Fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP

William Muñoz Rojas

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL DE LAS FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

FORTALECIMIENTO DE LAS CAPACIDADES TECNOLÓGICAS DEL CENTRO CIBERNÉTICO POLICIAL CCP

ALUMNO: MY WILLIAM MUÑOZ ROJAS

DIRECTOR: MAGISTER STEVEN JONES CHALJUB

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTA – COLOMBIA

2018

Página de aceptación del trabajo

"El trabajo deberá incluir una constancia de aprobación por parte de la coordinación del área de investigaciones de cada programa o maestría en donde se manifieste que el trabajo cumple los requisitos para ser sustentado ante el jurado evaluador. Dicha constancia sólo podrá ser emitida previo cumplimiento del requisito del formato de evaluación diligenciado por el docente de investigación y el tutor temático, o, según lo disponga el programa o departamento respectivo".

Dedicatoria y agradecimientos

Dedico este proyecto de grado a mi familia quienes me han brindado todo el apoyo en todo momento proporcionándome el buen ejemplo y depositaron su esperanza en mí.

A los docentes de la maestría quienes dieron lo mejor en cada curso para guiarme y enseñarme.

A todos los que me apoyaron para escribir y concluir este proyecto de grado.

Para ellos es esta dedicatoria de proyecto de grado, pues es a ellos a quienes se las debo por su apoyo incondicional.

Resumen

La problemática derivada del masivo uso del ciberespacio por parte de la sociedad en general, como parte del ejercicio social y económico ha derivado en la proliferación de cibercrimenes que requieren del estado y de la sociedad de mecanismos tecnológicos efectivos, que brinden capacidades para la atención integral de incidentes de naturaleza cibernética, operacionalizando las políticas públicas en materia de seguridad digital, ciberseguridad y ciberdefensa, mediante la implementación de nuevas capacidades para el análisis de malware, la utilización de nuevo software open source y la predicción del delito cibernético para facilitar la investigación criminal como parte de las capacidades propuestas para el Centro Cibernético Policial CCP, apoyando el cumplimiento de su misionalidad con una adecuada prevención, investigación y judicialización de los delitos informáticos, mediante la utilización de herramientas proporcionadas por las tecnologías de la información.

Palabras clave: cibercrimen, ciberespacio, CONPES, Centro Cibernético Policial CCP, condiciones y capacidades tecnológicas.

Abstract

The problematic derived from the massive use of the cyberspace by the society in general, as part of the social and economic exercise has resulted in the proliferation of cybercrime that require by the state and the society of effective technological mechanisms, that provide capacities for the comprehensive cybersecurity incidents, operating public policies on digital security, cybersecurity and cyber-defense, by implementing new capabilities for malware analysis, the use of new open source software and prediction of cybercrime to facilitate criminal investigation as part of the capabilities proposed for the CCP Police Cyber Center, supporting the fulfillment of its missionary responsibility with adequate prevention, investigation and prosecution of computer crimes, to the use of tools provided by information technologies.

key words: cybercrime, cyberspace, CONPES, Police Cyber Center, technological conditions and capabilities.

Tabla de contenido

Introducción

El creciente uso de las TIC's por toda la sociedad, la expansión de las redes de telecomunicaciones, las tendencias internacionales muestran que la inversión en la ciberseguridad es dinámico y crece continuamente resultando un espacio para el desarrollo económico y profesional.

Las amenazas en el entorno digital son numerosas y cada vez más sofisticadas, espacio aprovechado por los ciberdelincuentes ante la falta de mecanismos de protección y el desconocimiento de la comunidad sobre los riesgos asociados al uso del ciberespacio.

El Centro Cibernético Policial también conocido como CCP, cumple con funciones y responsabilidades administrativas, operativas sobre la investigación y la toma de decisiones dentro del proceso de investigación del cibercrimen, la pornografía infantil, los delitos financieros, delitos en la infraestructura crítica y el ciberterrorismo.

El CCP es una dependencia operativa de la Dirección de Investigación Criminal e INTERPOL (DIJIN e INTERPOL) de la Policía Nacional, creada por el gobierno nacional respondiendo a las expectativas del CONPES 3701.

Las Capacidades de la Policía Nacional ayudan a cumplir y hacer sostenible el Plan Estratégico Institucional "Comunidades Seguras y en Paz", en coherencia con la oferta de valor institucional y con las definiciones estratégicas.

Los indicadores de gestión de la DIJIN e INTERPOL, sobre la meta para contrarrestar los fenómenos de criminalidad y las contravención de manera focalizada y diferencial, mostraron un incumplimiento de los indicadores sobre reportes de hurto a celulares, desarticulación de estructuras de crimen organizado y la efectividad de la investigación criminal, estos indicadores son compartidos por todas las dependencias de la DIJIN e INTERPOL incluido el CCP.

La responsabilidad sobre la ciberseguridad no es exclusiva del CCP existen varias unidades encargadas de la ciberseguridad en Colombia.

El CCP en los últimos cinco (5) años ha realizado grandes adquisiciones de tecnología de la información relacionada con las condiciones y capacidades para la atención de ciberdelitos cuya información es de carácter pública.

Las adquisiciones tecnológicas realizadas por la DIJIN e INTERPOL para el CCP y la información publicada permitió proponer las capacidades del CCP como: CAI virtual, laboratorio forense y análisis de información estructurada y no estructurada.

La identificación del componente tecnológico y las herramientas necesarias para el CCP tuvo en cuenta el desempeño de los indicadores, las actuales capacidades propuestas para el CCP y los delitos informáticos para proponer el fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP a través de la implementación del C4 (Centro de mando, Control, Comunicaciones y Computación), el análisis de malware estático y dinámico, la predicción del delito cibernético y el uso de software open source en la investigación criminal.

1. Problemática del cibercrimen en Colombia

Durante los últimos 3 años a través de las plataformas dispuestas por Centro Cibernético Policial se recepcionaron 15.565 incidentes informáticos.

1.1 Caracterización de los delitos informáticos y las víctimas del cibercrimen

A partir del análisis de información, se identificaron aspectos comunes que permiten caracterizar el delito informático en Colombia según el informe del cibercrimen en Colombia 2016-2017, publicado por el Centro Cibernético Policial CCP, así:

1. El cambio en la selección de las víctimas, pasando del ciudadano común a las grandes empresas del sector público-privado, las cuales generan una mayor rentabilidad a la actividad criminal.
2. Nuevas plataformas de comercio electrónico utilizadas para estafar a través de phishing.
3. Servicios de Gobierno electrónico como vector de ataque para la distribución de malware.
4. La participación activa de personas con acceso a información privilegiada o sensible de la víctima a través de BEC (Business Email Compromise).
5. Vinculación cada vez más frecuente de ciudadanos extranjeros en las organizaciones criminales con injerencia en Colombia.
6. Presencia de usuarios Colombianos en la Deep Web.
7. Uso del Internet como herramienta de amenazas e instigación a delinquir.
8. Uso de monedas virtuales como formas de pago.

1.1.1 Ciberespacio.

El concepto de ciberespacio resulta más compleja de lo que podría parecer en la primera impresión ya que resulta de la unión de dos vocablos el de la cibernética y el espacio tal como lo describe Cicognani "el término ciber+espacio, el espacio asume el significado de *'materia física'* mientras que el ciber le da su característica *'inmaterial'* " (2007, p 35).

Definido por Gibson en un lenguaje metafórico como "una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos" (2002, p.69).

La Comisión de Regulación de Comunicaciones (en adelante CRC) reglamentó una definición del ciberespacio de manera técnica como "el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios" (Colombia, CRC, 2009, Resolución 2258, Art. 1).

