Propuesta de un modelo de ciberinteligencia basado en el ciclo de inteligencia utilizado por la Policía Nacional

Astrid Vannessa Castro Cortés

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

2020

MONOGRAFÍA DE GRADO
PROPUESTA DE UN MODELO DE CIBERINTELIGENCIA BASADO EN EL CICLO DE INTELIGENCIA UTILIZADO POR LA POLICÍA NACIONAL

ASTRID VANNESSA CASTRO CORTES

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA
ESCUELA SUPERIOR DE GUERRA
COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ, D.C.

2020

MONOGRAFÍA DE GRADO
PROPUESTA DE UN MODELO DE CIBERINTELIGENCIA BASADO EN EL CICLO DE INTELIGENCIA UTILIZADO POR LA POLICÍA NACIONAL

ASTRID VANNESSA CASTRO CORTES

DIRECTOR:

MAGISTER LUCAS ADOLFO GIRALDO RÍOS

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA
ESCUELA SUPERIOR DE GUERRA
COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ, D.C.

2020

DEDICATORIA

Dedico este proyecto de grado, en primera media a Dios, quien me dio la fortaleza y sabiduría para abordar cada una de las temáticas descritas en el presente trabajo.

Igualmente, doy gracias a mi familia que siempre me ha dado su apoyo incondicional en todos los ámbitos de mi vida y me ha infundido la tenacidad y valentía para afrontar de la mejorar manera, cada reto que me propongo.

También, le dedico este trabajo a mi compañero de vida, quien siempre ha sido mi mayor motivador, quien todos los días cuando sentía que no podía más me alentaba a continuar y tenía las palabras indicadas para hacerme olvidar de mis miedos y debilidades y confiar en mis capacidades y fortalezas.

Agradezco, igualmente a mis docentes de la maestría y en especial a mi asesor de trabajo de grado quien con su experiencia, conocimiento y enseñanzas permitió que yo pudiera encontrar la ruta y culminar satisfactoriamente este reto.

Finalmente, dedico este proyecto a mis compañeros que dentro de las aulas de clases y los debates académicos permitieron que adquiriera mayor conocimiento, el cual pude dejar plasmado en el presente trabajo de grado.

Gracias infinitas a cada una de las personas que contribuyeron de alguna manera para alcanzar esta meta que veía lejana.

RESUMEN

Atendiendo los retos que impone el rol que tiene actualmente las tecnologías de la información y de la comunicación en la nueva realidad que viven las personas, la Policía Nacional de Colombia como garante de la ciberseguridad del país debe fortalecer desde el rol de inteligencia y a partir de un modelo de ciberinteligencia, objeto de la presente investigación, las actividades de recolección, tratamiento, análisis y difusión de información en el ciberespacio, para la prevención y anticipación de ciberamenazas y la conceptualización de fenómenos que se presentan en este entorno; siendo necesario para ello, realizar la conceptualización de las características teóricas que tienen un modelo de ciberseguridad y ciberinteligencia y su relación con el ciclo de inteligencia, así como identificar las capacidades con las cuales cuenta esta institución para ejercer control sobre el ciberespacio, y de esta forma con todos los elementos identificados realizar la conceptualización del modelo de ciberinteligencia.

Palabras claves

Modelo, estándar, ciberseguridad, ciberinteligencia, cibercrimen, inteligencia, ciclo de inteligencia

ABSTRACT

In response to the challenges imposed by the current role of information and communication technologies in the new reality that people live, the Colombian National Police as guarantor of the country's cybersecurity must strengthen from the role of intelligence and from a cyberintelligence model, object of this research, the activities of collection, treatment, analysis and dissemination of information in cyberspace, for the prevention and anticipation of cyber threats and the conceptualization of phenomena that occur in this environment; being necessary for this, to carry out the conceptualization of the theoretical characteristics that have a cybersecurity and cyberintelligence model and its relationship with the intelligence cycle, as well as to identify the capacities that this institution has to exercise control over cyberspace, and of this form with all the elements identified to carry out the conceptualization of the cyberintelligence model.

Key words

Model, standard, cybersecurity, cyberintelligence, cybercrime, intelligence, intelligence cycle

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTADO DE SIGLAS Y ABREVIATURAS

ACINT: Inteligencia acústica avanzada.

AMERIPOL: Comunidad de Policías de América.

APK: Paquete de Aplicación Android (Android Application Package).

ASOBANCARIA: Asociación Bancaria y de Entidades Financieras de Colombia.

ASUIN: Área de Relaciones y Cooperación Internacional Policial de la Dirección General.

ATA: Programa de Asistencia Antiterrorismo de Estados Unidos.

C4: Centro de Capacidades para la Ciberseguridad de Colombia.

CAI: Comando de Acción Inmediata.

CCIT: Cámara Colombiana de Informática y Telecomunicaciones.

CCN: Centro Criptológico Nacional.

CCOC: Comando Conjunto Cibernético.

CCP: Centro Cibernético Policial.

CI3: Centro Integrado de Información de Inteligencia.

CIA: Agencia Central de Inteligencia de Estados Unidos.

CLACIP: Comunidad Latinoamericana y del Caribe de Inteligencia Policial.

CMM: Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones

CNI: Centro Nacional de Inteligencia.

COEST: Oficina de Comunicaciones Estratégicas.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

COMINT: Inteligencia de comunicaciones.

CONPES: Consejo Nacional de Política Económica y Social.

CRC: Comisión de Regulación de Comunicaciones

CSIRT: Grupo de Respuesta a Incidentes de Seguridad (Computer Security Incident Response Team).

CTF: Capturar la Bandera (Capture the Flag).

CYBINT: Ciberinteligencia.

DEA: Administración para el Control de Drogas de los Estados Unidos.

DIASE: Dirección Antisecuestro y Antiextorsión.

DIJIN: Dirección de Investigación Criminal e Interpol.

DINAE: Dirección Nacional de Escuelas.

DIPOL: Dirección de Inteligencia Policial.

DIPRO: Dirección de Protección y Servicios Especiales.

DISEC: Dirección de Seguridad Ciudadana.

EC3: Centro Europeo Contra el Cibercrimen.

EJERCOL: Ejercito Nacional de Colombia.

ELINT: Inteligencia Electrónica.

ESCIB: Estrategia Integral de Ciberseguridad.

ESTIC: Escuela de Tecnologías de la Información y las Comunicaciones.

EUROPOL: Oficina Europea de Policía.

FBI: Buró Federal de Investigaciones (Federal Bureau of Investigation).

FGN: Fiscalía General de Nación.

GAULA: Grupos de Acción Unificada por la Libertad Personal.

GEOINT: Inteligencia Geoespacial.

GLDTA: Grupo de Trabajo Americano de delitos Tecnológicos del INTERPOL.

HUMINT: Inteligencia de Fuentes Humanas.

ICBF: Instituto Colombiano de Bienestar Familiar.

ICE: Servicio de Inmigración y Control de Aduanas (Immigration and Customs Enforcement's)

ICONTEC: Instituto Colombiano de Normas Técnicas y Certificación.

IGCI: Complejo Global de INTERPOL para la Innovación (INTERPOL Global Complex for Innovation).

IMINT: Inteligencia de Imágenes.

INCOCREDITO: Asociación para la Investigación, Información y Control.

INTERPOL: Organización Internacional de Policía Criminal.

ISO: Organización Internacional de Normalización (International Organization for Standardization)

ITU: Unión Internacional de Telecomunicaciones (International Telecommunication Union).

KOICA: Agencia Internacional de Cooperación Coreana.

OEA: Organización de los Estados Americanos

OFITE: Oficina de Telemática.

ONU: Organización de las Naciones Unidas.

OSINT: Inteligencia de Fuentes Abiertas.

MASINT: Inteligencia de Reconocimiento y Signatura.

MINTIC: Ministerio de Tecnologías de la Información y Comunicaciones.

MNVCC: Modelo Nacional de Vigilancia Comunitaria por Cuadrantes.

NUCINT: Inteligencia Nuclear.

PHOTINT: Inteligencia Fotográfica.

POLFA: Policía Fiscal y Aduanera

PONAL: Policía Nacional de Colombia.

RADINT: Inteligencia de Radar.

SECOP: Sistema Electrónico de Contratación Pública

SICAF: Sistema de Investigación Criminal Antifraude.

SIGINT: Inteligencia de Señales.

SMS: Servicio de Mensajes Cortos (Short Message Service).

TECHINT: Inteligencia Técnica.

TELINT: Inteligencia Telemétrica.

TIC: Tecnologías de la Información y la Comunicación.

UDITE: Unidades de Investigaciones Tecnológicas.

UIAF: Unidad de Información y Análisis Financiero.

CAPITULO I

INTRODUCCIÓN

Teniendo en cuenta que las tecnologías de la información y de la comunicación juegan un rol importante ante las nuevas realidades que viven las personas, la Policía Nacional de Colombia atendiendo los retos que se imponen en esta materia, ha avanzado en la estructuración de estrategias que le permitan garantizar la estabilidad estatal y seguridad ciudadana en el ciberespacio, siendo aun necesario fortalecer la prevención y anticipación de fenómenos que se presentan en este entorno y que pueden llegar afectar a las personas, es por ello que evidenciando esta problemática, se propone en la presente monografía mejorar estos aspectos desde rol de inteligencia, mediante el diseño de un modelo de ciberinteligencia, que incluya actividades de planeación, recolección, tratamiento, análisis y difusión de información

Con base a lo anterior, en el presente trabajo se realiza una propuesta del modelo de ciberinteligencia para la Policía Nacional, por lo cual se realizó inicialmente una conceptualización a partir de las características teóricas que conlleva un modelo de ciberseguridad y ciberinteligencia y su relación con el ciclo de inteligencia, definiéndose para ello ciberinteligencia y presentándose los modelos propuestos por algunos autores. Asimismo, se hizo una revisión de lo que es inteligencia y ciclo de inteligencia, identificándose los modelos que son implementados por otras instituciones, realizándose a partir de esto un análisis de los elementos constitutivos del mismo.

Aunado a lo anterior, se revisaron las capacidades con las cuales cuenta actualmente la Policía Nacional para ejercer control sobre el ciberespacio, se hizo igualmente una

conceptualización de los elementos que conforman el ecosistema de ciberseguridad en la Policía Nacional de Colombia, identificando desde el nivel estratégico, de gestión y tecnológico, los actores y herramientas con los cuales cuenta, finalizando con la elaboración de un análisis que permitió comparar estos elementos con los de ciberinteligencia y validar cuáles pueden ser incluidos en el modelo.

Seguidamente, se procedió a realizar la conceptualización del modelo de ciberinteligencia a partir de los elementos identificados, describiendo los elementos que lo componen y cómo a partir del ciclo de inteligencia se pueden realizar las actividades en el ciberespacio. En la misma dirección, se determinaron de acuerdo con los resultados de los análisis realizados previamente que capacidades de la Policía Nacional deben ser fortalecidas.

Finalmente, con el modelo de ciberinteligencia se proyecta que la Policía Nacional pueda gestionar las actividades de inteligencia en el ciberespacio, como una capacidad adicional para fortalecer la ciberseguridad del País, mediante la prevención y anticipación de ciberamenazas y la conceptualización de fenómenos que se presentan en el ciberespacio.

1.1. Delimitación y alcance del tema de investigación

El presente trabajo se encuentra enmarcado en la línea de investigación "Seguridad Digital" de la Escuela Superior de Guerra, y la propuesta del modelo de ciberinteligencia que se quiere conceptuar se encuentra orientada a la prevención, anticipación y tratamiento de amenazas que se presentan en el ciberespacio, las cuales ponen en riesgo a las personas e intereses del país.

