologías de la información, además traer múltiples beneficios para la sociedad, también origina un incremento del uso de estas tecnologías para fines delictivos, por eso puede señalarse que la criminalidad informática constituye un reto enorme tanto para los sectores de la sociedad, desde los responsables de la infraestructura crítica de un país, pasando por los legisladores, y finalizando con las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

ii. Este avance 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 en la investigación y aplicación del derecho penal con innovadores formas de abordar los conocimientos en contexto y científicos-investigativos.

iii. Esta nueva fenomenología implica un abordaje o estudio transversal y longitudinal, donde se recopilen de manera centralizada datos e información en un solo punto en el tiempo que permitan examinar e identificar las relaciones entre las variables de interés.

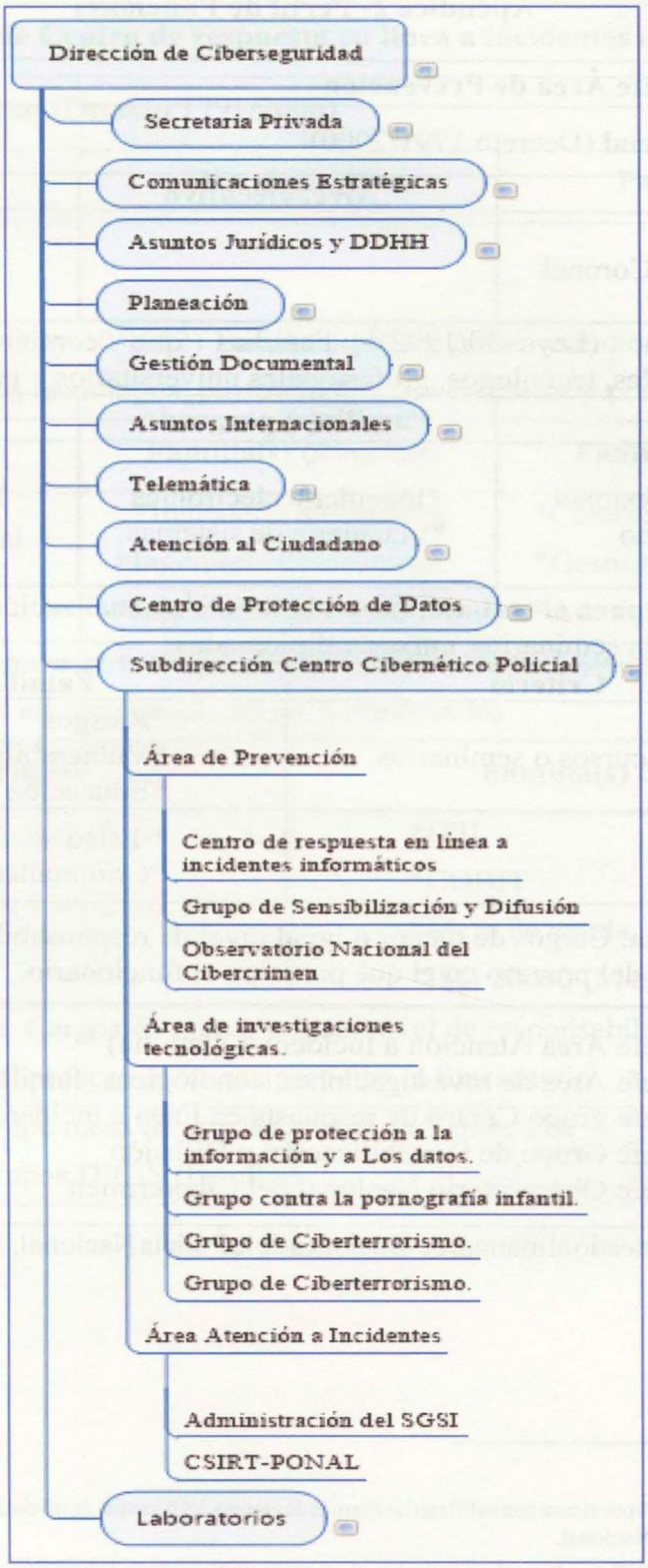
iv. Lo anterior, implica la unificación de unidades investigativas o centros de integración de investigación contra el ciber delito, que permitan coordinar las actuaciones de las distintas Agencias o unidades ante un ataque cibernético.