1.1.2. Cibercrimen.

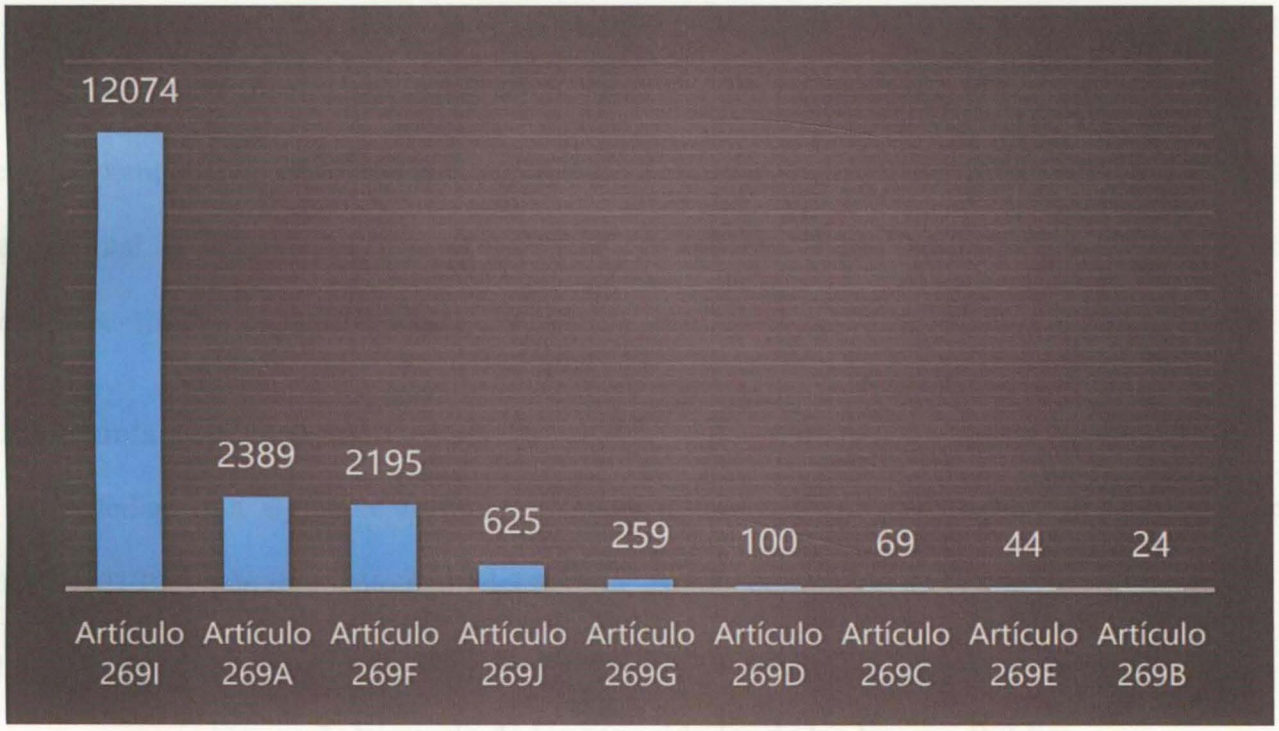
Desde la perspectiva de la seguridad nacional Cibercrímen (delito cibernético) es considerado como el "conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio" (Colombia, CONPES, 2017, p.15).

1.2 Ley 1273 de 2009

Según lo informado por el CCP durante los años 2014, 2015, 2016 y hasta el 10/03/2017, se han recibido 13.774 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país.

En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en el citado periodo de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades público-privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula en el ciberespacio.

Figura 1- Delitos informáticos denunciados en 2014, 2015, 2016 y hasta el 10/03/2017



Nota: Tomada del informe del cibercrimen en Colombia 2016-2017 (2017).

Siendo el artículo 269I hurto por medios informáticos y semejantes la tipología criminal de mayor frecuencia, equivalente al 68%, seguido de Artículo 269A acceso abusivo a un sistema informático con el 13% y el artículo 269F violación de datos personales con el 12%.

2 Capacidades de la Policía Nacional

2.1 Definición de la capacidad

La definición de capacidad hace referencia a la "habilidad de realizar una tarea, bajo ciertos estándares (como tiempo, ambiente o nivel de alistamiento específicos) a través de la combinación de diferentes medios (personal, equipo e infraestructura) y modos (doctrina, organización y arte operacional)".

Las capacidades distintivas son todas aquellas habilidades, destrezas, conocimientos y experticias que la Institución debe saber hacer especialmente bien, y que se convierten en ventajas competitivas de tal manera que ayudan a cumplir y a hacer sostenible el Plan Estratégico Institucional "Comunidades Seguras y en Paz", en coherencia con la oferta de valor institucional y con las definiciones estratégicas.

2.2 Fórmula de la capacidad

Mediante la siguiente fórmula se puede establecer que las Capacidades de la Fuerza Pública (CFP), en un momento dado del tiempo, estarán en función de la doctrina, el material y el equipo, la organización, el personal y la infraestructura con los que se cuenta en ese momento:

Figura 2- Fórmula de las capacidades de las Fuerza Pública

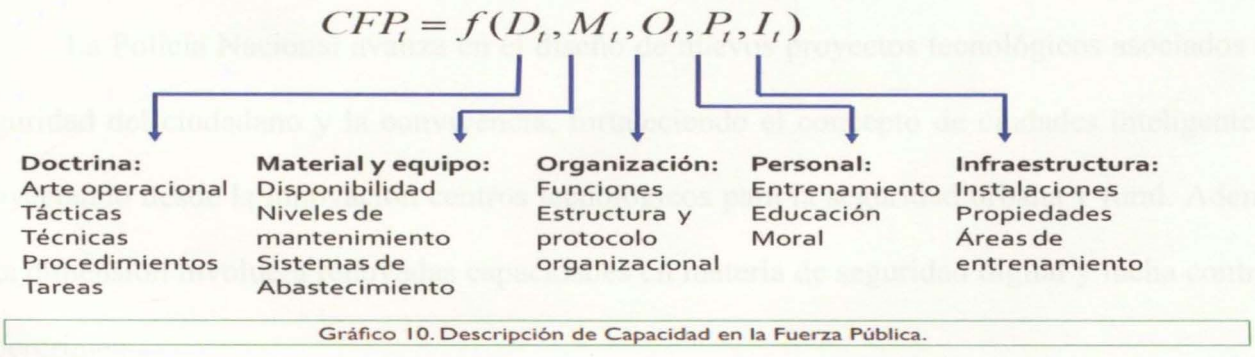


Gráfico 10. Descripción de Capacidad en la Fuerza Pública.

Nota: Tomada de Plan Estratégico Institucional Comunidades Seguras y en Paz 2015-2018 (2015).

2.3 Agrupaciones de capacidades de la Policía Nacional

La Policía Nacional ha definido y priorizado las siguientes agrupaciones de capacidad, así:

Policía judicial, criminalística, modelo nacional de vigilancia comunitaria por cuadrantes, seguridad rural, inteligencia y contrainteligencia policial, control de disturbios y manifestaciones sociales, espectáculos y eventos públicos, operaciones matriz operacional integrada policial, seguridad digital, TIC para conectividad, cobertura y movilidad, prevención, movilidad: vehículos, lanchas y semovientes equinos, Intervenciones policiales, control y protección ambiental, vigilancia y movilidad aérea, Infancia y adolescencia, control y seguridad policial, control NBQRE (nuclear, biológico, químico, reactivo, explosivo), gestión del riesgo de desastres, seguridad y movilidad en el tránsito multimodal y negociación y manejo de crisis.

Con el desarrollo de capacidades en policía judicial, administración de información judicial e investigación criminal, lideradas por la Dirección de Investigación Criminal e Interpol, se plantea responder a los retos que surgen frente a todo tipo de criminalidad y el apoyo a la justicia.

2.4 Desarrollo tecnológico para el servicio

La Policía Nacional avanza en el diseño de nuevos proyectos tecnológicos asociados a la seguridad del ciudadano y la convivencia, fortaleciendo el concepto de ciudades inteligentes, y proyectando desde la innovación centros tecnológicos para la seguridad urbana y rural. Además, esta dimensión involucra renovadas capacidades en materia de seguridad digital y lucha contra el cibercrimen.

2.5 Capacidades en Investigación Criminal

Las capacidades técnicas, tecnológicas e investigativas con las que cuenta la Institución a nivel nacional, regional y local, a través de la Dirección de Investigación Criminal e Interpol y en corresponsabilidad con las direcciones operativas (Antinarcóticos, Tránsito y Transporte, Antisecuestro y Antiextorsión, Carabineros y Seguridad Rural y Policía Fiscal y Aduanera), posibilita la administración de información y el desarrollo efectivo de la investigación judicial y criminalística para obtener resultados de impacto sobre los eslabones de las diferentes cadenas criminales, así como la identificación y desarticulación de las estructuras delincuenciales de mayor afectación a la seguridad pública y la seguridad ciudadana.

2.6 Balance de los indicadores de la DIJIN II trimestre de 2017

Según el Informe integral de la Gestión Institucional II Trimestre de la Policía Nacional, presenta el balance de los indicadores de la Dirección de Investigación Criminal e Interpol DIJIN, unidad policial de la que depende operativamente y administrativamente el CCP, el cual suma a las actividades operativas de la DIJIN e INTERPOL.