Así mismo, es impórtate aclarar que el propósito de este trabajo no es crear un centro de ciberinteligencia para la Policía Nacional de Colombia (PONAL). Lo que se pretende es elaborar una propuesta que contemple las características claves necesarias para la creación de un Modelo de Ciberinteligencia basado en el Ciclo de Inteligencia utilizado por la PONAL, el cual contribuya a la protección de las ciberamenazas que afectan los intereses del país. En este sentido, puede servir de guía para aquellos que visualicen al Ciclo de Inteligencia como una oportunidad adicional, a las que existan en su regiones o países, para tratar de mitigar las ciberamenazas, las cuales, según Villalba & Corchado (2017) son consideradas como nuevos riesgos que atentan contra la seguridad nacional.

Por otra parte, debido a la reserva de la información de inteligencia, algunos apartes del presente trabajo serán omitidos al momento de su impresión para que repose en los sistemas de información de la Escuela Superior de Guerra.

Finalmente, el alcance del presente trabajo será la Policía Nacional de Colombia, teniendo en cuenta que el modelo se soportará sobre la misionalidad de esta institución y por la naturaleza confidencial de alguna información, la investigación se realizará por medio de la revisión sistemática de literatura, contactos y entrevistas directas con actores en temas de ciberseguridad e inteligencia de la PONAL y experiencia del autor.

1.2. Planteamiento del problema de investigación

Con la aparición de las tecnologías de información y comunicación - TIC, las diferencias

espaciales y temporales entre diversos tipos de actividades sociales también se desvanecen. Con computadoras, teléfonos móviles e internet, muchas tareas diferentes como comprar, pagar las cuentas, hacer tareas, explorar un problema médico, comunicarse con amigos, proponer un negocio, planear una manifestación de protesta, tratar de conocer a personas interesantes, tiene su lugar en una nueva dimensión (Meyrowitz, 2008).

Esto confirma la importancia de considerar las repercusiones e impacto de las TIC en las personas. En torno a ellas, es que cobran vigencia hasta hoy nociones como la sociedad de la información, sociedad del conocimiento, sociedad de red, sociedad virtual, sociedad del «Big Data» (Gertrudis Casado et al., 2016), que se encuentran altamente ligados al fenómeno de las plataformas tecnológicas que hace alusión Gallegos (2007), cuando habla del conjunto de tecnologías que permite la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética.

De acuerdo con Uribe (2016), en 1960 McLuhan planteó que las plataformas tecnológicas son un determinante en la relación particular de la sociedad con las realidades a las cuales se estaba expuesto, permitiendo con esto entender que la producción, la reproducción y la distribución de la información a través de medios tecnológicos podrían ser principios constitutivos de las sociedades actuales; dichos principios estarían enmarcados en procesos tecnológicos con efectos puramente económicos, culturales y sociales, partiendo de que el internet y las redes sociales, tienen ahora mayor protagonismo en el manejo de la información y en los flujos de la comunicación (Arrojo, 2015).

Así mismo, las tecnologías de la información y de la comunicación, han ocasionado una dependencia tecnológica en las personas quienes a través de estas tienen la posibilidad y capacidad de almacenar, transformar, acceder y difundir información, transformando su naturaleza y provocando una fuerte subordinación, así como un cambio de hábitos en la vida diaria del ser humano (Pérez Zúñiga et al., 2018). Esto ha derivado en la aparición de una nueva cultura informática que no respeta fronteras y conduce a un mundo diferente e informado con la incorporación de las TIC y su principal insumo: la información, integrada a la vida cotidiana.

Lo expresado en el párrafo anterior, se evidencia en el caso concreto de Colombia, en el informe realizado por ITU *Measuring the information society report. Vol. 2*, (2018) el cuál dice que:

> *"Colombia es ahora un país más conectado con un mayor uso de las TIC, alcanzando niveles comparables a países similares en todo el mundo. Ha mostrado un aumento significativo en el consumo de banda ancha móvil y tiene potencial de crecimiento. El Gobierno ha realizado importantes esfuerzos para avanzar hacia la digitalización de la economía y mejorar la competencia y los niveles de calidad en los mercados de telecomunicaciones" (p. 39)*

Como se puede observar en la Tabla 1 el número de personas usando internet es del 62,3%, lo cual es sustancialmente superior al 48,6% del número de personas en el mundo.

Tabla 1. Indicadores claves para Colombia 2017. Fuente: ITU Report, (2018)

Indicadores claves para Colombia (2017)		Las Américas	El mundo
Usuarios de telefonía fija por cada 100 habitantes	14.2	23.9	13.0

Indicadores claves para Colombia (2017)		Las Américas	El mundo
Usuarios de telefonía móvil por cada 100 habitantes	126.8	111.8	103.6
Usuarios de banda ancha activos por cada 100 habitantes	48.8	89.5	61.9
Cobertura 3G (% de la población)	100.0	93.9	87.9
Cobertura LTE / WiMAX (% de la población)	96.0	84.3	76.3
Individuos usando internet (%)	62.3	67.5	48.6
Casas con un computador (%)	44.3	64.8	47.1
Casas con acceso a internet (%)	50.0	68.3	54.7
Banda de ancha Internacional por usuario de internet (Kbit/seg)	157.1	77.1	76.6
Usuarios de banda ancha fija por cada 100 habitantes	12.9	19.9	13.6
Usuarios de banda ancha fija por niveles de velocidad, % de distribución			
-256 Kbit/s a 2 Mbit/s	4.5	6.6	4.2
-2 a 10 Mbit/s	69.1	23.1	13.2
Igual o superior a 10 Mbit/s	26.4	70.3	82.6

Así mismo, en la Tabla 1 se evidencia que cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia se tiene de los sistemas de información y de las comunicaciones. Cualquier intrusión, manipulación, sabotaje, o interrupción de dichos sistemas pueden llegar a ser sufridos por millones de personas (Leiva, 2015) y estos sistemas se encuentran en el dominio que se conoce como ciberespacio. En la Tabla 2 se realiza una recopilación de diferentes definiciones del ciberespacio encontradas.

Tabla 2. Definición de ciberespacio. Fuente: elaboración propia a partir del documento "Controles de Seguridad Propuesta inicial de un Framework en el contexto de la Ciberdefensa" (Gastón Sack & Ierache, 2015, p. 3-4), lo expuesto en la resolución 2258 de 2009 expedida por la Comisión de Regulación de Comunicaciones y la Monografía 126 "El ciberespacio. Nuevo escenario de confrontación" (CESDEN, 2012)

Organismo o país	Definición
Comisión de Regulación de Comunicaciones	El ciberespacio es un 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 (Comisión de Regulación de Comunicaciones, 2009).

Organismo o país	Definición
Monografía 126 CESDEN "El ciberespacio. Nuevo escenario de confrontación"	El espacio artificial creado por, el conjunto de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial. El ciberespacio es sin embargo, mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio (CESDEN, 2012).
Real Academia Española.	Ámbito artificial creado por medios informáticos. Esto quiere decir que para implementar el ciberespacio se necesita de una infraestructura física de computadoras y líneas de comunicaciones que las mantengan interconectadas (Gastón Sack & Ierache, 2015, p. 3).
National Institute of Standards and Technology (NIST).	Dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de sistemas de información que incluyen: internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores (Gastón Sack & Ierache, 2015, p. 3).
Unión Europea.	Espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo.
Unión Internacional de Telecomunicaciones.	Lugar creado a través de la interconexión de sistemas de ordenador mediante Internet (Gastón Sack & Ierache, 2015, p. 3).
España.	Conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos (Gastón Sack & Ierache, 2015, p. 3).
Estados Unidos (DoD).	Dominio global dentro del entorno de la información, consistente en la red interdependiente de las infraestructuras de tecnología de la información incluida la Internet, redes de telecomunicaciones, sistemas informáticos, los procesadores y controladores (Gastón Sack & Ierache, 2015, p. 3).
Estados Unidos (National Military Strategy for Cyberspace Operations).	Dominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas asociadas (Gastón Sack & Ierache, 2015, p. 3).
Alemania.	Espacio virtual de todos los sistemas informáticos vinculados a nivel de datos a escala global. La base para el ciberespacio es el Internet como una red de conexión y transporte universal y accesible al público que puede ser complementada y más expandido en cualquier número de redes de datos adicionales. Sistemas de informáticos en un espacio virtual aislado no son parte del ciberespacio (Gastón Sack & Ierache, 2015, p. 4).
Reino Unido.	Todas las formas de actividades en redes digitales; esto incluye el contenido y acciones realizadas a través de redes digitales (Gastón Sack & Ierache, 2015, p. 4).

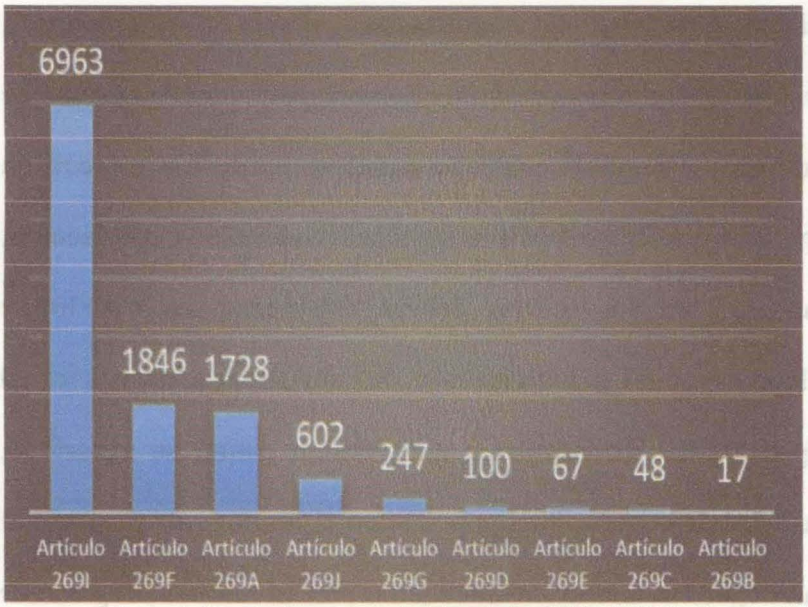
Para efectos de esta monografía se utilizará la definición expuesta por la Comisión de Regulación de Comunicaciones, teniendo en cuenta que describe al ciberespacio como un nuevo ambiente utilizado por los usuarios para interactuar, es decir, personas conviviendo en este entorno

y expuestos a sus amenazas y riesgos, los cuales deben ser gestionados con el fin de evitar los efectos no deseados que podrían afectar la integridad de los ciudadanos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016), como es el caso del cibercrimen el cual se entiende según Rayon y Gómez (2014) como:

> *"cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito" (p. 211)*

El cibercrimen contiene los delitos informáticos, toda vez que apoyados en la definición de Majid Yar (2006) donde dice que *"la delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino* más *bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar"* (p. 5), se entiende que todo delito informático es un cibercrimen.

Para el caso de Colombia, durante el 2017, según cifras de la Dirección de Investigación Criminal e Interpol (DIJIN), se presentaron 13.774 denuncias; en el 2014 la víctima potencial era el ciudadano con una representación del 92% de afectados, cifra que varió para el 2017 donde se registró un aumento de este tipo de delitos en un 28%, evidenciándose 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 a través del ciberespacio (Policía Nacional de Colombia, 2017) como se observa en la Figura 1.