v. Como complemento y con base en el diagnóstico realizado frente la actuación de la Policía Nacional para abordar el fenómeno de la cibercriminalidad se precisa la necesidad de abordar estas investigaciones con un enfoque transversal, en una unidad especializada y dotada de los medios humanos, técnicos y logísticos necesarios para la efectividad de su trabajo.

vi. Es así, entonces, que la propuesta de fortalecimiento y unificación de capacidades aquí presentada permitirá un nuevo modelo de investigación penal en delitos cibernéticos en la PONAL, basado en la formación, análisis, articulación y compartición de información, así como cooperación, colaboración y asistencia nacional e internacional relacionados con la seguridad y judicialización de delitos en el ciberespacio.

Apéndices

Gráfica 08. Muestra la estructura jerárquica de la DICIS en la Policía Nacional.



Gráfica 09 Muestra la estructura interna de la DICIS.

Apéndice 2- Perfil de Funciones

<table>
<tr><td colspan="3">1. Nombre: Jefe Área de Prevención</td></tr>
<tr><td colspan="3">2. Grado Policial (Decreto 1791/2000)[1]</td></tr>
<tr><td>Oficiales</td><td>Nivel ejecutivo</td><td>Patrulleros</td></tr>
<tr><td>*Coronel
*Teniente Coronel
*Mayor</td><td></td><td></td></tr>
<tr><td colspan="3">3. Educación: (Ley 30/1992)[2] Familias que contienen estudios técnicos Profesionales, tecnólogos, profesionales universitarios y posgrados.</td></tr>
<tr><td>Criterio</td><td>Familia(s) pregrado</td><td>Familias posgrado</td></tr>
<tr><td>*Requiere profesional universitario</td><td>*Ingeniería electrónica
*Ingeniería de sistemas</td><td>*Ciberseguridad
*Informática forense
*Seguridad de la información</td></tr>
<tr><td colspan="3">4. Formación para el trabajo: (Ley 115/1994)[3] Actualización de conocimientos evidenciados en seminarios, cursos y diplomados.</td></tr>
<tr><td colspan="2">Criterio</td><td>Familia(s) de formación</td></tr>
<tr><td colspan="2">*Requiere cursos o seminarios</td><td>*Riesgos
*Vulnerabilidades
*Educación</td></tr>
<tr><td colspan="2"></td><td>* Estadística
*Criminalística</td></tr>
<tr><td colspan="3">5. Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al Desarrollo del proceso en el que participa el funcionario.</td></tr>
<tr><td colspan="3">o Jefe Área Atención a Incidentes (familia) [4]
o Jefe Área de investigaciones tecnológicas (familia)
o Jefe grupo Centro de respuesta en línea a incidentes informáticos
o Jefe Grupo de Sensibilización y Difusión
o Jefe Observatorio Nacional del Cibercrimen</td></tr>
</table>

Tabla 04. Formato alineado al manual de funciones de la Policía Nacional. Fuente: Policía Nacional.

---

[1] Decreto 1791 de 2000 por el cual se modifican las normas de carrera del personal de oficiales, nivel ejecutivo, suboficiales y agentes de la Policía Nacional.

[2] Ley 30 de diciembre 28 de 1992 por la cual se organiza el servicio público de la Educación superior.

[3] Ley 115 de febrero 8 de 1994 por la cual se expide la ley general de educación.

[4] Familia: hace referencia a los grupos que dependen de área, lo que significa en términos de experiencia que el haberse desempeñado como jefe de cualquier de los grupos que la componen cuenta como experiencia para este cargo.