Tabla 1 – Indicadores de gestión de la DIJIN (II trimestre de 2017)

META	INDICADOR	DESEMPEÑO	EXPLICACIÓN
Contrarrestar los fenómenos de criminalidad y la contravención de manera focalizada y diferencial.	**Efectividad de la Investigación Criminal**	**Básico 84,28%** **Meta: 100%** **Resultado: 84,28%**	Este indicador se mide con las personas capturadas frente a las personas identificadas pertenecientes a bandas de delincuencia común y organizaciones asociadas a la Matriz Operacional Integrada Policial. Para el primer semestre, se identificaron 1.056 personas y se capturaron 890, demostrando una efectividad en la investigación criminal del 84,28% mejorando la del año pasado la cual ascendía a 70,65%.
	Desarticulación de estructuras de Crimen Organizado	**Deficiente** **0%** **Meta: 2** **Resultado: 0**	Para el primer semestre la meta proyectada fue de dos desarticulaciones de estructuras de crimen organizado pero no se presentó avance dado el pie de fuerza y outsourcing criminal de estas estructuras. Sin embargo, se logró la afectación en el componente estructural con las capturas de varios de sus cabecillas y/o integrantes de los Grupos Armados Organizado - GAO y los Grupos Delictivos Organizado – GDO, así: clan del golfo 319, los puntilleros 39, los pelusos 25, la construu 3, cordillera 20, la empresa 9, los botalones 1, los caqueteños 0, los costeños 1, los rastrojos 2, odines 28, oficinas de cobro 2 y los pachenka 25.
	Incidentes cibernéticos atendidos	**Satisfactorio** **100,50%** **Meta: 4.035** **Resultado: 4.055**	En el primer semestre se atendieron 4.055 incidentes cibernéticos atendidos, frente a 4.035 planteados en la meta, lo cual indica que la tendencia del cibercrimen es al aumento y se requiere del aumento de personal idóneo en este tipo de investigaciones para dar solución a los ciudadanos víctimas de estafa, suplantación de identidad, malware, phishing y la amenaza por redes sociales.
	Reportes de hurto a celulares	**Deficiente** **37.37%** **Meta: 225.708** **Resultado: 367.060**	De acuerdo a la información consolidada en la base de datos negativa "corte inglés", durante el segundo trimestre se evidenció un incremento en el número de los reportes del 7% con respecto al año anterior. No obstante se evidencia una reducción en cuatro (4) ciudades de las cuales se destacan: Bucaramanga con un -12%, seguida Villavicencio con -7, Ibagué con -6% y Cali -5%. Así mismo, se vienen adelantado una serie de actividades operativas tales como capturas 10.634, incautaciones equipos terminales móviles 24.502 y recuperaciones equipos terminales móviles 11.164, con el fin de afectar los diferentes eslabones de la cadena criminal que permitan reducir el delito de hurto de celulares y en consecuencia el reporte de celulares hurtados.

Nota: Elaboración propia a partir de datos tomados del Informe integral de la Gestión Institucional II Trimestre (2017).

3. Políticas públicas de ciberseguridad

3.1 CONPES 3701 de 2011

El Consejo Nacional de Política Económica y Social, estableció los lineamientos de política para ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional para contrarrestar el incremento de las amenazas informáticas que afectan significativamente al país. La problemática central se fundamenta en la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto.

A partir de ello se establecieron las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia.

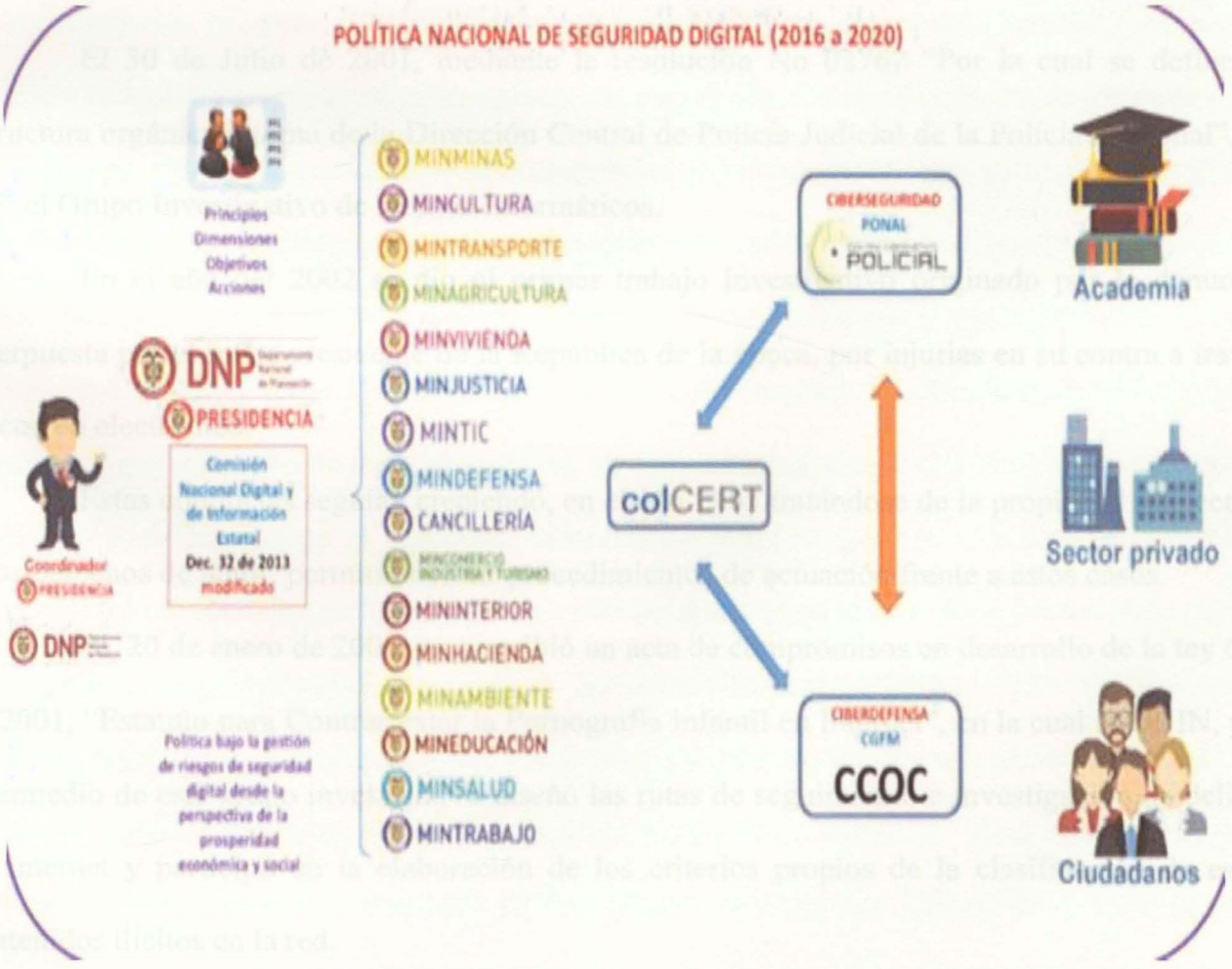
Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 "Prosperidad para Todos", como parte del Plan Vive Digital.

3.2 CONPES 3854 de 2017

El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países. Es precisamente por esto que la política nacional de seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más

importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

Figura 3- Visión de la política nacional de seguridad digital (2016 a 2020)



Nota: Tomada de la presentación de la política nacional de seguridad digital (2016).

4. Unidades encargadas de la ciberseguridad en Colombia

4.1 Centro Cibernético Policial

La Policía Nacional a través de la DIJIN e INTERPOL hace frente y adelanta investigaciones a todas las formas del crimen, de este modo la Institución ha recomendado las pautas al Gobierno Nacional y lo actualiza en las nuevas tendencias y amenazas del crimen organizado en Colombia.

Los delitos informáticos datan desde hace varios años en el país lo que ha permitido a la Policía Nacional crear un grupo especial para atender estas necesidades, promoviendo políticas y la reestructuración en las formas penales para el buen uso del ciberespacio.

El 30 de Julio de 2001, mediante la resolución No 02762 "Por la cual se define la estructura orgánica interna de la Dirección Central de Policía Judicial de la Policía Nacional", se creó el Grupo Investigativo de Delitos Informáticos.

En el año del 2002 se dio el primer trabajo investigativo originado por la denuncia interpuesta por el señor presidente de la República de la época, por injurias en su contra a través de correo electrónico.

Estas conductas seguían creciendo, en el año 2003 tratándose de la propiedad intelectual y los derechos de autor, permitió definir procedimientos de actuación frente a estos casos.

El 20 de enero de 2004, se suscribió un acta de compromisos en desarrollo de la ley 679 de 2001, "Estatuto para Contrarrestar la Pornografía infantil en Internet", en la cual la DIJIN, por intermedio de este grupo investigativo diseñó las rutas de seguimiento e investigación de delitos en Internet y participó en la elaboración de los criterios propios de la clasificación de estos contenidos ilícitos en la red.

Algunos de los resultados obtenidos están reflejados en varias operaciones que fueron consolidando al grupo, tales como: la operación enigma, operación navidad legal 2003, operación ciberpiratas y operación llave electrónica 2005.

En el año 2010 se cambia la denominación a Grupo Investigaciones Tecnológicas y participa en una serie de capacitaciones, seminarios y experiencias exitosas en los Estados Unidos, Chile, España y Bolivia, incorporando el talento humano del nivel ejecutivo, suboficiales y de oficiales con conocimientos en tecnología e ingeniería de sistemas.

El Gobierno Nacional observó que la capacidad del Estado para enfrentar las amenazas cibernéticas presentaba grandes debilidades. Pese a que se contaba con iniciativas gubernamentales, privadas y de la sociedad civil que buscaban contrarrestar su efecto, no existía una coordinación interinstitucional apropiada, de este modo, Colombia era uno de los países que no tenía una estrategia nacional en ciberseguridad y ciberdefensa, que incluyera un sistema organizacional y un marco normativo e institucional lo suficientemente fuerte para afrontar los nuevos retos en aspectos de seguridad cibernética.