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

Figura 1. Denuncias por violación a la ley 1273 de 2009. Fuente: Policía Nacional de Colombia, (2017)

La Policía Nacional atendiendo los retos que se imponen en esta materia, ha avanzado en la estructuración de estrategias que le permitan garantizar la estabilidad estatal y seguridad ciudadana en el ciberespacio, a partir de las directrices impartidas en la Política de Seguridad de Ciberseguridad y Ciberdefensa (Ministerio de Interior y de Justicia et al., 2011), en la cual se establece que el Centro Cibernético Policial (CCP) estará encargado de la Ciberseguridad del territorio colombiano.

Por otra parte, no se debe desconocer que la Policía Nacional a través de la Dirección de Inteligencia Policial en cumplimiento a su función de inteligencia, debe proteger los derechos humanos, prevenir, anticipar y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional (Congreso de la República, 2013) por lo cual debe contribuir con la prevención y anticipación de ciberamenazas (cibercrimen).

Finalmente, la Policía Nacional debe entablar medidas para atacar estas amenazas, entendiendo que los riesgos son particularmente importantes en el ciberespacio donde la ruta que los datos siguen a través de Internet raramente se puede controlar o incluso predecir con precisión (Raymond, 2014), siendo necesario generar desde el rol de inteligencia actividades de recolección, tratamiento y análisis de información, para lo cual se deberá establecer un modelo de ciberinteligencia que se oriente a la prevención y anticipación de amenazas presentes en el ciberespacio, a las cuales están expuestos los ciudadanos y que atentan contra su seguridad, cumpliendo de esta forma su misionalidad de generar inteligencia, con el objetivo de prevenir la materialización de riesgos que puedan llegar a afectar a los ciudadanos en Colombia (Congreso de la República, 2013), el cual en la actualidad no existe.

1.3. Pregunta de investigación

¿Cómo incorporar la ciberinteligencia en el modelo del ciclo de inteligencia utilizado por la Policía Nacional?

1.4. Justificación

La actividad de policía en su entorno natural, debe contemplar la totalidad de riesgos asociados al sistema de acción social de la convivencia, entre ellos los crecientes fenómenos de interacción humana que se desarrollan el ciberespacio, en donde de acuerdo con Miró (2011) aparece un nuevo ámbito de oportunidad delictiva en un contexto de riesgo criminal distinto al espacio nacional físico tradicional.

> *"...conforme las TIC vayan avanzando y la vida diaria de las personas se vaya desarrollando en el ciberespacio, aumentando los bienes que son puestos en el mismo, incrementándose el valor de la información, y ampliándose las formas de interacción social en Internet, la delincuencia en Internet aumentará y no será, como parece ahora, testimonial, sino que tendrá cada vez mayor importancia.". (Miró, 2011, p. 38) .*

Por su parte, el Departamento Nacional de Seguridad de España en su Estrategia de Seguridad Nacional (2013), expone que las amenazas en el espacio digital están adquiriendo una dimensión que va más allá de la tecnología, convirtiéndose el ciberespacio en un escenario con características propias marcadas por su componente tecnológico que gracias a su fácil accesibilidad, anonimidad, alta conexión y dinamismo, permite la generación de acciones negativas en el ámbito de la ciberseguridad las cuales han aumentado notablemente en número, alcance y sofisticación. Aunado a lo anterior, el Departamento Nacional de Planeación de Colombia afirma que:

> *"El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil."* (Ministerio de Interior y de Justicia et al., 2011).

Este nuevo contexto tecnológico demanda la intervención estatal con el fin de regular la actividad social que se desarrolla en estos espacios virtuales, y es precisamente la institución

policial, dada su misión constitucional (Constitución política de Colombia, 1991, art. 218), el organismo llamado a realizar esta intervención, para garantizar la seguridad ciudadana en relación a la prevención del cibercrimen.

Dado lo anterior, el Gobierno Nacional consciente de la nueva problemática define su Política de Seguridad Digital, estableciendo como uno de sus objetivos el "fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos" para lo cual planteó como una de sus estrategias para su cumplimiento, mejorar las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológicas del CCP de la Policía Nacional y la de los organismos de Inteligencia del Estado (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

Por lo anterior, la Policía Nacional en cumplimiento a su misión de mantener las condiciones necesarias para asegurar que los habitantes de Colombia convivan en paz descrita en el artículo 218 de la Constitución (Constitución Política de Colombia, 1991), se le otorgó con la creación de la Dirección de Inteligencia Policial y expedición de la Ley 1621 de 2013 la función de inteligencia y contrainteligencia, facultándola para utilizar medios humanos o técnicos en el desarrollo de actividades de recolección, procesamiento, análisis y difusión de información, siendo uno de sus objetivos prevenir amenazas internas o externas que atenten contra de la seguridad nacional (Congreso de la República, 2013).

A partir de lo descrito anteriormente y dado que la inteligencia es un campo de estudio multidisciplinar, los procesos de transformación (digitalización de información, hiperconexión,

presencia online, etc.) han provocado que muchas de las nuevas amenazas asociadas a estos desarrollos den como resultado la necesidad adecuar las tareas de inteligencia a una realidad marcada por el uso intensivo de tecnología conectada (C. T. Blanco, 2017), requiriéndose que la función de inteligencia para el cumplimiento de su misión deba desarrollarse en el ciberespacio.

En efecto, en este ambiente son detectadas peligrosas amenazas y vulnerabilidades que en caso de concretarse pueden poner en riesgo la seguridad de las personas, por lo cual se hace necesario contar con una capacidad de monitorear y generar alertas tempranas para evitar situaciones críticas que afecten la seguridad pública e inclusive la nacional, a partir de la aplicación de técnicas y métodos tradicionales del ámbito de la inteligencia, (C. T. Blanco, 2017).

Lo expresado anteriormente, conlleva a revisar la metodología de obtención y procesamiento de la información para la producción de inteligencia y contrainteligencia policial, descrita a través del ciclo de inteligencia compuesta por las fases de "planear y dirigir", "recolectar", "tratar", "analizar" y "comunicar e integrar" (Policía Nacional de Colombia, 2014), con el fin de modernizarlo e incorporar el uso de tecnologías que permitan mejorar las capacidades de detección y respuesta, proporcionando información relevante para apoyar el proceso de tomas de decisiones en cuestiones relativas al ciberespacio (Candau, 2017).

Por lo anterior, y en cumplimiento a la estrategia de fortalecimiento de los organismos de inteligencia responsables de la ciberseguridad, la Dirección de Inteligencia de la Policía Nacional tiene la responsabilidad de migrar sus actividades al espacio digital, adaptando su modelo actual del ciclo de inteligencia a uno de ciberinteligencia, que le permita dar cumplimiento a su

misionalidad y contribuir al cumplimiento de los objetivos de la Política Nacional de Seguridad Digital, establecida en el CONPES 2016, todo a su vez enmarcado en el cumplimiento constitucional y legal existente, aspecto que también fue evidenciado en el CONPES 3701 "Política de Ciberseguridad y Ciberdefensa" (Ministerio de Interior y de Justicia, 2011).

1.5. Objetivos

Objetivo General

Proponer un modelo de ciberinteligencia basado en el ciclo de inteligencia utilizado por la Policía Nacional.

Objetivos Específicos

1. Describir las características teóricas y conceptuales que conlleva un modelo de ciberseguridad y ciberinteligencia en términos específicos y su relación con el ciclo de inteligencia.
2.
3. Identificar las capacidades y los componentes en la Policía Nacional para la construcción del modelo de ciberinteligencia soportado en el ciclo de inteligencia actual.
4. Conceptuar un modelo de ciberinteligencia para la Policía Nacional el cual se adapte al ciclo de inteligencia.

1.6. Marco Metodológico

Se utilizará una metodología cualitativa, la cual es la recolección de información basada en la observación de comportamientos naturales, discursos, respuestas abiertas para la posterior interpretación de significados (Hernández et al., 2014). El método cualitativo analiza el conjunto del discurso entre los sujetos y la relación de significado para ellos, según contextos culturales, ideológicos y sociológicos (Rodríguez et al., 1996), así mismo el tipo de modelo utilizado para el desarrollo del trabajo será una de tipo causal, la cual trata de explicar las causas por las cuales ocurren determinadas situaciones, hechos o fenómenos. En ese sentido, en este tipo de trabajo se encontrará la descripción de las variables de un fenómeno, así como el análisis de la relación que existe entre ellas y sus respectivas consecuencias en el modelo y los lineamientos.

CAPITULO II

CARACTERÍSTICAS TEÓRICAS Y CONCEPTUALES QUE CONLLEVA UN MODELO DE CIBERSEGURIDAD Y CIBERINTELIGENCIA EN TÉRMINOS ESPECÍFICOS Y SU RELACIÓN CON EL CICLO DE INTELIGENCIA

1. Diferencia entre modelo, método, metodología y técnica

Para el presente trabajo es fundamental establecer la razón por la cual se eligió un modelo para representar el ciclo de inteligencia, partiendo de lo expuesto por Mintzberg (2005), quien establece que los modelos permiten la construcción científica bajo la cual se sustenta la realidad de una organización, por lo tanto, este será la representación o el arquetipo de la realidad que se pretenderá desplegar luego en la institución.

Para entender con mayor detalle la diferencia entre modelo, método, metodología y técnica se presentan sus definiciones en la Tabla 3.

Tabla 3. Definición de conceptos. Fuente: Elaboración propia a partir de Mintzberg, (2005)

Elemento	Definición
Modelo	Modelo es la forma en que se concibe que ha de desarrollarse la representación o el arquetipo de una realidad organizacional. Un modelo es la manera que tiene las personas en las organizaciones de considerar como se va a proceder en las actividades o labores encomendadas. Se puede decir que un modelo es la construcción científica bajo la cual se sustenta la realidad de una organización (Mintzberg et al., 2005). En suma, el modelo es la representación teórica de algo que posteriormente se lleva a la práctica en un contexto concreto.

Elemento	Definición
Método	El método es la manera de poner en práctica el modelo construido. El método se relaciona con un determinado estilo de gerencia que pone en práctica de forma coherente el modelo que se tenga como "creencia". El método posibilita que se desarrollen las actividades que se desarrolle en las organizaciones las prácticas necesarias para la aplicación del modelo descrito (Mintzberg et al., 2005).
Metodología	Con la metodología se concreta el método en el contexto determinado para la consecución de unos objetivos determinados en función de la realidad empresarial y de las características específicas. Se distingue del método porque concreta aún más dependiendo del medio en el que se esté y de los recursos con los que se cuente. La metodología es uno de los elementos fundamentales que contiene el conjunto de estrategias, procedimientos y acciones organizadas y planificadas por las personas de la organización, de manera consciente y reflexiva, con la finalidad de posibilitar el cumplimiento de los objetivos generales de la organización.
Técnica	Las técnicas o estrategias son lo más concreto en la realidad de las aulas. Son la aplicación última del modelo diseñado que desarrollan y aplican las actividades concretas en momentos específicas para determinadas personas.

Por lo anterior, se puede reafirmar y concluir que el modelo es la forma más cercana de entender, representar, construir y definir el ciclo de inteligencia para la institución.

2. Ciberseguridad

En el marco de la presente investigación es necesario identificar los conceptos que se requerirán para establecer la propuesta del modelo de ciberinteligencia, para lo cual se iniciará con el término de ciberseguridad el cual conforme a lo expuesto por el CONPES 3701, es la "capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (Ministerio de Interior y de Justicia et al., 2011, p. 2).