1 **Nombre: Jefe Centro de respuesta en línea a incidentes informáticos**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos Profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas *Ingeniero Industrial	*Ciberseguridad *Gestión de proyectos *Administración
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*ITIL *COBIT *Mesa de ayuda *ISO 20000 (Mesa de ayuda)	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Grupo mesa de ayuda Oficina de Telemática o Jefe Grupos DICIS (Familia)		

<table>
<tr><td colspan="3">1 Nombre: Jefe Grupo de Sensibilización y Difusión</td></tr>
<tr><td colspan="3">2 Grado Policial (Decreto 1791/2000)</td></tr>
<tr><td>Oficiales</td><td>Nivel ejecutivo</td><td>Patrulleros</td></tr>
<tr><td>*Mayor
*Capitán</td><td></td><td></td></tr>
<tr><td colspan="3">3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, Tecnólogos, profesionales universitarios y posgrados.</td></tr>
<tr><td>Criterio</td><td>Familia(s) pregrado</td><td>Familias posgrado</td></tr>
<tr><td>*Requiere profesional universitario</td><td>*Ingeniería electrónica
*Ingeniería de sistemas
*Comunicador social</td><td>*Ciberseguridad
*Seguridad de la Información
*Comunicación interna y externa</td></tr>
<tr><td colspan="3">4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados</td></tr>
<tr><td colspan="2">Criterio</td><td>Familia(s) de formación</td></tr>
<tr><td colspan="2">*Requiere cursos o seminarios</td><td>*Manejo de público
*Expresión oral</td></tr>
<tr><td colspan="3">4 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario.</td></tr>
<tr><td colspan="3">o Jefe Grupo comunicaciones estratégicas
o Jefe Grupos DICIS (Familia)</td></tr>
</table>

1 **Nombre: Jefe Observatorio Nacional del Cibercrimen**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Teniente Coronel *Mayor *Capitán		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Psicología *Estadístico (a) *Matemático (a)	*Criminología *Ciberseguridad *Investigación
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados.		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Patrones/analítica/probabilidad	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Observatorio del Delito (DIJIN) o Jefe Grupos DICIS (Familia)		

1 **Nombre: Jefe Área Atención a Incidentes**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
* Coronel *Teniente Coronel *Mayor		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas	*Seguridad de la Información *Ciberseguridad *Ciberdefensa *Redes y telecomunicaciones *Electrónica/sistemas
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*ISO 27035(Atención a incidentes) *ISO 27002 (SGSI) *CERT/CSIRT	
	*Protección de datos personales *Continuidad del negocio	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Grupo seguridad de la información Oficina de Telemática o Jefe Grupo CSIRT-PONAL o Jefe Centro de Protección de datos unidades Policía Nacional o Jefe Grupo Administración del SGSI o Jefe Área de investigaciones tecnológicas (familia)		

1 Nombre: Jefe grupo administración SGSI		
2 Grado Policial (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas	*Seguridad de la Información *Ciberseguridad *Ciberdefensa *Redes y telecomunicaciones *Electrónica/sistemas
4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*ISO 27035(Atención a incidentes) *ISO 27002 (SGSI) *CERT/CSIRT *Protección de datos personales *Continuidad del negocio	

- Jefe Grupo seguridad de la información Oficina de Telemática
- Jefe Grupo CSIRT-PONAL
- Jefe Centro de Protección de datos unidades Policía Nacional

1 **Nombre: Jefe grupo CSIRT-PONAL**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		

3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas	*Seguridad de la Información *Ciberseguridad *Ciberdefensa *Redes y telecomunicaciones *Electrónica/sistemas *Informática forense

4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimiento evidenciados en seminarios, cursos y diplomados	
Criterio	**Familia(s) de formación**
*Requiere cursos o seminarios	*ISO 27035(Atención a incidentes) *CERT/CSIRT * Ethical Hacking *Seguridad de redes
	*Informática Forense *Análisis de malware

5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario

- Jefe Grupo seguridad de la información Oficina de Telemática
- Jefe Grupo CSIRT-PONAL
- Jefe Centro de Protección de datos unidades Policía Nacional
- Jefe Grupo Administración del SGSI
- Jefe Área de investigaciones tecnológicas (familia)