Además del creciente aumento de usuarios de Internet, la elevada dependencia de la infraestructura crítica nacional a los medios electrónicos, así como el notables incremento de incidentes y delitos contra la seguridad cibernéticas, tales como el uso de Internet con fines terroristas, el sabotaje de servicios, espionaje y hurto por medios electrónicos, entre otros.

Para responder a esta necesidad, el Gobierno Nacional definió el CONPES 3701 en el año 2011 formulando la política de ciberseguridad y ciberdefensa, el cual estaba a cargo de las entidades involucradas tales como el Ministerio de Defensa, colCERT (Grupo de respuesta a incidentes cibernéticos de Colombia), CCOC (Comando Conjunto Cibernético), CCP (Centro

Cibernético Policial), de este modo se buscó una colaboración activa para la resolución de incidentes cibernéticos en el país.

El grupo se transformó en un área después de la aprobación del CONPES 3701 de 2011, lo que le permitió investigar el delito apoyándose en grupos especializados para atender las diferentes modalidades del delito informático, como lo fueron: el Grupo Investigativo en Ciberterrorismo GICIB, el Grupo de Investigativo Delitos Contra la Información y los datos GIDAT, el Grupo Investigativo Delitos Contra la Pornografía Infantil y otros Abusos en Internet GRUPI y el Grupo Nacional de Laboratorios de Informática Forense GRULAF.

En relación con la seguridad cibernética, Colombia también ha sido objeto de ataques, un caso a resaltar fue el recorrido durante el primer semestre de 2011, cuando el grupo hactivista autodenominado Anonymous atacó a los portales de la Presidencia, los Ministerios del Interior y de Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas Web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos anexos a Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que cuentan PayPal, el banco Suizo Post Finance, MasterCard, Visa y páginas Web del gobierno suizo.

También se pueden mencionar las denuncias reportadas por los ciudadanos a la Policía Nacional. De enero a diciembre de 2009, con base en la Ley 1273/09; se atendieron 575 delitos informáticos, que van desde el acceso abusivo a un sistema informático (259) hasta el hurto por medios informáticos y semejantes (247), interceptación de datos informáticos (17), la violación de datos personales (35), la transferencia no consentida activos (8), la suplantación de sitios Web (5), el daño informático (3) y la obstaculización ilegitima de un sistema informático (1). Así mismo, durante el 2010, la cantidad de delitos y contravenciones aumento en 7% al alcanzar un

total de 995 delitos informáticos, siendo el hurto por medios informáticos el incremento más representativo al pasar de 247 a 502 delitos equivalente al 103%.

A través de la Resolución No. 05839 de 2015 se creó el centro cibernético policial CCP que es la actual estructura orgánica de la DIJIN e INTERPOL alineada con el CONPES 3854 de 2016.

Figura 4- Evolución del Centro Cibernético Policial CCP

El Centro Cibernético Policial también conocido como CCP, es la Unidad Colombiana contra el Cibercrimen, creada por el gobierno nacional respondiendo a las expectativas consignadas en el CONPES 3701, tiene la responsabilidad en la lucha contra la ciberdelincuencia en el territorio nacional, a través de la prevención y la judicialización de los delitos informáticos.

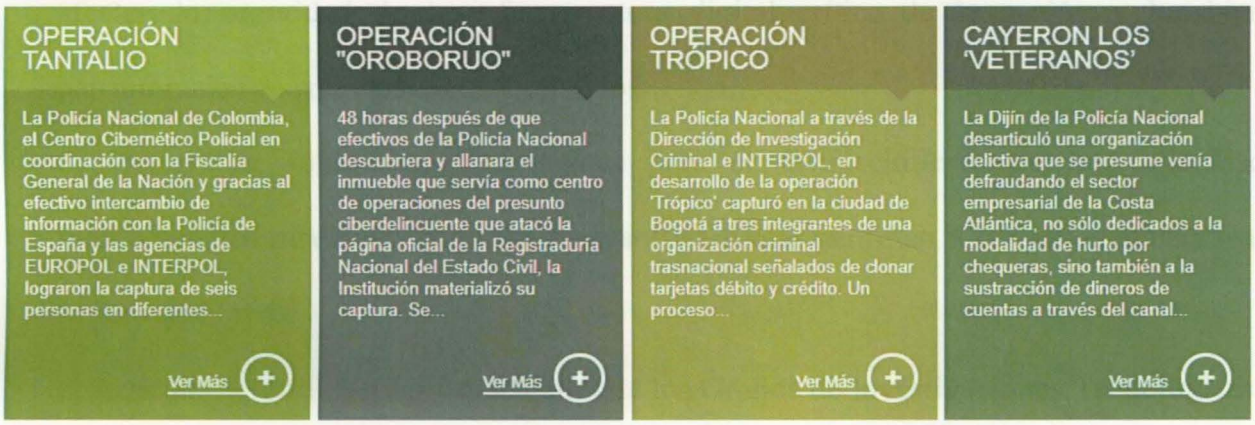
Es una dependencia operativa de la Dirección de Investigación Criminal e INTERPOL (en adelante DIJIN e INTERPOL) "encargada de desarrollar estrategias, programas y proyectos para la ciberseguridad, ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal" (Colombia, DIJIN e INTERPOL, Resolución 5839, 2015, Art 15).

El CCP está a cargo de funciones y responsabilidades administrativas, operativas, de la

investigación y la toma de decisiones dentro del proceso de investigación del cibercrimen.

La estructura interna del CCP las responsabilidades y tareas del proceso de investigación se distribuyen en la pornografía infantil, los delitos financieros, el ciberterrorismo y la infraestructura crítica.

Figura 5- Resultados operativos destacados Centro Cibernético Policial CCP



Nota: Tomada de https://caivirtual.policia.gov.co/ (2017).

4.1.1 Funciones del Centro Cibernético Policial.

Las funciones de centro cibernético policial se encuentran debidamente normadas en la resolución antes mencionada así:

1. Desarrollar la capacidad de detección; prevención, investigación, análisis, correlación, convergencia tecnológica, procedimientos de respuesta frente a situaciones de crisis informática, planes de contingencia específicos y judicialización de las amenazas que afecten la ciberseguridad en el ámbito nacional.

2. Dar cumplimiento a los requerimientos emanados por las autoridades judiciales en materia de investigación de los delitos de su competencia.

3. Liderar procesos investigativos y operaciones de carácter nacional e internacional contra organizaciones cibercriminales dedicadas a la vulneración de la integridad

personal, patrimonio económico, la disponibilidad, integridad, confidencialidad de la información que circulan por el ciberespacio y los delitos Cibernéticos que afectan a niños, niñas y adolescentes.

4. Desarrollar procesos investigativos contra organizaciones cibercriminales y ciberterroristas que atentan contra la integridad de personas, e incidentes informáticos que afecten la seguridad de la infraestructura digital crítica de la nación y los bienes patrimoniales de entes públicos y privados.

5. Desarrollar soluciones tecnológicas para el fortalecimiento de las capacidades institucionales mediante aplicaciones o software que permitan a los cibernautas un uso seguro de la web.

6. Articular y fortalecer las capacidades de los Grupos de Investigaciones Tecnológicas de las Seccionales de Investigación Criminal.

7. Fortalecer el Observatorio Nacional del Cibercrimen, como unidad de análisis del comportamiento de las modalidades criminales que afectan la ciberseguridad, generando información para la difusión de amenazas cibernéticas a través del Centro Nacional de Alerta Temprana Cibernética, logrando identificar nuevas modalidades y tendencias en la materia, despliegue de mapas criminales, georreferenciación y localización real de la perspectiva cibercriminal para la toma acertada de decisiones de carácter estratégico en el gobierno nacional.

8. Liderar la celebración de convenios, acuerdos de cooperación y alianzas estratégicas a nivel nacional e internacional con agencias de policía judicial y organismos estatales y privados que luchen contra las manifestaciones del cibercrimen.

9. Alcanzar y fortalecer los conocimientos, habilidades, experiencia y capacidades

tecnológicas mediante una formación profesional y especializada y la adquisición de medios de última generación para lograr los objetivos previstos en la Estrategia Nacional de Ciberseguridad en Colombia.

10. Desarrollar actividades de control a los proveedores o servidores, administradores y usuarios de redes globales de información para evitar la promulgación de imágenes, textos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con niñas, niños y adolescentes.