Por su parte, Fojón y Sanz establecen que la ciberseguridad "consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados" (Fojón & Sanz, 2010, p. 2).

De igual forma, la Unión Internacional de Telecomunicaciones – ITU (2008) define ciberseguridad como el "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" (p.9).

Así mismo, la ITU (2008) dice que la ciberseguridad permite alcanzar y mantener la confidencialidad, integridad y disponibilidad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

En complemento a lo anterior, Sancho (2017) establece que la ciberseguridad es considerada también una condición, que permite a los ciudadanos, organizaciones e instituciones beneficiarse de la utilización de ciberespacio, al ser esta una dimensión en la cual se efectúan las relaciones sociales en forma más rápida y económica en diferencia a otras, lo cual obliga a reconocer la importancia de la seguridad en esta nueva dimensión y asumirla con su complejidad.

Lo anterior, genera una nueva preocupación frente a como generar controles para garantizar la seguridad de los ciudadanos en el ciberespacio, lo cual ha obligado a los estados y

organizaciones a diseñar marcos o frameworks que permitan coordinar y estandarizar las actividades en pro de la ciberseguridad.

2.1. Marcos de Ciberseguridad

Como ejemplo de esto, se encuentra el "Marco para la mejora de la seguridad cibernética en infraestructuras críticas" definido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), el cual es una "metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información" (Instituto Nacional de Estándares y Tecnología, 2018, p. 3) y cuenta con un núcleo compuesto por cinco funciones: identificar, proteger, detectar, responder y recuperar (Figura 2).

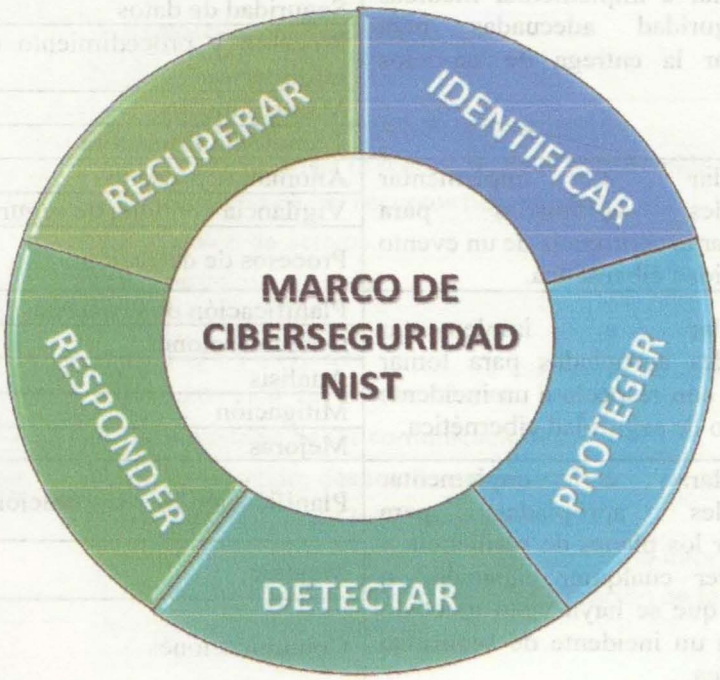


Figura 2. Marco de Ciberseguridad NIST. Fuente: (Instituto Nacional de Estándares y Tecnología, 2018)

La funciones del marco de ciberseguridad NIST, tienen unas categorías y subcategorías que describen actividades específicas de seguridad cibernética que suelen ser comunes en los sectores de infraestructura críticas que le permite a las organizaciones administrar sus riesgos de forma adecuada y coordinada (Instituto Nacional de Estándares y Tecnología, 2018), como se observa en la Tabla 4.

Tabla 4. Funciones y categorías del modelo NIST. Fuente: elaborado a partir de la información del Instituto Nacional de Estándares y Tecnología, (2018)

FUNCIÓN	DESCRIPCIÓN	CATEGORIAS
Identificar	Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.	Gestión de activos
		Entorno empresarial
		Gobernanza
		Evaluación de riesgos
		Estrategia de gestión de riesgos
		Gestión del riesgo de la cadera de suministro
Proteger	Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.	Gestión de identidad y control de acceso
		Conciencia y capacitación
		Seguridad de datos
		Procesos y procedimiento de protección de la información
		Mantenimiento
		Tecnología Protectora
Detectar	Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.	Anomalías y eventos
		Vigilancia continua de seguridad
		Procesos de detección
Responder	Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.	Planificación de respuesta
		Comunicaciones
		Análisis
		Mitigación
		Mejoras
Recuperar	Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.	Planificación de recuperación
		Mejorar
		Comunicaciones

Por otra parte, también existen normas técnicas como la ISO/IEC 27001, la cual contiene los requisitos y metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización (Instituto Nacional de Normas Técnicas y Certificación - ICONTEC, 2013). Esta norma específica los requisitos necesarios para establecer, implementar, mantener y mejorar la seguridad de la información mediante la aplicación del ciclo PHVA (planear, hacer, verificar y actuar), apoyado en 14 numerales y 114 controles para seguridad de la información (Instituto Nacional de Normas Técnicas y Certificación - ICONTEC, 2013) como se observa en la Figura 3.

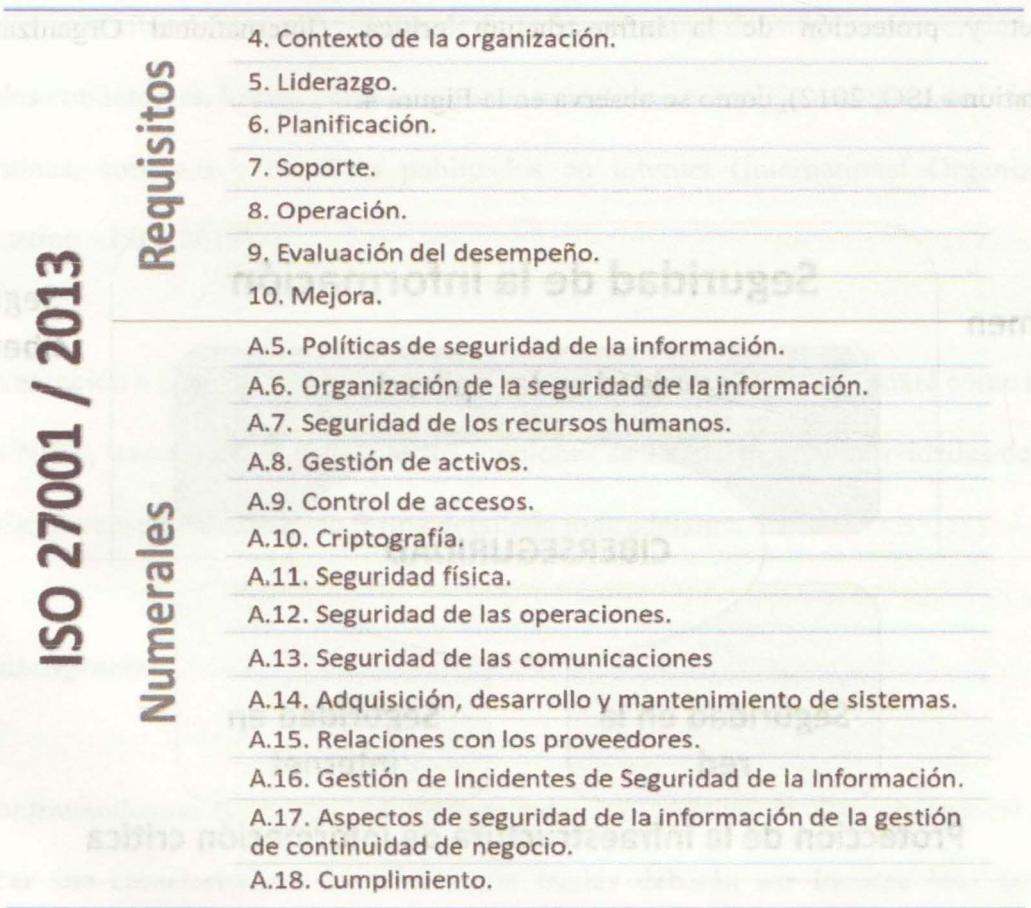


Figura 3. Estructura de la norma ISO 27001-2013. Fuente: elaboración propia a partir de la información Instituto Nacional de Normas Técnicas y Certificación – ICONTEC, (2013)

Como una de las características principales de la ISO/IEC 27001 es la inclusión de los requisitos para la valoración y tratamiento de riesgos de seguridad de la información, os cuales son adaptados a las necesidades de las organizaciones (Instituto Nacional de Normas Técnicas y Certificación - ICONTEC, 2013).

Otra norma que establece de forma más directa un marco de ciberseguridad es la norma ISO/IEC 27032, la cual a partir de un enfoque estratégico y técnico ofrece una guía para implementar buenas prácticas de seguridad para organizaciones, destacando las dependencias con otros dominios de seguridad como la seguridad de la información, seguridad en la red, seguridad en internet y protección de la infraestructura crítica. (International Organization for Standardization - ISO, 2012), como se observa en la Figura 4.

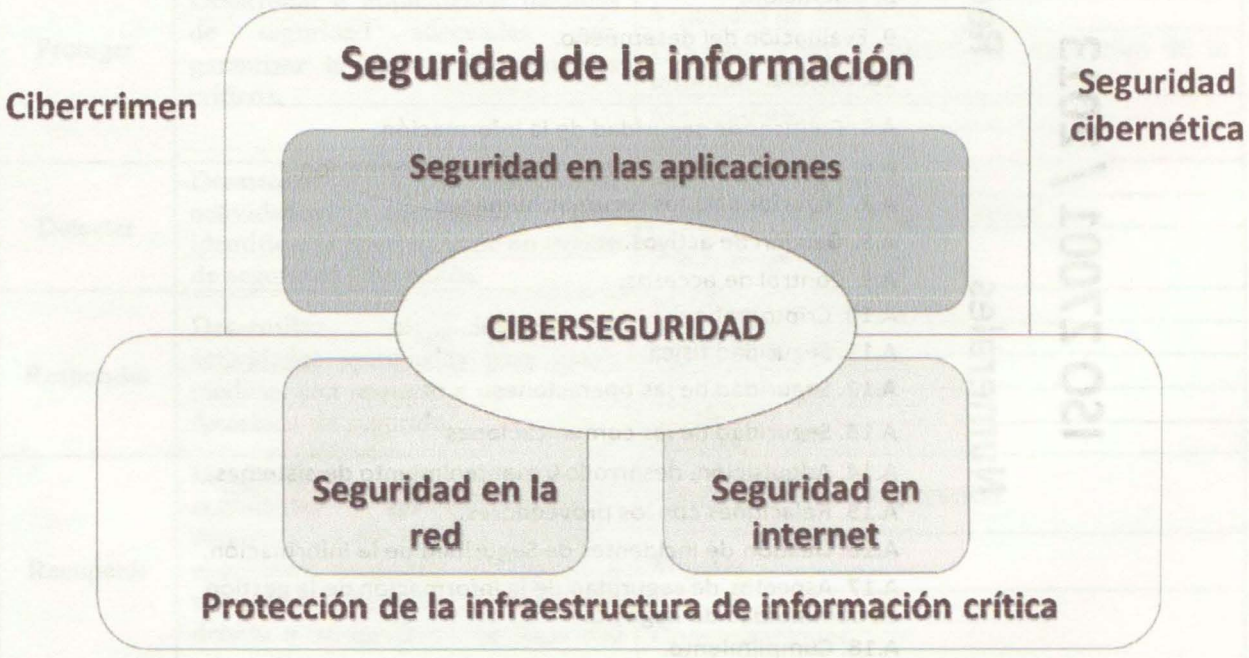


Figura 4. Relación entre ciberseguridad y otros dominios de seguridad. Fuente: International Organization for Standardization - ISO, (2012).