1 **Nombre: Jefe Área de investigaciones tecnológicas**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
* Coronel *Teniente Coronel *Mayor		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas *Criminalista *Abogado(a)	*Seguridad de la Información *Criminología y victimología *Derecho penal *Derecho informático *Investigación criminal
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimiento evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Investigación *Informática forense	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Seccional de Investigación criminal (familia) o Jefe Área de investigaciones tecnológicas (familia) o Jefe Área de prevención (familia)		

1 **Nombre: Jefe Grupo de protección a la información y a los datos**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas *Criminalista *Abogado(a)	*Seguridad de la Información *Criminología y victimología *Derecho penal *Investigación criminal
4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimiento evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Investigación/Informática forense	
5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Seccional de Investigación criminal (familia) o Jefe Grupos DICIS (Familia)		

1 **Nombre: Jefe Grupo contra la pornografía infantil**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas *Criminalista *Abogado(a) *Psicólogo	*Seguridad de la Información *Criminología y victimología *Investigación criminal
4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Investigación contra la pornografía infantil	
5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe Seccional de Investigación criminal (familia) o Jefe Grupos DICIS (Familia)		

1 **Nombre: Jefe Grupo contra la extorsión y el fraude**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Ingeniería de sistemas *Criminalista *Abogado(a)	*Criminología y victimología *Investigación criminal
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Contraextorsión y fraude *Criptomonedas	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
○ Jefe GAULA[5] (familia) ○ Jefe Grupos DICIS (Familia)		

[5] Grupos de acción unificada por la libertad personal de la Dirección Antisecuestro y Antiextorsión.

1 **Nombre: Jefe grupo de Ciberterrorismo**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Mayor *Capitán		
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) pregrado**	**Familias posgrado**
*Requiere profesional universitario	*Ingeniería electrónica *Criminalista *Abogado(a)	*Investigación criminal *Ciberdefensa *Ciberterrorismo
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*Policía Judicial *Investigación *Contraterrorismo	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Jefe seccional de investigación o Jefe Grupos DICIS (Familia)		

1 Nombre: Investigador de Incidentes

2 Grado Policial (Decreto 1791/2000)

Oficiales	Nivel ejecutivo	Patrulleros
*Teniente *Subteniente	*Comisario *Subcomisario *intendente *Subintendente	*Patrullero

3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.

Criterio	Familia(s) Técnico/Tecnólogo	Familias Pregrado
*Requiere Técnico/Tecnólogo Pregrado universitario	* Electrónica *Sistemas *Telecomunicaciones *Policía Judicial	*Ingeniero Electrónico *Ingeniero de Sistemas

4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados

Criterio	Familia(s) de formación
*Requiere cursos o seminarios	*ISO 27035(Atención a incidentes) *CERT/CSIRT * Ethical Hacking *Seguridad de redes
	*Informática Forense *Análisis de malware

5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario

- Analista de seguridad de la información
- Perito forense
- Analista de redes
- Administrador base de datos
- Desarrollador
- Recolector y analista de información
- Investigador judicial

1 Nombre: Analista de Seguridad de la Información		
2 Grado Policial (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Teniente *Subteniente	*Comisario *Subcomisario *intendente *Subintendente	*Patrullero
3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s)** Técnico/Tecnólogo	**Familias Pregrado**
*Requiere Técnico/Tecnólogo Pregrado universitario	* Electrónica *Sistemas	*Ingeniero Electrónico *Ingeniero de Sistemas
4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimiento evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	*ISO 27002 (SGSI) *Protección de datos personales *Continuidad del negocio	
	*Administración firewall, IPS[6], SIEM[7] y antivirus	
5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Analista de seguridad de la información o Perito forense o Analista de redes o Administrador base de datos o Desarrollador o Recolector y analista de información o Investigador judicial		