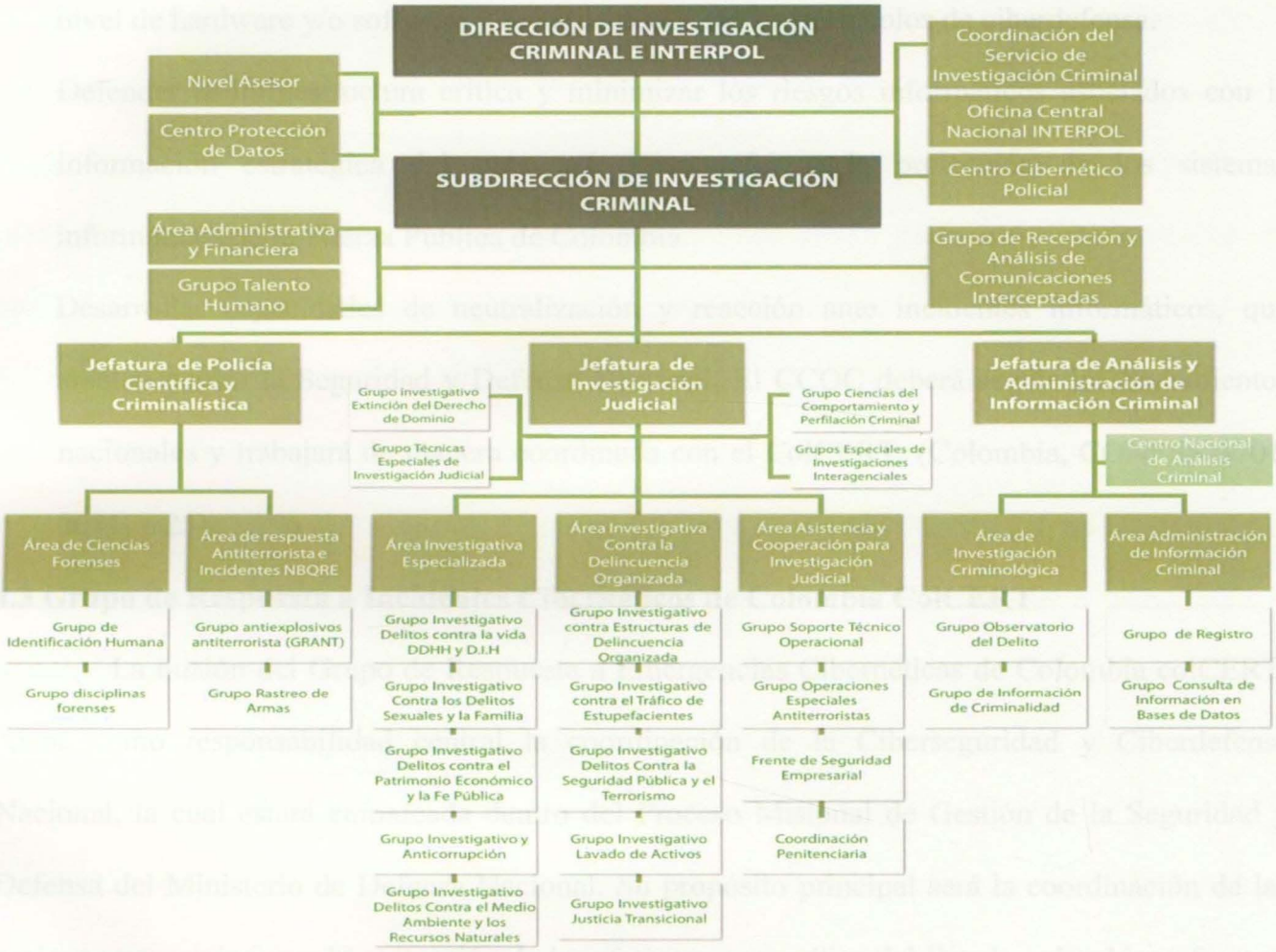
11. Atender los incidentes cibernéticos reportados por los ciberciudadanos a través de los canales de comunicación oficiales del Centro Cibernético Policial, adoptando los protocolos de tratamiento de la evidencia digital y su trámite ante la autoridad competente.

12. Realizar ciberpatrullajes 24/7 en la web, con el propósito de identificar amenazas desde y hacia Colombia en contra de la ciberseguridad ciudadana, desarrollando la capacidad de identificación y detección de factores comunes en los incidentes de su conocimiento así como la vulneración a la disponibilidad, integridad y confidencialidad de la información que circulan por el ciberespacio.

13. Insertar oportunamente las actividades y los resultados investigativos en los sistemas de información para la actualización y el análisis criminal.

14. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia. (DIJIN e INTERPOL, Resolución 5839, 2015, Art 15)

Figura 6 - Estructura orgánica de la Dirección de Investigación Criminal e INTERPOL



Nota: Tomada de https://www.policia.gov.co/direccion/investigacion-criminal/organigrama (2015).

4.2 Comando Conjunto Cibernético CCOC

El CONPES 3701 designó al Comando General de las Fuerzas Militares, como responsable CCOC este organismo debe prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales, las funciones generales del CCOC son:

Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.

Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.

Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional. El CCOC deberá seguir los lineamientos nacionales y trabajará de manera coordinada con el ColCERT. (Colombia, CONPES 3701, 2011, p.25)

4.3 Grupo de Respuesta a Incidentes Cibernéticos de Colombia ColCERT

La misión del Grupo de Respuesta a Emergencias Cibernéticas de Colombia colCERT, "tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional". (ColCERT, 2017)

5. Análisis de las condiciones y capacidades tecnológicas actuales del CCP

Dentro del Mapa Estratégico Institucional de la policía Nacional se encuentra el objetivo estratégico DHI6 para potenciar la gestión del conocimiento, la innovación, implementación y uso sostenible de las TIC´s, a través de la potenciación la Institución pretende fortalecer e implementar una infraestructura tecnológica dinámica que permita fortalecer sus capacidades para garantizar una mejor oferta de valor Institucional en la generación de productos de inteligencia y calidad de las investigaciones, que permitan comprender y atender los fenómenos que atentan contra la seguridad y convivencia ciudadana.

Bajo el concepto de revolución industrial de cuarta generación como anticipo de un nuevo desarrollo de la humanidad, la Policía Nacional viene adquiriendo las tecnologías de la información y las comunicaciones y las nuevas técnicas de investigación que le permitan a la Institución estar al nivel de las nuevas tendencias en seguridad ciudadana.

La cuarta revolución se basa en la hiperconectividad de redes y el acceso a la información y al conocimiento; la sociedad y la economía cada día es más digitales.

Las APP provistas por la Institución vinculan al ciudadano en la prevención, la seguridad y la convivencia; el uso de tecnología para el servicio de policía desde las calles y sistema de atención y respuesta virtual del servicio de policía al ciudadano, marcan el derrotero en esta línea.

La razón que justifica el fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP es para atender la demanda futura relacionada con la cuarta revolución industrial, En tal sentido, así como se mueven los nuevos factores económicos y se genera riqueza, también los ciberdelincuentes están a la expectativa.

El CCP en los últimos cinco (5) años ha realizado cuatro grandes adquisiciones de tecnología de la información relacionada con las condiciones y capacidades para la atención de

ciberdelitos cuya información es de carácter pública y se encuentra disponible en el portal de contratación del Estado Colombiano SECOP I.

Como justificación del componente tecnológico y herramientas necesarias para el CCP, se tiene la baja financiación para efectos del cumplimiento de los objetivos de la política de seguridad digital en la tabla 2 se encuentran los recursos asignados y las fuentes de los mismos, los cuales se ejecutarán durante el horizonte de la política nacional de seguridad digital en Colombia, estableciendo una reducción apreciable en los próximos años.

Tabla 2 –Financiamiento estimado, 2016-2019

Entidad	2016	2017	2018	2019	Total
Ministerio de Defensa Nacional	14.618	7.392	7.583	7.782	37.375
Ministerio de Tecnologías de la Información y las Comunicaciones	8.750	13.950	13.000	9.550	45.250
Dirección Nacional de Inteligencia	-	-	500	1.000	1.500
Ministerio de Justicia y del Derecho	-	200	250	-	450
Ministerio de Educación Nacional	-	75	150	120	345
Departamento Nacional de Planeación	75	75	-	-	150
Total	23.443	21.692	21.483	18.452	85.070

Nota: tomado del CONPES 3854 de 2016.

5.1 Adquisiciones tecnológicas del CCP

Las consultas públicas permitieron establecer las adquisiciones tecnologías realizadas por la DIJIN para el CCP según los siguientes procesos contractuales:

PN DIJIN SA 015 de 2015 cuyo objeto fue la "adquisición de hardware, software y transferencia de conocimiento para el fortalecimiento del Centro Cibernético Policial de la

Dirección de Investigación Criminal e INTERPOL "(DIJIN e INTERPOL, 2015), implementó a través de los contratos 03-2-10061-15, el equipo de detección electrónica Orion 2.4 non-linear junction detector (detecta y localiza equipos electrónicos como cámaras ocultas, micrófonos y otros dispositivos electrónicos, independientemente de si el dispositivo está radiante, cableado o apagado), como parte de la implementación del modelo de análisis de investigación de alta tecnología basado en crímenes de explotación sexual y abuso a menores, con el contrato 03-2-10062-15, se operacionalizó la segunda fase implementación de laboratorio de análisis de datos F.D.A a través licencias software arbutus (análisis de datos en fraudes corporativo), se adquirieron los equipos para la investigación cibernética a través un (1) sistema de detección y análisis de cibercrimen contra amenazas adaptativas avanzadas.