Así mismo la ISO/IEC 27032, se enfoca en dos aspectos, la primera es la de cerrar las brechas entre los diferentes dominios de la seguridad, para los cual aborda los riesgos comunes entre estos como son: ataques de ingeniería social, hacking, malware, software espía y otros softwares potencialmente no deseados; el segundo enfoque, está relacionado con la colaboración, teniendo en cuenta que existe la necesidad de compartir información, coordinar y manejar eficientemente los incidentes entre todas las partes interesadas que interactúan en el ciberespacio (International Organization for Standardization - ISO, 2012).

Como aspecto importante de la ISO/IEC 27032, es que esta norma no aborda temas relacionados con ciberdelitos, protección de la infraestructura de información crítica y delitos relacionados con internet, lo cual considera que es un entorno complejo resultado de la interacción entre personas, software y servicios publicados en internet (International Organization for Standardization - ISO, 2012).

En atención a lo expuesto anteriormente, para el presente trabajo se tomará como referencia el modelo NIST, teniendo en cuenta que sus funciones se asemejan a las actividades del ciclo de inteligencia, el cual será descrito de forma detallada más adelante.

2. Ciberinteligencia

Continuando con el capítulo, se requiere indagar el termino de ciberinteligencia con el fin de verificar sus características principales, las cuales deberán ser incorporadas como parte fundamental del modelo que se proyecta establecer en la presente investigación.

Inicialmente, al hacer una revisión etimológica del término de ciberinteligencia, se evidencia que está conformado por dos palabras: ciber (hace referencia al ciberespacio) e inteligencia, por lo cual puede decirse que hace referencia a la confluencia de dos posibles disciplinas (Blanco, 2018)

INSA por su parte, define la ciberinteligencia como *"los productos y procesos a lo largo del ciclo de inteligencia para evaluar las capacidades, intenciones y actividades, técnicas y de otro tipo, de posibles adversarios y competidores en el dominio cibernético"* (INSA, 2015, p. 7).

De igual forma, el Centro de Innovación SEI define ciberinteligencia como la *"adquisición y el análisis de información para identificar, rastrear y predecir capacidades, intenciones y actividades cibernéticas que ofrecen cursos de acción para mejorar la toma de decisiones"* (Carnegie Mellon University, 2013, p. 2). Este concepto está mucho más próximo a la conceptualización clásica de inteligencia.

Así mismo, el Centro de Innovación SEI capturó las características del análisis de ciberinteligencia y creó un enfoque que muestra con mayor precisión las interdependencias y las influencias externas en el proceso de ciberinteligencia, como se observa en la Figura 5. Este enfoque incorpora cómo la tecnología influye en la forma en que se realiza el análisis e identifica de forma exclusiva las funciones que integran la tecnología, utilizando para ello cinco funciones (Tabla 5) la cuales capturan las interdependencias e influencias externas (Carnegie Mellon University, 2013).

Figura 5. Marco Analítico de Ciberinteligencia. Fuente: (Carnegie Mellon University, 2013)

Tabla 5. Funcionarios del Marco Analítico de Ciberinteligencia. Fuente: elaboración propia a partir de la información presenta por el Centro de Innovación SEI (Carnegie Mellon University, 2013)

Funciones	Descripción
Medio ambiente	Establece el alcance del esfuerzo de la ciberinteligencia e influye en los datos necesarios para lograrlo.
Recopilación de datos	A través de medios automatizados y laboriosos, los analistas exploran las fuentes de datos, recopilan información y la agregan para realizar análisis.
Análisis funcional	Los analistas utilizan los datos recopilados para realizar análisis técnicos y personalizados, generalmente en apoyo de una misión de seguridad cibernética.
Análisis estratégico	Los analistas aplican una lente estratégica a los datos funcionales e informan esta inteligencia a las partes interesadas o la utilizan para influir en el medio ambiente. Si el análisis funcional intenta responder al "qué" y al "cómo" de las amenazas cibernéticas, el análisis estratégico tiene como objetivo responder "quién" y "por qué".
Informar y retroalimentar	La inteligencia se difunde a las partes interesadas, proporcionan comentarios y / o utilizan la inteligencia para influir en el medio ambiente

Continuando con las definiciones de ciberinteligencia, la Estrategia Nacional de Inteligencia de los Estados Unidos (2014) establece que esta es la recopilación, procesamiento, análisis y difusión de información de todas las fuentes de inteligencia sobre programas cibernéticos, intenciones, capacidades, investigación y desarrollo, tácticas y actividades e indicadores operativos de actores extranjeros; identificando el impacto o posibles efectos sobre la seguridad nacional, los sistemas de información, la infraestructura y los datos, así como la caracterización de la red, o comprensión de los componentes, estructuras, uso y vulnerabilidades de los sistemas de información extranjeros.

Aunado a lo anterior, Javier Candau opina que desde el Centro Criptológico Nacional (CCN) creen que la ciberinteligencia es más compleja y coincide con la definición del profesor Manuel Torres Soriano, quien considera la ciberinteligencia como *"la actividad analítica cuyo propósito es proporcionar información relevante para apoyar el proceso de toma de decisiones en cuestiones relativas al ciberespacio"* (Candau, 2017).

Por su parte, Blanco (2018), considera que a la hora de adoptar una definición sobre ciberinteligencia, es preciso atender tanto a la raíz del concepto, con sus dos componentes "ciber" e "inteligencia", como a la doctrina de inteligencia que muestra claramente el CCN-CERT, al proponer el siguiente concepto: *"proceso (y producto final) de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas y orientado a la toma de decisiones, en tiempo, lugar y forma"* (Blanco, 2018, p. 20).

Igualmente, Blanco (2018) identifica algunos elemento a tener en cuenta a la hora de definir

ciberinteligencia:

1. Es un proceso característico de inteligencia.
2. Se realiza sobre el ciberespacio, el cual es el centro de dedicación de la ciberinteligencia, convirtiéndose en un medio para obtener y analizar datos e información y como una fuente de riesgos y amenazas a la seguridad nacional.
3. Es realizado por especialistas, tanto en ciberseguridad como en análisis de inteligencia.
4. Exige unos requisitos formales para poder ser considerado como inteligencia, y siendo válido para un momento y lugar.
5. Su objetivo es la acción, el apoyo a la toma de decisiones

Finalmente, Blanco (2018) a partir del análisis del marco de trabajo de ciberseguridad del National Institute of Standard and Tecnology, propone el proceso de ciberinteligencia descrito en la Figura 6, el cual es el resultado de unificarlo con el ciclo tradicional de inteligencia y el modelo NIST:

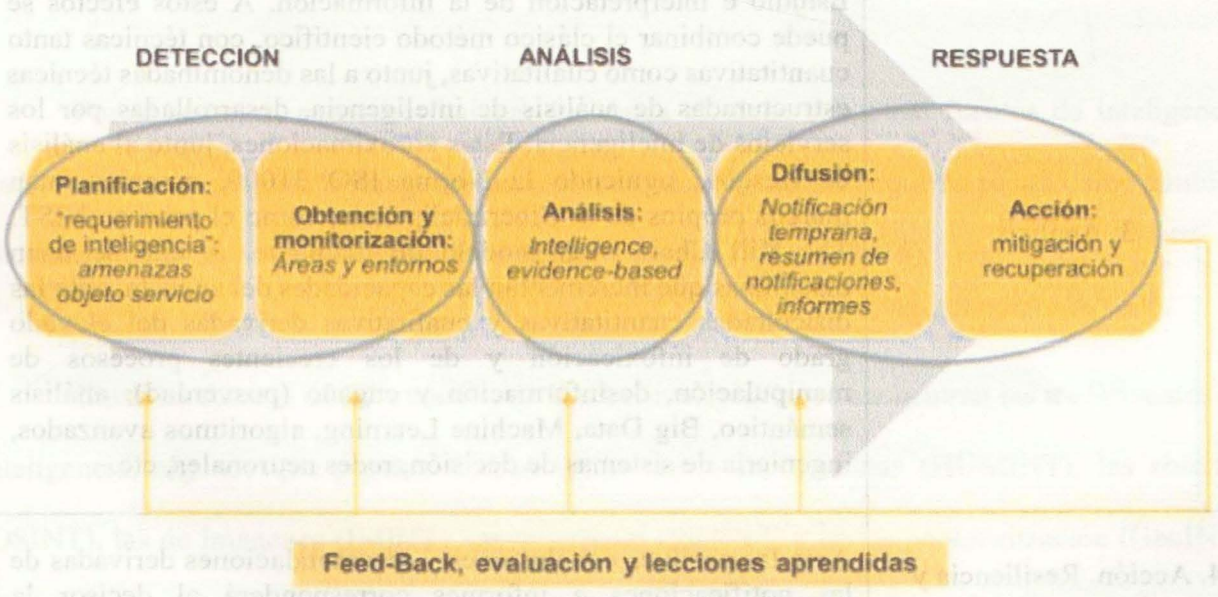


Figura 6. Proceso de Ciberinteligencia. Fuente: Blanco, (2018).

Las actividades del proceso de ciberinteligencia se describen en la Tabla 6:

Tabla 6. Actividades del Proceso de Ciberinteligencia. Fuente: Blanco, (2018), p. 24.

Funciones	Descripción
1. Definición, planificación y parametrización	De acuerdo con el requerimiento de inteligencia (el "para qué" que genera la necesidad del análisis), se procede a determinar el alcance, plazos y recursos precisos. Posteriormente se lleva a cabo un plan para la parametrización de las fuentes y palabras claves sobre las herramientas de detección automatizada que se puedan utilizar, de manera que los sistemas queden preparados para la monitorización automática.
2. Obtención y monitorización:	Una vez los sistemas de inteligencia han sido parametrizados y puestos en operación de acuerdo con la fase anterior, los mismos se encargarán de la recopilación automática de la información para la detección de potenciales eventos de ciberseguridad y su posterior análisis por parte de los operadores y analistas del servicio. En esta fase se realizan tareas como la propia obtención, filtrado, evaluación, clasificación e integración de la información.
3. Análisis	Estudio e interpretación de la información. A estos efectos se puede combinar el clásico método científico, con técnicas tanto cuantitativas como cualitativas, junto a las denominadas técnicas estructuradas de análisis de inteligencia, desarrolladas por los servicios de inteligencia. Estas aproximaciones, junto al análisis de riesgos, siguiendo la Norma ISO 31000, complementan marcos propios de la Ciberinteligencia, como el proceso NIST, The Kill Chain o el modelo de diamante. A ello se unen disciplinas que incrementan las capacidades del analista, ante las dificultades cuantitativas y cualitativas derivadas del elevado grado de infoxicación y de los crecientes procesos de manipulación, desinformación y engaño (posverdad): análisis semántico, Big Data, Machine Learning, algoritmos avanzados, ingeniería de sistemas de decisión, redes neuronales, etc.
4. Acción. Resiliencia y respuesta	Ante las posibles conclusiones y recomendaciones derivadas de las notificaciones e informes corresponderá al decisor la adopción de las medidas oportunas o necesarias.

Funciones	Descripción
5. Retroalimentación y mejora continua	Periódicamente se llevan a cabo ejercicios para compartir conocimientos, mejorar la calidad de los entregables, disminuir los tiempos de respuesta y abordar oportunidades de mejora. Igualmente abordan desviaciones y oportunidades de mejora en base a los resultados de los indicadores de medición de cada servicio, con el objetivo de mejorar de manera continuada y maximizar la eficiencia de las actividades, la calidad de los entregables y minimizar los tiempos de respuesta.