[6] Sistema de prevención de intrusos
[7] Sistema de correlación de eventos

1 **Nombre: Investigador Judicial**		
2 **Grado Policial** (Decreto 1791/2000)		
Oficiales	**Nivel ejecutivo**	**Patrulleros**
*Teniente *Subteniente	*Comisario *Subcomisario *intendente *Subintendente	*Patrullero
3 **Educación**: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.		
Criterio	**Familia(s) Técnico/Tecnólogo**	**Familias Pregrado**
*Requiere Técnico/Tecnólogo Pregrado universitario	* Policía Judicial *Criminalista *Sistemas *Electrónica	*Ingeniero Electrónico *Ingeniero de Sistemas *Abogado *Criminalista
4 **Formación para el trabajo**: (Ley 115/1994) Actualización de conocimiento evidenciados en seminarios, cursos y diplomados		
Criterio	**Familia(s) de formación**	
*Requiere cursos o seminarios	* Policía Judicial *Investigación	
	*Contraterrorismo *Contraextorsión y fraude *Criptomonedas * Contra la pornografía infantil	
5 **Experiencia**: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario		
o Perito forense o Recolector y analista de información		

1 Nombre: Perito Informático

2 Grado Policial (Decreto 1791/2000)

Oficiales	Nivel ejecutivo	Patrulleros
*Teniente *Subteniente	*Comisario *Subcomisario *intendente *Subintendente	*Patrullero

3 Educación: (Ley 30/1992) Familias que contienen estudios técnicos profesionales, tecnólogos, profesionales universitarios y posgrados.

Criterio	Familia(s) Técnico/Tecnólogo	Familias Pregrado
*Requiere Técnico/Tecnólogo Pregrado universitario	* Policía Judicial *Criminalista *Sistemas *Electrónica *Forense	*Ingeniero Electrónico *Ingeniero de Sistemas *Abogado *Criminalista *Informática forense

4 Formación para el trabajo: (Ley 115/1994) Actualización de conocimientos evidenciados en seminarios, cursos y diplomados

Criterio	Familia(s) de formación
*Requiere cursos o seminarios	* Policía Judicial
	*Forense móvil, base de datos, red *Análisis de malware *Fuentes abiertas *Pentesting *Seguridad de redes

5 Experiencia: Cargos de menor o igual nivel de responsabilidad que aportan al desarrollo del proceso en el que participa el funcionario

- Perito forense
- Recolector y analista de información
- Investigador de incidentes
- Analista de seguridad de la información

Bibliografía

AMERIPOL -Comunidad de Policias de America. (s.f.). *AMERIPOL*. Obtenido de http://www.ameripol.org/portalAmeripol/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m2p1p2&content_id=20162&folderNode=20127.

Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677. (2014). *Cibercrimen: particularidades en su investigación y enjucionamiento* .

APA . (2018). *Documento Normas APA.* Obtenido de http://normasapa.net/marco-metodologico-tesis/

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

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

Bejarano, M. J. (2011). Documento informativo IEEE.

CC-CSIRT POLICIA . (2018). *https://cc-csirt.policia.gov.co/Publicaciones/quienes_somos.* Obtenido de https://cc-csirt.policia.gov.co/Publicaciones/quienes_somos

CCDOE NATO Coopertaive Cyber Defence Centre of Excellence. (s.f.). *Tallin proceso Manual* . Obtenido de https://ccdcoe.org/tallinn-manual.html

Centro Cibernetico Policial - Capitan Miranda. (2018). *Centro Ciberetico Policial* . Obtenido de https://caivirtual.policia.gov.co/

Centro Cibernetico Policial - Policia Nacional . (Junio de 2018). *Centro Cibernetico Policial.* Obtenido de Centro Cibernetico Policial

CGFM Planeación por Capacidades. (02 de 03 de 2017). *Comando General de las Fuerzas Militares ¨Planeación por Capacidades¨.* Obtenido de http://www.cgfm.mil.co/2017/03/02/transformacion-basada-planeacion-capacidades/

CIBERNÉTICA, O. S. (2018). Obtenido de https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

Ciberoperaciones - Héctor Gómez Arriagada. (Abril de 2013). *Monografias y ensayos: ciberoperaciones.* Obtenido de https://revistamarina.cl/revistas/2013/4/gomez.pdf