El proceso contractual PN DIJIN SA 021 de 2014 cuyo objeto fue la "implementación del Centro Cibernético de la Policía Nacional - adquisición de equipos para la investigación forense de la Dirección de Investigación Criminal e INTERPOL", (DIJIN e INTERPOL, 2014), el contrato 03-2-10089-14 permitió la adquisición de licencias así como su implementación del software y entrenamiento IDEA (licencias stand alone de la herramienta de análisis de datos) y el contrato 03-2-10090-14 permitió la adquisición de licencias server-stand alone del software ACL (análisis de datos) y entrenamiento.

El proceso PN DIJIN SA 011 DE 2014 cuyo objeto fue la "implementación del Centro Cibernético de la Policía Nacional - adquisición de equipos para la investigación forense de la Dirección de Investigación Criminal e INTERPOL" produjo los contratos 03-2-10060-14 que permitió la adquisición del software arbutus para la implementación del laboratorio de análisis de código malicioso A.C.M, el contrato 03-2-10061-14 permitió la adquisición de un (01) servidor para la instalación de las licencias server de los software ARBUTUS, ACL e IDEA.

El proceso PN DIJIN SA 017 2013 para la implementación del centro cibernético de la Policía Nacional – adquisición de equipos de análisis forense para dispositivos móviles con destino a la Dirección de Investigación Criminal e INTERPOL, estableció el contrato 03-2-10119-13 para adquisición equipos de análisis forense para dispositivos móviles Cellebrite Ufed Touch Ultimate (solución forense móvil, con interfaz gráfica, que permite la extracción física, lógica y de todos los datos y contraseñas de teléfonos móviles, dispositivos GPS, portátiles y tabletas).

De lo anterior es posible evidenciar las condiciones y capacidades tecnológicas actuales con los recursos propios del Centro Cibernético Policial CCP.

5.2 Propuesta de capacidades tecnológicas del CCP

Las adquisiciones tecnológicas realizadas por la DIJIN e INTERPOL para el CCP y la información publicada en la página web https://caivirtual.policia.gov.co/ permiten proponer las capacidades que tiene el CCP, debido a que no se encontró información detallada y específica de las capacidades tecnológicas actuales de esta unidad policial, así:

5.2.1 CAI virtual.

La página web https://caivirtual.policia.gov.co/ presenta los servicios prestados por el CCP, enfocado a la atención de incidentes, reporte de delitos, campañas de prevención recomendaciones, boletines, guías, informes e infografías de ciberseguridad, permite la descarga de aplicaciones móviles para el fortalecimiento de la ciberseguridad y el análisis de muestras de malware.

5.2.2 Laboratorio forense.

Permite realizar labores de adquisición, investigación y análisis de evidencias digitales mediante hardware y software especializado.

El laboratorio cuenta con duplicadores forenses de alta velocidad, dispositivos de toma de imágenes forenses, bloqueadores de dispositivos, kit para recuperación de datos, estaciones forenses portátiles y de escritorio, sistema de almacenamiento centralizado de evidencias digitales que soporta todas las labores del laboratorio.

El laboratorio forense de la Policía Nacional Colombiana, atiende de manera gratuita a los ciudadanos víctimas del cibercrimen, para acceder a sus servicios debe mediar una orden judicial emitida por un juez, también debe existir una investigación en curso por oficio o solicitud expresa y por ende una denuncia para proceder a realizar el proceso de investigación.

Laboratorio de análisis de código malicioso A.C.M, análisis forense para dispositivos móviles Cellebrite Ufed Touch Ultimate

5.2.3 Análisis de información estructurada y no estructurada.

El análisis forense de datos (FDA, por sus siglas en inglés) combina el uso generalizado de Big data, así como el análisis estadístico y cualitativo, con modelos explicativos y predictivos para guiar e identificar evidencias.

La evidencia basada en hechos permite la toma de decisiones de judiciales prácticas, dirige los esfuerzos de investigación hacia las áreas que más lo necesitan y optimiza los resultados.

Los servicios de FDA están compuestos por metodologías proactivas y reactivas que utilizan la información contenida en el conjunto de datos de los investigados, con información estructurados y no estructurados, lo que permite detectar e investigar con mayor eficiencia casos de error, desperdicio, uso indebido, abuso, corrupción, incumplimiento y fraude.

6. Identificación del componente tecnológico y herramientas necesarias para el CCP

Como parte de las recomendaciones del CONPES 3854 es necesario la elaboración y ejecución de "planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, del CCP y del CCOC", (diciembre de 2019).

La identificación del componente tecnológico y las herramientas necesarias para el CCP tuvo en cuenta el desempeño de los indicadores, las actuales capacidades propuestas para el CCP, las restricciones financieras, revolución industrial de cuarta generación y los delitos informáticos para proponer el fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP, así:

6.1 C4 (Centro de mando, Control, Comunicaciones y Computación)

El CCP, se encuentra en proceso para la adquisición de soluciones tecnológicas centralizadas de última generación en hardware y software, con el fin de atender, prevenir, detectar, disuadir, investigar y judicializar cualquier tipo de delito informático o amenaza cibernética.

6.2 Análisis de malware

El software que cause daños a los usuarios, equipos o red como virus, troyanos, rootkits o spyware pueden considerarse como malware.

Las herramientas de análisis de malware deben ser capaces de detectar determinar el daño causado y detectar si se han infectado otros ficheros, una vez que se localiza un fichero malicioso, se añade a una base de datos de firmas de malware para asegurar que el mismo fichero no vuelve a entrar en la red o dispositivo, que es el principio de funcionamiento de los antivirus.

Existen dos formas fundamentales de abordar el análisis de malware: análisis estático y dinámico. El análisis estático examina el malware sin llegar a ejecutarlo y el análisis dinámico observa lo que ocurre en el sistema cuando es ejecutado (ficheros modificados, conexión con máquinas remotas) (Sikorski y Honig, 2012).

6.2.1 Análisis estático.

Consiste en examinar el fichero y proveer información sobre su estructura y funcionalidad, Este análisis es más básico y seguro (ya que no estamos ejecutando código malicioso) pero no es tan efectivo contra ficheros malware que están ofuscados.

El método más usado para identificar malware es basado en firmas. Cuando un fichero sospechoso entra en el sistema, se genera su hash (medición matemática de la integridad de un archivo) para su posterior comparación con una base de datos de firmas de malware. El problema reside en que los autores de malware pueden modificar fácilmente su código y así evadir este tipo de análisis.

Otro método de análisis, es la búsqueda de cadenas de caracteres en el programa. Es posible que en el código haya alguna URL o IP que nos dé una pista del comportamiento de la aplicación. Sin embargo, muchas veces las herramientas de detección de cadenas de caracteres interpretan erróneamente datos o direcciones de memoria como cadenas de caracteres.

El malware empaquetado u ofuscado contiene muy pocas cadenas de caracteres. Esto nos dificulta el conocer la funcionalidad del fichero. Sin embargo, si encontramos un fichero que contiene pocas cadenas de caracteres significativas, nos sugiere que puede estar ofuscado. En el caso de los ficheros PE (Portable Executable), lo que más información nos aportan es las librerías que importan. Estas están definidas en la cabecera del fichero.

(Valero. 2017 p. 9)

6.2.2 Análisis dinámico.

Se basa en técnicas que observan el comportamiento de la ejecución de malware en el sistema. Este tipo de análisis nos permite detectar el funcionamiento del malware (aunque esté ofuscado). Para llevar a cabo un análisis dinámico de malware, se requiere de un ambiente seguro donde se pueda ejecutar cualquier tipo de fichero malicioso sin que haya riesgo de dañar al dispositivo o la red. Estos análisis se suelen llevar a cabo en máquinas virtuales o sandboxes. Una sandbox es una máquina virtual con software preinstalado para analizar la ejecución de malware. Suele realizar acciones como generar una red virtual para observar la interacción del malware con la red. Los problemas de una sandbox, es que si el malware requiere opciones por línea de comandos no se va llegar a ejecutar ningún código ya que el programa se va a quedar esperando una entrada. Otro problema, es que hay software programado para ejecutarse a una determinada hora del día. Por ejemplo, si analizamos el malware por el día y este sólo se ejecuta por la noche, no se va a detectar ninguna actividad sospechosa. También hay malware capaz de detectar si están corriendo en una máquina virtual y son capaces de cambiar su comportamiento. Esto lo hace para evitar el ser detectado como aplicaciones maliciosas en caso de estar ejecutándose en una sandbox. Otro problema es que la sandbox debe tener un Sistema operativo donde el malware pueda ejecutarse. Por ejemplo, un fichero puede servir para dañar Windows XP pero no ejecutarse correctamente en Windows 7.

6.2.3 Herramientas de análisis de malware

YARA es un sistema multiplataforma disponible para Windows, Linux y Mac OS, es una herramienta que ayuda a identificar y clasificar familias de malware. Con YARA, se

describen familias de malware basadas en información binaria o textual de los ficheros. Estas descripciones, se guardan en reglas que son aplicadas a los ficheros para determinar si pertenece a una clase o no. Por ejemplo, podemos crear una regla donde se detecta aquellos ficheros que acceden a una de dos posibles URL maliciosas.