Otros autores como Eva Martín (Martin, 2016), consideran que la ciberinteligencia es un prerrequisito para mantener la superioridad en el ciberespacio, la cual incluye la ciber vigilancia y el ciber reconocimiento. Asimismo, opina que la ciberinteligencia no debe limitarse a comprender las actividades y operaciones de red, esta debe incluir la obtención y el análisis de información para elaborar un producto y oportuno, relevante y con contexto que ayude a los decisores, teniendo presente que las fuentes de información pueden extenderse a una amplia variedad de datos sobre redes, ciberactividades en curso por todo el mundo y hechos geopolíticos destacados, lo importante es que contribuya a reducir la incertidumbre para el decisor.

Por lo anterior, conviene fusionar los datos técnicos con otras fuentes de inteligencia tradicionales para mejorar la imagen situacional, no basta con analizar qué ha pasado, sino también identificar cómo se ha hecho, quién lo ha hecho y porqué (Martin, 2016).

Entre las fuentes de información de la ciberinteligencia, se encuentran las tradicionales de inteligencia, algunos que pueden resultar útiles serían las humanas (HUMINT), las abiertas (OSINT), las de imágenes (IMINT), las de señales (SIGINT, y las de geolocalización (GeoINT) (Kornmaier & Jaouen, 2014).

Finalmente, para la presente investigación se tendrá en cuenta como definición de "ciberinteligencia" la expuesta por el Centro de Innovación SEI, en la cual se precisa como la recolección y el análisis de la información para identificar, rastrear y predecir cibercapacidades, intenciones y actividades que ofrecen cursos de acción para mejorar la toma de decisiones (Carnegie Mellon University, 2013), orientándolo principalmente a temas de ciberseguridad en cuanto a prevención de amenazas o incidentes de naturaleza cibernéticos a los que están expuestos las personas.

3. Cibercrimen

El desarrollo de Internet y de las nuevas tecnologías asociadas con la información y las comunicaciones convierten al ciberespacio en un lugar de oportunidades para las personas y comunidades, pero también lo hace un escenario para la ejecución de actividades delictivas de diversa índole, como comportamientos de acoso escolar y extorsión, hasta reclutamiento criminal (Ministerio de Defensa Nacional, 2019) o en otros caso se ejecuten ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual y hasta la integridad física y la vida (Rayón Ballesteros & Gómez Hernández, 2014).

Afortunadamente, aunque la mayoría de las conductas no son, en esencia, algo nuevo en sí mismas la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, confiere a estas conductas una especial configuración que obligan a romper los esquemas clásicos (Rayón Ballesteros & Gómez Hernández, 2014), y se convierten en retos para la seguridad ciudadana, particularmente en cuanto a prevención, capacidades de persecución y articulación

institucional (Ministerio de Defensa Nacional, 2019).

Tales conductas, de acuerdo a Casabona (2006) es lo que se considera cibercrimen, que según este autor es cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.

Por su parte, Gustavo Saín (2018) opina que el cibercrimen no representa un tipo de criminalidad específica, no es parte del crimen completo ni organizado, ni tampoco pueden ser considerados delitos de cuello blanco. Igualmente, aclara que cuando se habla de delitos informáticos se hace referencia a aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto de este. En este sentido, los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo (Sain, 2018).

En complemento a lo anterior, Sain (2018) afirma que los delitos informáticos pueden clasificarse en dos grandes grupos:

1. Aquellos que requieren de una sofisticación técnica para su comisión, generalmente basado en la elaboración de programas maliciosos desarrollados por hackers que buscan vulnerar los dispositivos o redes, generalmente con fines económicos y aquellos delitos que adquieren una nueva vida en la nube y son intermediados por servicios y aplicaciones web

como las amenazas, los fraudes, el grooming.

2. Delitos vinculados a la violación de la privacidad de las personas.

Por su parte, Marcelo Tamperini (2018) define cibercrimen como:

> *"una serie de delitos informáticos que ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas, donde los sujetos pasivos de los delitos son elementos fungibles y sin interés para el ciberdelincuente, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje" (p. 56).*

Como ejemplo de esta definición, Tamperini (2018), ejemplifica como cibercrimen el ransomware, un tipo de malware (software malintencionado) que tiene como objetivo bloquear cifrando el acceso a toda o parte de la información que contiene el equipo, para después poder pedir un rescate a cambio de su liberación, siendo esto uno de los casos donde los ciberdelincuentes no están interesados en el objetivo o en la víctima, en su información en particular, sino que se realiza de forma masiva, buscando un fin de lucro, que es el pago por el rescate.

Otro caso similar de cibercrimen, son las estafas electrónicas como la captación ilegítima de datos confidenciales (datos de las tarjetas de crédito por ejemplo), generalmente a través del phishing, el cual es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por un contacto (Temperini, 2018)

En consecuencia a lo anterior, diferentes países han fortalecido sus niveles de cooperación con otros países y sus respectivas unidades policiales especializadas y dotadas de medios técnicos necesarios para hacer frente a la delincuencia. Ejemplo de esto es la firma el Convenio sobre Ciberdelincuencia, en Budapest el 23 de noviembre de 2001, el cual supone la respuesta a la necesidad de tener medios eficaces de cooperación para la lucha contra la cibercriminalidad. (Rayón Ballesteros & Gómez Hernández, 2014)

En este convenio, se hace referencia a la necesidad de prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes, datos informáticos y datos personales, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación de estos como delitos y facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional (Consejo de Europa, 2001), agrupándolos de acuerdo a la Tabla 7.

Tabla 7. Delitos establecidos en el Convenio de Ciberdelincuencia. Fuente: elaboración propia a partir de la información extraída del Convenio de Budapest (Consejo de Europa, 2001)

Clasificación de los delitos	Delitos asociados	Artículos
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	- Acceso ilícito - Interceptación ilícita - Ataque a la integridad de los datos - Ataques a la integridad del sistema - Abuso de los dispositivos	2 al 6
Delitos Informáticos	- Falsificación informática - Fraude informático	7 al 8
Delitos relacionados con el contenido	- Delitos relacionados con la pornografía infantil.	9
Delitos relacionados con infracciones de la propiedad intelectual y de los delitos afines	- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	10

Con respecto a Colombia este convenio fue aprobado mediante la Ley 1928 de 2018 "Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest" pero aún se encuentra en proceso de aprobación el proyecto de ley para implementarlo.

En la actualidad, Colombia cuenta con la Ley 1273 de 2009 que modificó el Código Penal y creó un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y estableció la preservación de los sistemas que utilicen las tecnologías de la información y las comunicaciones (Congreso de la República, 2009), lo que originó que se tipificaran los delitos que se relacionan en la Tabla 8.

Tabla 8. Delitos Informáticos en Colombia. Fuente: elaboración propia a partir de la información abstraída de la Ley 1273 Congreso de la República, (2009)

Clasificación de los delitos	Delitos asociados	Artículos
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	- Acceso abusivo a un sistema informático. - Obstaculización ilegítima de sistema informático o red de telecomunicación. - Interceptación de datos informáticos. - Daño Informático. - Uso de software malicioso. - Violación de datos personales - Suplantación de sitios web para capturar datos personales	269A 269B 269C 269D 269E 269F 269G
De los atentados informáticos y otras infracciones	- Hurto por medios informáticos y semejantes - Transferencia no consentida de activos	269I 269J

De esta forma, la ley 1273 identifica como delitos informáticos aquellos en los que el nexo común alrededor del cual se producen es un ordenador o un dispositivo electrónico con conexión a Internet, bien porque el objeto sobre el que recae la conducta es el propio sistema, el programa

informático o el equipo, bien porque ese sistema es utilizado como medio a través del cual se realiza la conducta delictiva o bien porque el bien jurídico protegido es la integridad de la información, la confidencialidad de la misma o los datos y los sistemas o programas informáticos.

Finalmente, en relación con Colombia la Cámara Colombiana de Informática y Telecomunicaciones en su informe "Tendencias Cibercrimen Colombia 2019 – 2020", describe que las dinámicas del cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a la Policía Nacional con 30.410 casos durante el 2019 (Cámara Colombiana de Informática y Telecomunicaciones & Policía Nacional de Colombia, 2019). Así mismos, del total de casos registrados, 17.531 fueron denunciados por infracción a la Ley 1273 de 2009, equivalente a un 57%. En la Figura 7, se puede observar el crecimiento del cibercrimen durante los últimos años.

Figura 7. Estadística de crecimiento cibercrimen en Colombia por año. Fuente: Cámara Colombiana de Informática y Telecomunicaciones & Policía Nacional de Colombia, (2019)

Frente a los delitos informáticos más denunciado se encuentra el "Hurto por medios informáticos" con un total de 31.058 casos, al parecer porque los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca. En segundo lugar, se encuentra la "Violación de datos personales" con 8.037 casos. El tercer delito más denunciado es el "Acceso abusivo a sistema

informático" con 7.994 casos, y esto se explica en razón a que, en las fases primarias de los Ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos. En cuarto lugar, con 3.425 casos se encuentra la "Transferencia no consentida de activos", conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas. Finalmente, en quinto lugar se sitúa el delito de Uso de Software Malicioso con 2.387 casos (Cámara Colombiana de Informática y Telecomunicaciones & Policía Nacional de Colombia, 2019).

Frente a otras tendencias relacionadas con el cibercrimen, en el la Tabla 9 se describen las relacionadas en el informe realizado por Cámara Colombiana de Informática y Telecomunicaciones y la Policía Nacional de Colombia (2019).

Tabla 9. Tendencias en cibercrimen Colombia 2019 – 2020. Fuente: elaboración propia a partir de la información consignada en el informe "Tendencias Cibercrimen Colombia 2019 – 2020" (2019)

Tendencia	Descripción
Ataque BEC	Los cibercriminales diseñan escenarios simulados para engañar a empleados clave suplantando a ejecutivos, con el fin de que realicen acciones no autorizadas que conllevan a defraudar a las empresas o consiguen suplantar a sus clientes y proveedores mediante el robo de identidad basado en ingeniería social. Los principales vectores de engaño en 2019 fueron: - 80%: Correos Fraudulentos Personalizados (Spear fishing). - 60%: Suplantación de identidad 60. - 53%: Enmascaramiento de correos (Spoofing). - 37% Infección de sitios frecuentemente visitados por empleados (watering hole).
Rasomware	Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú (16%), México (14%), Brasil (11%) y Argentina (9%). Las PYMES fueron el blanco preferido por los atacantes, ya que conocen que los niveles de seguridad suelen ser más bajos en este tipo de compañías. - 717 empresas reportaron ataque por ransomware.

Tendencia	Descripción
Ataque DDoS	Según cifras del Centro Cibernético Policial, 170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes.
Malware	La infección por malware sigue en crecimiento, pasando de 99 casos de empresas que reportaron infección de malware en su infraestructura en el año 2018 a más de 705 casos registrados durante el año 2019. Siendo las PYMES las más afectadas por estos ataques. Los métodos de dispersión de malware son: - 63%: Correos con notificaciones suplantando entidades públicas. - 32%: Redireccionamiento hacia sitios web infectados por el atacante. - 5%: Descarga de aplicaciones maliciosas.
Sim Swapping	Según datos de la Comisión Federal de Comercio de los EE.UU FTC por sus siglas en inglés (Federal Trade Commission), los casos reportados por robo de identidad para la obtención de SIMCARD ante operadores de telefonía celular representan actualmente 9,8% del total de casos reportados en 2018. - 99: celulares son reportados como robados en Colombia cada hora. - 30%: hurto de celulares en Colombia durante el 2019.
Cryptojacking	Un ataque de cryptojacking tiene como objetivo generar criptomonedas por medio de comandos computacionales de un tercero. - 56 millones de dólares es el estimado percibido por la criptominería ilegal. - 33.000 sitios web Se calcula que están infectados.