CISCO. (2018). *Reporte Anual de Ciberseguridad.* Obtenido de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

Comando Conjunto Cibernético. (2018). *Comando Conjunto Cibernético*. Obtenido de https://www.ccoc.mil.co/

Comision de Regulacion de Comunicaciones . (Mayo de 2018). *Comision de Regulacion de Comunicaciones* . Obtenido de https://www.crcom.gov.co/es/pagina/inicio

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

Consejo de Europa en Estrasburgo. (2001). *Convenio Sobre la Ciberdelincuencia* . Council Europe, Budapest. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Constitución Politica de Colombia 1991. (s.f.). Obtenido de https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Convenio sobre la Ciberdelincuencia . (2011). Budapest.

Daft, R. L. (2015). *Teoría y diseño organizacional.* Cengage Learning.

Daniel, F. B. (2018). *Ciberseguridad Ciberespacio y Ciberdelincuencia.*

Departamento Nacional de Planeación . (2014). *Bases del Plan Nacional de Desarollo 2014-2018*. Obtenido de https://www.minagricultura.gov.co/planeacion-control-gestion/Gestin/Plan%20de%20Acci%C3%B3n/PLAN%20NACIONAL%20DE%20DESARROLLO%202014%20-%202018%20TODOS%20POR%20UN%20NUEVO%20PAIS.pdf

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

Departamento Nacional de Planeación. (11 de Abril de 2016). *CONPES 3854*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento Nacional de Política Económica y Social. (14 de Julio de 2011). *Documentos Conpes 3701*. Recuperado el 21 de Noviembre de 2016, de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

DINAE Policía Nacional de Colombia . (2018). *Documento Dirección Nacional de Escuelas*. Obtenido de https://www.policia.gov.co/direcciones/educacion-policial

Económica, C. N. (2016). *Consejo Nacional de Política Económica y Social, 2016.*

EFE Agencia. (10 de Febrero de 2015). *Gobierno crea agencia para detectar amenazas ciberneticas y evitar ataques*. Recuperado el 21 de Noviembre de 2016, de http://www.efe.com/efe/usa/sociedad/gobierno-crea-agencia-para-detectar-amenazas-ciberneticas-y-evitar-ataques/50000101-2533620

Enter.co Enterprise. (2016). *Microsof abrensu laboratorio global contra el cibercrimen.* Recuperado el 21 de Noviembre de 2016, de http://www.enter.co/especiales/enterprise/microsoft-abre-su-laboratorio-global-contra-el-cibercrimen/

ESPAÑA, R. I. (2015). Obtenido de https://blog.realinstitutoelcano.org/reto-la-ciberdefensa-la-union-europea/

Europol. (2016). *European Cybercrime Centre-EC3*. Recuperado el 21 de Noviembre de 2016, de https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-1

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

Fiscalía General de la Nación. (2018). *Fiscalia General de la Nación*. Obtenido de https://www.fiscalia.gov.co/colombia/

Grupo de Delitos Telemáticos Unidad Central Operativa. (2011). *GDT Grupo de Delitos Telemáticos Unidad Central Operativa*. Recuperado el 21 de Noviembre de 2016, de https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Guardia Di Finance. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Guardia_di_Finanza

HERNÁNDEZ, D. M.-J. (2014). *Cibercrimen: particularidades en su.* Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677.

Interpol. (s.f.). *Interpol Connecting Polica For a Safer Word.* Recuperado el 21 de Noviembre de 2016, de 2016: https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI

Lewis, J. A. (2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad.* Bogotá.

Ley 1273, 2009. (s.f.). *2009.*

Ley de Delitos Informáticos . (2009).

LLINARES, F. M. (2015). *LA OPORTUNIDAD CRIMINAL EN EL CIBERESPACIO.* Revista Electrónica de Ciencia Penal y Criminología.

MAYA, R. P. (2017). *Los cibercrímines: un nuevo paradigma de criminalidad* . Bogotá: Universidad de los Andes.