ClamAV es un antivirus, que tiene como objetivo detectar troyanos, virus, malware y otras amenazas. Se ha convertido en un estándar de facto para el análisis de software en servidores de email. Escanea archivos y ficheros comprimidos (ZIP, RAR, ARJ,TAR,...) y además soporta ficheros especiales como HTML, RTF o PDF. La aplicación incluye un escáner demonio (clamd) y una aplicación de análisis por línea de comandos (clamscan). También contiene una herramienta para actualizar la base de datos de firmas llamada freshclam.

VirusTotal es un sitio web desarrollado por Hispasec que permite el análisis online de ficheros. Este sistema usa un total de 54 antivirus para analizar los ficheros en busca de malware. VirusTotal provee de una API para Java que permite automatizar procesos de análisis. Sin embargo, para su uso requiere de una clave que se consigue al registrarse en la comunidad de VirusTotal. Está limitado a 4 peticiones por minuto.

Metascan es una herramienta online gratuita de análisis de malware. Este sistema una el escaneo de ficheros con varios motores de análisis (como los antivirus de ESET, AVG o MacAfee). Al igual que VirusTotal, posee una API para Java y requiere de una clave conseguida el registrarse en el portal OPSWAT. Tiene un límite de 1500 peticiones de búsqueda de hash y 25 peticiones de análisis de ficheros por hora.

Cuckoo es un sistema de código libre que automatiza el análisis dinámico de malware. Es uno de los sandbox más usados actualmente. Se encarga de ejecutar y analizar ficheros en

tiempo real. El sandbox Cuckoo consiste en un software central de gestión que maneja la ejecución y análisis de ficheros. Cada análisis se ejecuta en una máquina virtual aislada. La infraestructura de Cuckoo está compuesta por una máquina Host (con el software de gestión) y un conjunto de máquinas huésped (máquinas virtuales que ejecutan los ficheros). El Host ejecuta todo el proceso de análisis mientras que cada huésped se encarga de ejecutar los ficheros de forma segura.

6.3 Predicción del delito cibernético

Adoptar modelos predictivos de comisión del delito cibernético en ambientes controlados con el fin de estudiar y posteriormente prevenir y neutralizar, a través de herramientas de BigData e inteligencia artificia.

Con capacidad de generar procesos de alerta en materia preventiva de manera permanente y en tiempo real.

Una aplicación importante de Big Data en el ámbito de la aplicación de la ley es la predicción del cuerpo de la Policía, mediante la aplicación principalmente de las técnicas analíticas cuantitativas para identificar posibles objetivos de intervención y para prevenir el crimen, o resolver crímenes pasados haciendo predicciones estadísticas. Se utiliza por la aplicación de la ley, para predecir los patrones futuros de delincuencia e identificar áreas vulnerables, así como para la minería de datos.

La predicción de la policía es vista como un método que permite trabajar de manera más efectiva y proactiva con recursos limitados. Los métodos utilizados se dividen en cuatro categorías generales: la predicción de los delitos, la predicción de los delincuentes, la predicción de las identidades de los autores y la predicción de las víctimas de la delincuencia.

Si bien el concepto de policía preventiva no es nuevo, es la gran cantidad de datos, las

diferentes fuentes de datos y la velocidad a la que se pueden analizar estos datos, ofrece nuevas promesas en la lucha contra el cibercrimen, los datos tradicionales de la delincuencia tales como datos de las redes sociales para proporcionar acceso en tiempo real permite reaccionar más rápido y explorar más indicios.

Dado que el análisis de Big Data suele ser inadecuado para responder a la cuestión de la causalidad, puede crear más retos para los investigadores para producir evidencia de apoyo dada la gran cantidad de datos que deben analizarse. Por otra parte, el análisis de Big Data puede utilizarse para señalar las áreas más prometedoras para una investigación, es decir, dónde encontrar relaciones causales. Para ello, se necesita estar en condiciones de combinar de manera efectiva y eficiente las pruebas de diferentes fuentes y presentarlas de manera significativa.

Sin embargo, existe el riesgo de utilizar datos grandes incorrectamente o excesivamente. Por lo tanto, es importante utilizar las herramientas analíticas cuidadosamente, proporcionalmente y de acuerdo con la legislación y los reglamentos pertinentes.

Otra área de Big Data que ya es relevante para la investigación se espera que aumente es el análisis de información de código abierto o de inteligencia de código abierto. (IOCTA 2014)

6.4 Software Open Source en la investigación criminal

El Software distribuido y desarrollado libremente, ofrece ventajas económicas en escenarios de reducción del presupuesto como se puede inferir de la información del CONPES 3854 de 2016, para su implementación la propuesta de estas herramientas fueron el resultado de múltiples consultas bibliográficas, en la tabla 3 se puede observar distintos software forense de común utilización en las agencias de investigación, el software open source propuesto cuenta con la mayor referenciación, comunidades de desarrollo sólidas y maduras, con estos criterios se construyó la tabla 3.

Existen una variedad de suites de herramientas o distribuciones GNU/Linux que han consolidado las diferentes herramientas dedicadas al análisis forense.

Tabla 3 –Comparativo software forense

Software forense	Tipo de licencia	Uso	Desventajas
CAINE	Open source	Computación forense	Desconocimiento en la programación. Dependencia de la comunidad (programadores)
SIFT	Open source	Computación forense	Desconocimiento en la programación. Dependencia de la comunidad (programadores)
DEFT	Open source	Computación forense	Desconocimiento en la programación. Dependencia de la comunidad (programadores)
FTK ®	Privativa	Computación forense	Costo del licenciamiento
ENCASE®	Privativa	Computación forense	Costo del licenciamiento
OXYGEN FORENSIC ®	Privativa	Teléfonos móviles	Costo del licenciamiento
XWF (X-Ways) ®	Privativa	Computación forense	Costo del licenciamiento

Entre las suite que fueron analizadas están orientadas a dispositivos móviles y otras más generales.

7.2.1 CAINE Linux (Computer Aided Investigative Environment)

Es una distribución GNU/Linux de origen italiana, creada por Giancarlo Giustini para el Centro de Investigación en Seguridad (CRIS).

Es un entorno forense que integra herramientas de software existentes, que proporcionar una interfaz gráfica amigable.

CAINE propone tres objetivos:

1. Un entorno interoperable que apoya el investigador digital durante las fases de la investigación digitales.
2. Una interfaz gráfica fácil de usar.
3. Una compilación semiautomática del informe final.

7.2.1 SIFT (SANS Investigative Forensic Toolkit)

Creado por un equipo internacional de expertos forenses encabezado por el instituto SANS (SysAdmin Audit Networking and Security Institute) para la respuesta de incidentes y análisis forense digital que se puso a disposición de toda la comunidad como un servicio público.

Está basado en Ubuntu LTS 14.04 y puede ser integrado con REMnux, un kit de herramientas para ingeniería inversa y análisis de malware.

Permite examinar de forma segura almacenamientos, múltiples sistemas de archivos y diferentes formatos de evidencia. Incluye más de 100 herramientas, 44 para el análisis forense en diferentes ámbitos: discos duros, redes, analizar artefactos maliciosos, entre otros.

SIFT soporta los sistemas de archivos NTFS, ISO9660, HFS+, Raw data, espacio de intercambio (Swap), FAT 12/16/32, EXT 2/3/4, UFS ½ y vmdk. También soporta una gran variedad de formatos de imágenes forenses como Raw, AFF, AFD, AFM, AFFLib, EWF (EnCase), Split raw, affuse, Split ewf, mount_ewf.py y ewfmount.

7.2.2 DEFT (Digital Evidence and Forensic Toolkit)

Es una distribución que se compone de GNU/Linux y DART (Kit de herramientas de Respuesta Digital Avanzada).

Esta suite está dedicada al análisis forense digital y actividades de inteligencia. La versión 8.2 está basada en Ubuntu 12.10 y cuenta con DART es su versión 2.

DART es una suite para la gestión y respuesta ante incidentes desde sistemas operativos Windows, que incluye un lanzador de herramientas para este sistema operativo.

Hay ciertas características a DEFT que minimizan el riesgo de alterar los datos que están siendo sometidos a análisis.

Algunas de estas características son:

1. En el arranque, se analiza el sistema no utiliza las particiones de intercambio en el sistema.

2. Durante el inicio del sistema no hay guiones automáticos de montaje.

3. No existen sistemas automatizados para cualquier actividad durante el análisis de las pruebas.

4. Todas las herramientas de almacenamiento y adquisición de tráfico de red en masa no alteran los datos que se adquirieron.

DEFT nos ofrece sus herramientas distribuidas entre las siguientes categorías:

Analysis - Herramientas de análisis de ficheros de diferentes tipos Antimalware - Búsqueda de rootkits, virus, malware, así como PDF con código malicioso.

Data recovery - Software para recuperación de ficheros

Hashing - Scripts que permiten la realización de cálculo de hashes de determinados procesos (SHA1, SHA256, MD5) Imaging - Aplicaciones que podemos utilizar para realizar los clonados y adquisición de imágenes de discos duros.