Por otra parte, es importante mencionar que han surgido otros tipos de fenómenos que también deben ser considerados como amenazas a la ciberseguridad de las personas, pero que no son catalogados como cibercrimen, por ejemplo, las campañas de desinformación que se generan en el ciberespacio, que consisten en estrategias de comunicación global en las cuales mediante la de creación de aplicaciones, sitios web o plataformas gubernamentales oficiales para la publicación de contenido, el uso de cuentas reales, falsas o automatizadas para interactuar con los usuarios en las redes sociales, o creación de contenido sustantivo como imágenes, videos o publicaciones de blog (Bradshaw & Howard, 2017), buscan difundir propaganda en favor o en contra del gobierno, atacar a la oposición o montar campañas de desprestigio, conversaciones distractoras o críticas

para alejar los temas importantes, generar división y polarización y reprimir la participación a través de ataques personales o acoso (Bradshaw & Howard, 2019), logrando con esto desestabilizar el orden social de un país.

4. Inteligencia

La Real Academia Española define la inteligencia como la capacidad de entender o comprender y resolver problemas, así como el propio conocimiento, comprensión o acto de entender (2014). Esta inteligencia, en un primer acercamiento al término, perseguiría la obtención de datos que una vez procesados se convierten en información y esta, tras su entendimiento o comprensión, deriva en conocimiento que será utilizado para la prevención y resolución de problemas y el proceso de toma de decisiones (Hilsman, 1952).

Sherman Kent (1986) como el autor de los primeros trabajos de inteligencia, en su texto titulado "Inteligencia estratégica para la política mundial norteamericana", la define desde tres perspectivas diferentes, como proceso o actividad, organización y producto:

1. Proceso o actividad: comprende los procedimientos y medios que se utilizan para definir las necesidades de los decisores, establecer la búsqueda de información, su obtención, valoración, análisis, integración e interpretación hasta convertirla en inteligencia, y su difusión a los usuarios. También incluye los mecanismos y medidas de protección del proceso y de la inteligencia creada por medio de las actividades de contrainteligencia necesarias (Kent, 1986).
2. Organización: se refiere a los organismos y unidades que realizan las actividades de

transformación de la información en inteligencia y la protegen (Kent, 1986).

3. Producto: plantea que es el resultado que se obtiene al someter los datos, la información y el conocimiento a un proceso intelectual que los convierte en informes adecuados para satisfacer las necesidades de los decisores políticos, militares, policiales, empresariales, etc., (Kent, 1986).

Así mismo Kent, aproxima al concepto de inteligencia como componente de la seguridad nacional desarrollando en varias esferas: en función del nivel de decisión (nacional, departamental u operativa), la finalidad (estratégica, táctica, operativa o prospectiva), la necesidad (básica o general, actual o crítica), el origen y el método de obtención, el territorio sobre el que se elabora la información en atención a las materias o campos de conocimiento (geográfica, política, sociológica, militar, de objetivos, científico tecnológica, económica, criminal, holística, sociocultural, etc.) (Kent, 1986).

Por su parte, Mark Lowenthal (2012), considera que la inteligencia es una parte más de maquinaria de ayuda al proceso de toma de decisiones de la información y es un proceso por el cual tipos específicos de información importante para la seguridad nacional son requeridos, recolectados, analizados y distribuidos a los políticos; igualmente dice que se trata de una actividad esencialmente estatal que se inicia con el secreto de información para la preservación de su seguridad tanto interna como externa, muchas veces vinculada con la doctrina de seguridad nacional.

Así mimo, el Estado Mayor Conjunto de los Estados Unidos en su publicación Joint Intelligence 2.0 (2013), plantea que la inteligencia es el producto resultante de la recopilación,

procesamiento, integración, evaluación, análisis e interpretación de la información disponible sobre naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles, o áreas de operaciones reales o potenciales, siendo esta definición similar a la establecida por Kent en relación a la inteligencia como producto. Igualmente, dice que la finalidad de la inteligencia es anticipar o predecir situaciones y circunstancias futuras, e informa las decisiones al iluminar las diferencias en los cursos de acción disponibles (Joint Chiefs of Staff, 2013).

Por otra parte, en el contexto colombiano la Ley 1621 de 2013 define la función de inteligencia y contrainteligencia, como:

> *"aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta Ley." (Congreso de la República, 2013, p. 1)*

Esta definición, permite especificar que la actividad de inteligencia es ejercida por organismos especializados y establece funciones específicas que la diferencian de otras competencias estatales, que para el caso de Colombia de acuerdo con la Ley 1621 de 2013, los únicos organismos que llevan a cabo la función de inteligencia y contrainteligencia son las dependencias de las Fuerzas Militares y la Policía Nacional organizadas por estas para tal fin, la

Unidad de Información y Análisis Financiero (UIAF), y por los demás organismos que faculte para ello la ley, siendo estos a su vez los organismos que conforman la comunidad de inteligencia (Congreso de la República, 2013).

Aunado a lo anterior, es importante mencionar la diferencia que el marco constitucional y legal realiza entre la función de inteligencia y contrainteligencia y aquella desarrollada por Investigación Criminal, teniendo en cuenta que esta última es definida por la Corte Constitucional como "la sucesión de actos que se despliegan con el fin de recaudar los elementos de convicción requeridos para que, en el juicio, el juez de conocimiento someta a valoración las pruebas y determine, en su neutralidad, el grado de responsabilidad del procesado" (Corte Constitucional, 2005, p.13)

En esta medida, la investigación criminal pretende recaudar pruebas y establecer los responsables de una conducta delictual que se desenvolverá en el marco de un proceso penal, en tanto, la función de inteligencia y contrainteligencia se desarrolla por organismos especializados del Estado del orden nacional, empleando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con la finalidad de proteger los derechos humanos, anticipar, prevenir y combatir amenazas internas o externas contra la seguridad y defensa nacional, vigencia del régimen democrático, y otros fines (Corte Constitucional, 2012).

Por otra parte y continuando con la contextualización de inteligencia, Loubet (1992) bajo el contexto policial y con fundamento en la doctrina francesa, señala la necesidad de que los cuerpos de policía dispongan de una fuente de información, a partir de la cual se tramiten al sistema

político (democrático), las demandas y los apoyos ciudadanos, según se distingan los grupos sociales en los que corresponde al cuerpo de policía preservar el orden social.

Aunado a lo anterior, la Policía Nacional de Colombia, enmarca en su doctrina el término "Inteligencia Policial", estableciendo que su finalidad es producir conocimiento especializado para anticipar y prevenir situaciones y fenómenos en los ámbitos ambiental, económico, político y social y de seguridad pública, coadyuvando al cumplimiento de la misionalidad institucional en el marco de la conveniencia de los habitantes de Colombia (Policía Nacional de Colombia, 2014) y la define como:

> *"el resultado de la búsqueda, recolección, tratamiento y análisis de la información correlacionada con el conocimiento disponible, de inmediata o potencial importancia para mantener la seguridad pública, contribuir en la definición de políticas y directrices de las administraciones públicas en todas sus esferas, diseñar estrategias institucionales, orientarla ejecución de planes y operaciones en cumplimiento de la misión policial y prevenir y contrarrestar la acción delincuencial en sus diferentes modalidades"* (Policía Nacional de Colombia, 2014, p. 20).

Así mismo, la inteligencia policial enmarca todo un proceso constructivista que comprende la articulación de capacidades humanas, tecnológicas y gerenciales, sobre un efectivo sistema de administración de la información y bajo un enfoque tridimensional como lo contempla Sherman Kent en su visón y concepto de inteligencia organizacional que comprende la estructura, el conocimiento y los procesos (Kent, 1986).

5. Disciplinas de inteligencia

En la relección de información se evidencian diferentes métodos utilizados para obtener los datos y la información, los cuales de acuerdo Rafael Jiménez (2018) se pueden clasificar según el método utilizado para su adquisición y según el medio en que se encuentra, como se muestra en la Tabla 10.

Tabla 10. Clases de procedimientos de Obtención de Información según el método utilizado para su adquisición. Fuente: Jimenez, (2018)

SEGÚN EL MÉTODO DE OBTENCIÓN	SEGÚN EL MEDIO EN EL QUE SE ENCUENTRA LA INFORMACIÓN
HUMINT (Clásicos humanos)	**HUMINT** (En poder de personas)
	OSINT* (En fuentes abiertas)
SIGINT (Por o a través de señales y transmisiones de cualquier clase) ❑ **COMINT** (Comunicaciones) • **CLÁSICAS** • **CYBINT** (A través del ciberespacio) • **TEMPEST** (De emanaciones no intencionadas) ❑ **ELINT** (Electrónicas) ○ **RADINT** (de radares) ○ **TELINT** (De telémetros) ○ **MASINT** (De medición de señales) • **ACINT** (Por o de señales acústicas) • **TELINT** (Por o de señales telemétricas) • **NUCINT** (De radicaciones nucleares)	**SIGINT** (En señales y transmisiones de cualquier clase) ❑ **COMINT** (Comunicaciones) • **CLÁSICAS** • **CYBINT** (En el ciberespacio) • **TEMPEST** (En emanaciones no intencionadas) ❑ **ELINT** (Electrónicos) ○ **RADINT** (En radares) ○ **TELINT** (En telémetros) ○ **MASINT** (En señales de cualquier tipo) • **ACINT** (En señales acústicas) • **TELINT** (En señales telemétricas) • **NUCINT** (En radicaciones nucleares)
IMINT (Por o mediante el análisis de imágenes) ❑ **GEOINT** (Por o de imágenes o info. geoespacial) ❑ **PHOTINT** (Por o de fotografía)	**IMINT** (En imágenes) ❑ **GEOINT** (En imágenes o info. geoespacial) ❑ **PHOTINT** (En fotografías)
TECHINT (SIGINT e IMINT: Por métodos técnicos: químicos, electrónicos, informáticos, radiológicos, etc..)	**TECHINT** (SIGINT e IMINT: Por métodos técnicos: químicos, electrónicos, informáticos, radiológicos, etc..)
*** El tipo de información OSINT pude obtenerse por métodos HUMINT, SIGNINT o IMINT, o por varios de ellos simultáneamente.**	

6. Ciclo de Inteligencia

En los últimos años, los campos de intervención ligados a la defensa nacional, la seguridad, las políticas preventivas de riesgos naturales y humanos han sido testigos de la difusión de estudios y debates en torno a la especificidad de la inteligencia mediante distintos acercamientos teóricos y

metodológicos (Velasco et al., 2010), entre los cuales se encuentra el llamado "ciclo de inteligencia", con el cual a partir de la aplicación de un conjunto de actividades de naturaleza intelectual permite el paso de la información al conocimiento (Navarro, 2004).