Mayor MILENA ELIZABETH REALPE DIAZ - Jefe de Prospectiva y Cooperación del Comando Conjunto Cibernético - CCOC . (29 de Noviembre de 2017). *LA CIBERDEFENSA EN COLOMBIA* . Obtenido de https://www.cci-es.org/documents/10694/468834/3.+CCOC+PLAN+NACIONAL.pdf/84da120e-3bd6-478c-99c8-1f88c3543355;jsessionid=5E61914D5E08633E7DD315CB4A68FC94?version=1.0

Mayor Saavedra - Centro Cibernetico Policial. (s.f.). Obtenido de https://caivirtual.policia.gov.co/

Ministerio de Defensa . (2016). *el Plan Estratégico del Sector Defensa y Seguridad – Guía de planeamiento estratégico 2016-2018*. Obtenido de https://www.mindefensa.gov.co/.../Mindefensa/.../Planeacion/.../Guia_Planeamiento_E...

Ministerio de Defensa. (Marzo de 2011). *Documento Infromativo del IEEE 09/2011*. Recuperado el 21 de Noviembre de 2016, de Nuevo Concepto de la OTAN: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

Ministerio de Defensa Nacional - Policia Nacional de Colombia. (2018). *Centro Cibernetico Policial*. Recuperado el 21 de Noviembre de 2016, de http://www.ccp.gov.co/

Ministerio de Defensa Nacional. (Mayo de 2016). *Visión de Futuro de las Fuerzas Armadas*. Obtenido de https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estrategia_planeacion/proyeccion/documentos/vision_futuro_FA.pdf

Ministerio de las Tecnologias de la Información y las Comunicaciones. (01 de Mayo de 2018). Obtenido de https://www.mintic.gov.co/portal/604/w3-article-3707.html

Ministerio de las Tecnologias y Comunicaciones - MINTIC. (Octubre de 2018). Obtenido de https://www.mintic.gov.co/portal/604/w3-article-6120.html

MInisterio de las Telecomunicaciones y de la Información - MINTIC. (s.f.). Obtenido de https://www.mintic.gov.co

Ministerio de Relaciones Exteriores. (06 de Septiembre de 2018). *www.Cancilleria.gov*. Obtenido de http://www.cancilleria.gov.co/en/newsroom/news/2018-06-25/19306

MINTIC. (2018). *'Creación de una trayectoria profesional en seguridad digital'.*

Monografias. (2005). *Métodos y metodologías aplicadas en tesis y monografías de relaciones públicas.*

Naciones Unidas -12° Congreso de las Naciones Unidas Sobre la Prevención del Delito y Justicia Penal . (2010). *Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el del delito cibernético* . Brasil .

Office of the Director or National Intelligence. (2016). *Office of the Director or National Intelligence - united States of America.* Recuperado el 21 de Noviembre de 2016, de https://www.dni.gov/index.php/contact-us

Organización de Estados Americanos - OEA. (2018). *Seguridad Cibernética.* Obtenido de https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

Organización de los Estados Americanos . (2018). *Seguridad CIbernetica* . Obtenido de http://www.oas.org/es/temas/seguridad_cibernetica.asp

Organization of American States (OEA) - Banco Interamericano de Desarrollo (BID). (2016). *OBSERVATORIO DE LA CIBERSEGURIDAD EN AMERICA LATINA Y EL CARIBE.* Obtenido de https://publications.iadb.org/.../Ciberseguridad-Estamos-preparados-en-America-Latina-...

OTAN. (2015). *OTAN -Organización del Tratado del Atlántico Norte.* Obtenido de https://www.nato.int/nato-welcome/index_es.html

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

Policia Nacioanal-Centro-Capacidades-Ciberseguridad. (06 de Agosto de 2018). *https://www.policia.gov.co/noticia/policia-nacional-inaugura-centro-capacidades-ciberseguridad-colombia-c4*. Obtenido de https://www.policia.gov.co/noticia/policia-nacional-inaugura-centro-capacidades-ciberseguridad-colombia-c4