Mobile Forensics - Análisis de Blackberry, Android, iPhone, así como información sobre las típicas bases de datos de dispositivos móviles en SQLite utilizadas por las aplicaciones.

Network Forensics - Herramientas para procesamiento de información almacenada en capturas de red.

OSINT - Aplicaciones que facilitan la obtención de información asociada a usuarios y su actividad.

Password recovery - Recuperación de contraseñas de BIOS, ficheros comprimidos, ofimáticos, fuerza bruta, etc.

Reporting tools - Por último, dentro de esta sección encontraremos herramientas que nos facilitarán las tareas de generación de informes y obtención de evidencias que nos servirán para documentar el análisis forense.

Captura de pantalla, recopilación de notas, registro de actividad del escritorio, etc.

En abril de 2015 se lanzó DEFT Zero42, diseñada para ser la versión ligera de DEFT. Está centrado en la copia forense de evidencias digitales (es decir, los discos duros, dispositivos USB y unidades de red), optimizado para correr en solo 400 Mb, permitiendo que se cargue por completo en memoria RAM. Basado en Lubuntu 04.14.02 LTS y se desarrollará en paralelo con las futuras versiones completas de DEFT. Soporta versiones de 32 y 64 bits, con UEFI y arranque seguro.

8 Lineamientos o metodología usados en el trabajo

La metodología adoptada en el trabajo de grado fue el de la investigación aplicada está buscó la generación de conocimiento con aplicación directa a los problemas del Centro Cibernético Policial, en este trabajo de de grado, el problema fue establecido en el formato ficha de inscripción trabajos de grado con el respectivo rigor metodológico, buscando la resolución práctica del problema y la aplicación del conocimiento adquirido mediante las consultas bibliográficas e identificando los lineamientos del Gobierno Nacional y de la Policía Nacional, con la idea de consolidar la información para la satisfacción de cada uno de los objetivos propuestos.

8.1 Pregunta de investigación

La pregunta de investigación formulada fue:

¿Cuenta actualmente el CCP con las capacidades tecnológicas necesarias para hacer frente al crimen y la delincuencia que afecta la seguridad digital nacional?

8.2 Respuesta pregunta de investigación

El Centro cibernético policial no cuenta con las capacidades tecnológicas necesarias para hacer frente al crimen y la delincuencia que afecta la seguridad digital Nacional, porque realizado el presente proyecto de grado se estableció que existe una tendencia al alza de los delitos cibernéticos en Colombia y una reducción del presupuesto, que obliga a la formulación de iniciativas como el presente proyecto de grado, para buscar alternativas para el fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP y de esta manera lograr los objetivos institucionales trazados para la Dirección de investigación criminal e INTERPOL y por la Policía Nacional.

Conclusiones

La investigación realizada en este trabajo de investigación ha permitido arribar a las siguientes conclusiones:

PRIMERA: la proliferación de los delitos de naturaleza cibernética requiere el uso de herramientas especializadas y actualizadas por parte del CCP para mejorar los indicadores de gestión de la DIJIN e INTERPOL.

Las amenazas cibernéticas siguen siendo una importante preocupación de seguridad en Colombia. La existencias de Incidentes políticamente motivados han incluido presuntas violaciones a la privacidad y a la seguridad de la información.

El Centro cibernético policial informa que un número cada vez mayor de ataques con motivación financiera causados por la combinación de factores como el uso masivo de las nuevas tecnologías de la información y el desconocimiento de las normas de seguridad en el uso de estas herramientas.

Para desarrollar aún más la institucionalidad y la capacidad para abordar las amenazas cibernéticas, Colombia preparó una política en seguridad digital materializada en el CONPES 3854 de 2016, en consulta con la Organización de Estados Americanos, la Organización para la Cooperación y el Desarrollo Económico, entre otros, esta política incluye una estrategia nacional y un conjunto de objetivos prioritarios para minimizar los niveles de riesgo.

SEGUNDA: para el cumplimiento de las funciones preventivas e investigativas del CCP podrá analizar la conveniencia en la utilización de nuevas herramientas identificadas para el análisis de malware y la predicción del delito cibernético.

Las capacidades de la Fuerza Pública, en un momento dado del tiempo, estarán en función de la doctrina, el material y el equipo, la organización, el personal y la infraestructura

con los que se cuenta en ese momento, este concepto es aplicado por la oficina de planeación de la Policía Nacional.

Las capacidades técnicas, tecnológicas e investigativas con las que cuenta la Institución a nivel nacional, regional y local, a través de la Dirección de Investigación Criminal e Interpol y en corresponsabilidad con las direcciones operativas (Antinarcóticos, Tránsito y Transporte, Antisecuestro y Antiextorsión, Carabineros y Seguridad Rural y Policía Fiscal y Aduanera), posibilita la administración de información y el desarrollo efectivo de la investigación judicial y criminalística para obtener resultados de impacto sobre los eslabones de las diferentes cadenas criminales, así como la identificación y desarticulación de las estructuras delincuenciales de mayor afectación a la seguridad pública y la seguridad ciudadana.

TERCERA: el CCP requiere de nuevas inversiones para la adquisición de hardware y software, especializado así como el aumento de las capacidades para atender el creciente número de investigaciones por las violaciones a la ley 1273 de 2009.

La cuarta revolución se basa en la hiperconectividad de redes y el acceso a la información y al conocimiento; la sociedad y la economía cada día son más digitales.

La razón que justifica el fortalecimiento de las capacidades tecnológicas del Centro Cibernético Policial CCP es para atender la demanda futura relacionada con la cuarta revolución industrial, En tal sentido, así como se mueven los nuevos factores económicos y se genera riqueza, también los ciberdelincuentes están a la expectativa.

El componente tecnológico y herramientas necesarias para el CCP, se tiene la baja financiación para efectos del cumplimiento de los objetivos de la política de seguridad digital el horizonte de la política nacional de seguridad digital en Colombia, establece una reducción apreciable en los próximos años.

CUARTA: En las herramientas de open source se encuentra toda una gama de opciones que posibilitan realizar un análisis de evidencia digital. Estás herramientas de fácil acceso por su disponibilidad para su descarga y posterior uso.

Las herramientas analizadas están más orientadas al proceso forense en general, a los equipos de cómputo tradicionales y a las redes de comunicación.

La informática forense y la seguridad informática son dos líneas de estudio muy interesantes que pueden ser abarcadas por futuros proyectos de grado.

Recomendaciones

El CCP podría revisar con la Secretaría general de la PONAL la viabilidad de utilizar Software Open Source en la investigación criminal.

Referencias

Colombia, CONPES (2011) 3701, *lineamientos de política para ciberseguridad y ciberdefensa.* Recuperado el 1 de agosto de 2017, de: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Colombia, CONPES (2016) *3854, Política Nacional de seguridad digital.* Recuperado el 1 de agosto de 2017, de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Colombia, CRC (2009) *Resolución 2258, Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007.* Recuperado el 5 de agosto de 2017, de: http://www.csirt-ccit.org.co/text/Legal/2258.pdf

Colombia, Congreso de la República (2009) Ley 1273 de 2009, *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.* Recuperado el 8 de agosto de 2017, de:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Colombia, Policía Nacional (2005) *Resolución 05839, por la cual se define la estructura orgánica interna de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias y se dictan unas disposiciones.* Bogotá D.C. Recuperado el 10 de agosto de 2017, de: https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

Colombia, CRC (2009) *Resolución 2258, Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007.* Recuperado el 5 de agosto de 2017, de: http://www.csirt-ccit.org.co/text/Legal/2258.pdf

Centro Cibernético Policial, CCP. (2017) Informe. *Amenazas del Cibercrimen en Colombia 2016-2017.* Bogotá D.C: Recuperado el 2 de agosto de 2017, de: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Gibson, W. (2002). Neuromante. Barcelona: Minotauro.

Acerca de. (2017. Julio, 17). Recuperado el 05 de agosto de 2017, de http://www.colcert.gov.co/?q=acerca-de

Sikorski, M. & Honig, A. (2015) *Practical Malware Analysis*. San Francisco, CA: No Starch Press, Inc.

Oktavianto, D. & Muhardianto, I. (2013) *Cuckoo Malware Analysis*. Birmingham, U: Packt Publishing Ltd.

Internet Organised Crime Threat Assessment IOCTA (2016). europol.europa.eu. Recuperado el 15 de agosto de 2017, de https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

Internet Organised Crime Threat Assessment IOCTA (2014). europol.europa.eu. Recuperado el 15 de agosto de 2017, de https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf

Plan Estratégico Institucional Comunidades Seguras y en Paz 2015-2018 (2015). policia.gov.co. Recuperado el 18 de agosto de 2017, de https://www.policia.gov.co/sites/default/files/descargables/plan-estrategico-institucional-2015-2018.pdf

Informe integral de la Gestión Institucional II Trimestre (2017). policia.gov.co. Recuperado el 16 de agosto de 2017, de https://www.policia.gov.co/sites/default/files/descargables/informe - integral-de-gestion-2-trimestre-de-2017.pptx