Policia Nacional - CAI VIRTUAL . (2018). *https://caivirtual.policia.gov.co/contenido/cai-virtual-0.* Obtenido de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Policia Nacional - Centro-Capacidades-Ciberseguridad-Colombia-C4. (06 de Junio de 2018). *Centro-Capacidades-Ciberseguridad-Colombia-C.* Obtenido de

https://www.policia.gov.co/noticia/policia-nacional-inaugura-centro-capacidades-ciberseguridad-colombia-c4

POLICIA NACIONAL - DIPON - OFITE -ARADI. (2011). *EVOLUCION DE LA CIBERSEGURIDAD - CSIRT PONAL - Capitán ALEX URIEL DURAN SANTOS.* Bogotá .

Policia Nacional - Dirección Nacional de Escuelas . (Mayo de 2018). *Dirección Nacional de Escuelas - Maestría en Ciberseguridad e Informatica Forense*. Obtenido de https://www.policia.gov.co/sites/default/files/convocatoria-docentes-realizar-maestria-ciberseguridad-informatica-forense.pdf

Policia Nacional - Escuela de Telematica. (Mayo de 2018). *Escuela de Tecnologías de la Información y las Comunicaciones "Teniente Coronel Jorge Luis Mauledoux Barón" - ESTIC*. Obtenido de https://www.policia.gov.co/escuelas/telematica

Policia Nacional - Infancia -Adolecencia. (mayo de 2018). Obtenido de https://www.policia.gov.co/especializados/infancia-adolescencia

Policia Nacional - Informe 'Amenazas del Cibercrimen en Colombia 2016-2017'. (Marzo de 2017). *Informe: Amenzas del Cibercrimen en Colombia 2016-2017*. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Policia Nacional - Investigación Criminal . (s.f.). Obtenido de https://www.policia.gov.co/direccion/investigacion-criminal

Policia Nacional - Plan Estrategico Institucional -Vision 2030. (s.f.). *Plan Estrategico Institucional - Visión 2030.* Obtenido de https://www.policia.gov.co/sites/default/files/descargables/plan-estrategico-institucional-2015-2018.pdf

Policia Nacional - PONAL. (s.f.). Obtenido de https://www.policia.gov.co/

Policia Nacional de Colombia - CSIRT-PONAL. (2015). *CSIRT-PONAL*. Recuperado el 21 de Noviembre de 2016, de https://cc-csirt.policia.gov.co/

Policía Nacional de Colombia - PONAL. (8 de Noviembre de 2018). Obtenido de https://www.policia.gov.co/mision-vision-mega-principios-valores-funciones

Policia Nacional de Colombia. (2015). *CSIRT-PONAL*. Recuperado el 21 de Noviembre de 2016, de https://cc-csirt.policia.gov.co/

Revista de la OTAN. (Febrero de 2018). *OTAN*. Obtenido de https://www.nato.int/docu/review/2011/11-september/cyber-threads/es/index.htm

Rodríguez, N. S.-B.-J. (2017). *La significativa evolución en seguridad de la información para la Policía.* Bogotá: Revista LOGOS CIENCIA & TECNOLOGÍA.

THIBER. (2016). Obtenido de THIBER: http://www.thiber.org/2016/07/07/nuevo-paso-de-la-otan-en-la-ciberdefensa/

UNODC-United Nations Office on Drugs and Crime. (2013). *Estudio exhaustivo sobre el delito cibernético* .

Wilson Bernardo Guerrero Romero. (s.f.). *DOCUMENTO CONPES 3701 LINEAMIENTOS DE POLITICAS PARA LA CIBERSEGURIDAD Y CIBERDENSA* . Bogotá: Seminario de Investigación Aplicada, Universidad Piloto de Colombia.

www.gobiernoellinea.gov.co. (11 de Julio de 2018). *http://estrategia.gobiernoenlinea.gov.co/623/w3-article-75639.html*. Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-article-75639.html

www.webinfomil.com. (2015). *Colombia tendra Gaula élite y Cibergaula* . Obtenido de http://www.webinfomil.com/2015/02/colombia-tendra-gaula-elite-y-cibergaula.html