Para comprender mejor la definición de ciclo de inteligencia, es necesario identificar la diferencia entre dato, información e inteligencia, que para este caso presenta el Estado Mayor Conjunto de los Estados Unidos en su publicación Joint Intelligence 2.0 (2013), en donde describen que los datos sin procesar en sí mismos tienen una utilidad relativamente limitada, sin embargo, cuando los datos se recopilan y se procesan en una forma inteligible, se convierten en información y adquieren una mayor utilidad; asimismo la información por sí sola puede ser de utilidad para el mando institucional, pero cuando se relaciona con otra información y se considera a la luz de la experiencia pasada, da lugar a una nueva comprensión de la información, como se observa en la Figura 8.

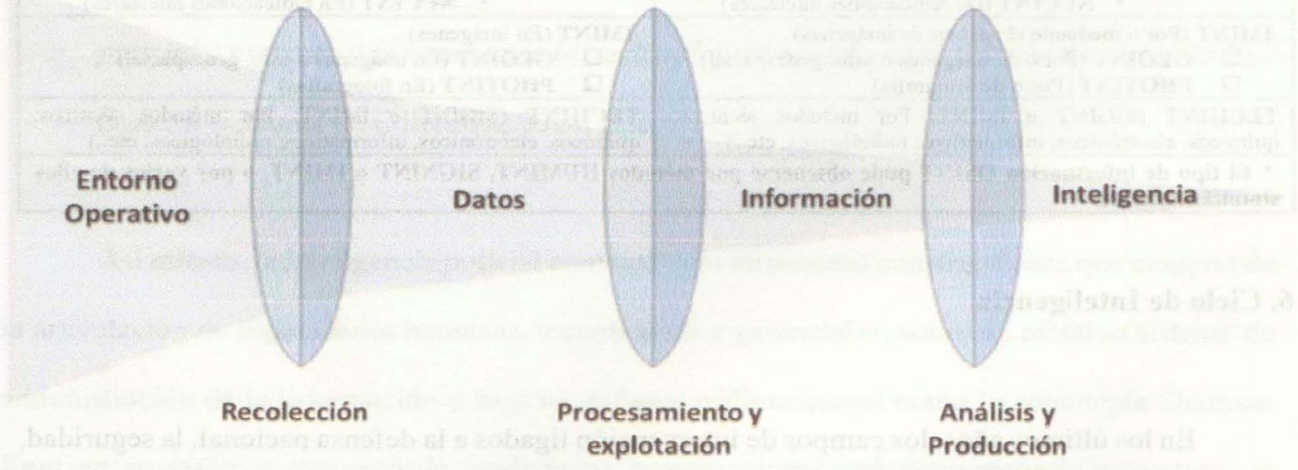


Figura 8. Relación entre dato, información e inteligencia. Fuente: Joint Chiefs of Staff, (2013)

De acuerdo con lo anterior, la inteligencia puede ser comprendida a través de una serie de pasos que conforman un ciclo, el cual tiene como principales características la recolección de información (datos), su posterior procesamiento y análisis, seguido luego de la entrega de la misma a aquellas instituciones y/o personas que son las llamadas a establecer las diferentes decisiones en torno a un eventual problema, o en su defecto generar las soluciones pertinentes, para finalmente generar el adecuado proceso de retroalimentación (Navarro, 2004).

Lo anterior se ve apoyado por Cepik y Antunes (2004), quienes dicen que el ciclo de inteligencia se trata de un conjunto de métodos y técnicas orientadas hacia la recolección, análisis y producción de conocimiento para la toma de decisiones. Por su parte, Lowenthal (1992) dice que la definición del "Ciclo de Inteligencia" plantea en realidad una serie de relaciones con el ciclo informativo/comunicativo general, así como el papel jugado por la cadena documental en la generación de Inteligencia.

Del mismo modo, Sainz de la peña (2012) define el ciclo de inteligencia como la secuencia de actividades por la que se obtienen y procesa información para convertirlas en inteligencia y a su vez esta se pone a disposición de los que la necesitan, concluyendo que el ciclo es un modelo único que se adapta a cada situación particular y que a su vez, sus elementos básicos vinculan a un peticionario/usuario de conocimiento especializado (Inteligencia) a quien se le debe satisfacer sus requerimientos específicos de inteligencia aplicando un método concreto. Estos requerimientos de conocimiento expresan la voluntad y la necesidad de aumentar la carga informativa procesada sobre un tema concreto con el objeto de fundamentar la toma de decisiones (Navarro, 2004).

Por su parte, otros autores sitúan el proceso de producción de inteligencia como el resultado de la adaptación del método científico a la generación de inteligencia realizado por parte de los servicios de inteligencia en el segundo tercio del siglo XX con objeto de ordenar racionalmente su trabajo (Herman, 1996, p. 286) y cuyo desarrollo se encuentra, además, fuertemente influido por los avances técnicos y tecnológicos, sobre todo en el ámbito de la información, iniciados a finales del siglo XIX y que llegan hasta nuestros días.

De igual forma, Navarro (2004) define el Ciclo de Inteligencia *como "un conjunto de actividades de naturaleza intelectual (que) determina taxativamente el paso de la información al conocimiento"* (p. 51), al tiempo que señala el mismo autor, en una perspectiva más general, que la mayor parte de los servicios de Inteligencia a nivel mundial, definen el Ciclo como:

> *"Una serie de cinco pasos orientados a la generación de conocimiento estratégico útil, verdadero y ajustado a los requerimientos de información preestablecidos por un destinatario final (decidor), a quien se difunde selectivamente el resultado final plasmado en un instrumento determinado" (Navarro, 2004, p. 55).*

Otra definición emitida por Navarro pero en conjunto con Velasco (2009) es que el ciclo de inteligencia es una serie de fases sistematizadas mediante las cuales se desarrolla el trabajo intelectual de generación de nuevo conocimientos, útiles, veraces y ajustados a los requerimientos de inteligencia, que a su vez son delimitados previamente por un usuario o destinatario final.

Por lo anterior, se dice que el Ciclo de Inteligencia puede dividirse para una adecuada

comprensión, en diferentes fases, que se encuentran interconectadas en una secuencia lógica. Pero sin perjuicio de la anterior definición donde se establecen cinco pasos, estos deben ser adoptados como la parte básica y esencial del Ciclo, considerando la ampliación de este para la obtención de un mejor resultado de Inteligencia (Holzmann & Gallardo, 1997).

No obstante, la tipificación de determinadas etapas básicas dentro del ciclo tiene como principal finalidad otorgar las diferentes etapas que constituyen el denominado Ciclo, en un ordenamiento lógico y apto para una correcta comprensión y funcionamiento del mismo, son: a) planificación y dirección; b), obtención de la información; c), proceso; d), análisis y generación de inteligencia; y e), difusión (Navarro, 2004).

En complemento a lo anterior, Sainz de la Peña (2012) dice que las actividades del ciclo se suelen clasificar en cuatro "fases": dirección, obtención, elaboración y difusión y que en algunos ejércitos, la fase de Dirección se divide en dos, una de Planificación y otra de Dirección propiamente dicha. Cabe anotar que las actividades se denominan Ciclo por su carácter de revisión y actualización constante. Una información nueva puede provocar un cambio en el análisis de la situación lo que, a su vez, origina una nueva necesidad de inteligencia.

Por otra parte, otros autores argumentan que el proceso de inteligencia requiere el uso de la aplicación de un modelo que permita tratar la información eficientemente para aportar un conocimiento veraz y exacto al usuario final. Generalmente se admite que este proceso está constituido por las siguientes fases (Cline et al., 1989):

- Planteamiento. Determinación de las necesidades de inteligencia.
- Obtención de información.
- Elaboración.
- Difusión de inteligencia.

7. Ciclos de inteligencia implementados en otras entidades

El "ciclo de inteligencia" permite representar la inteligencia como proceso de acuerdo con lo expuesto por Sherman Kent (1986), aunque este puede tener variaciones en algunos pasos o aspectos dependiendo de la organización que lo implemente.

A continuación se hará una revisión de algunos ciclos de inteligencia, extractados de instituciones de carácter gubernamental que cumplen una función ya sea de seguridad o defensa nacional, similar a la Policial Nacional, lo cual permitirá verificar las diferentes fases que lo conforman y como varían dependiendo de las organizaciones o entidades que lo implementan.

7.1. Agencia Central de Inteligencia – CIA Estado Unidos

En la comunidad de inteligencia norteamericana las fases del ciclo reciben otro nombre, distinguiendo también la fase de obtención de la de procesamiento por lo cual tiene cinco etapas como se muestra en la Figura 9: planeación y dirección, recolección, procesamiento, análisis y producción y diseminación (Agencia Central de Inteligencia, 2013):

Figura 9. Ciclo de Inteligencia de la Agencia Central de Inteligencia. Fuente: elaboración propia a partir la información de la CIA (2013)

En la Tabla 11 se describen cada una de las fases de este ciclo de inteligencia de la Agencia Central de Inteligencia de los Estados Unidos:

Tabla 11. Fases del Ciclo de Inteligencia de la Agencia Central de Inteligencia de los Estados Unidos. Fuente: elaboración propia a partir la información de la CIA (2013)

Fases	Descripción
Planeación y Dirección	Cuando se tiene una tarea relacionada con un trabajo específico, se inicia con la planificación para saber cómo se hará. Se enumera lo que se sabe sobre el problema y lo que se necesita descubrir. Se discuten formas de reunir la inteligencia necesaria.
Recolección	Se recopila información abiertamente y de forma encubierta (secretamente). En esta fase se leen periódicos extranjeros y artículos de revistas, igualmente se escucha la radio extranjera y se ven transmisiones de televisión en el extranjero, estás últimas son ejemplos de fuentes "abiertas". Otras fuentes de información pueden ser "secretas" (o secretas), como la información recopilada con dispositivos de escucha y cámaras ocultas. Incluso se usan tecnologías como la fotografía satelital.
Procesamiento	Se toma toda la información que se ha recopilado y se plasma en un informe de inteligencia. Esta información puede ser desde un documento traducido hasta una descripción de una foto satelital.

Fases	Descripción
Análisis y Producción	Durante este paso, se observa de cerca toda la información y se determina cómo ajustarla, mientras se da respuesta a la tarea original. Igualmente, se evalúa lo que está sucediendo, por qué está sucediendo, qué podría ocurrir después y cómo afecta los intereses de Estados Unidos.
Diseminación	En este paso final, se entrega el análisis final por escrito a un formulador de políticas, el mismo formulador de políticas que inició el ciclo. Después de leer el análisis final y aprender la respuesta a la pregunta original, el formulador de políticas puede regresar con más preguntas. Entonces todo el proceso comienza de nuevo.

7.2. Estado Mayor Conjunto de los Estados Unidos - Joint Chiefs of Staff

Teniendo en cuenta los acontecimientos del 11 de septiembre de 2001, hicieron que las diferentes agencias de inteligencia de Estados Unidos tomaran la decisión de formar la "Joint Intelligence", cuyo fin primordial es unificar la doctrina de inteligencia de cada una de esas agencias, establecer las responsabilidades y niveles que cada uno de los miembros deben adelantar para cumplir con su misión de contrarrestar las amenazas que enfrenta este país (Joint Chiefs of Staff, 2013).

Para este caso, el Estado Mayor Conjunto de los Estados Unidos ha planteado las actividades, ver Figura 10, mediante lo que se denomina "The Joint Intelligence Process", este consta de seis categorías interrelacionadas de operaciones de inteligencia caracterizadas por amplias actividades llevadas a cabo por el personal y las organizaciones de inteligencia las cuales son: planificación y dirección; colección; procesamiento y explotación; análisis y producción; difusión e integración; y evaluación y retroalimentación (Joint Chiefs of Staff, 2013). Los elementos constitutivos del Proceso de Inteligencia Conjunta se listan en la Tabla 12.

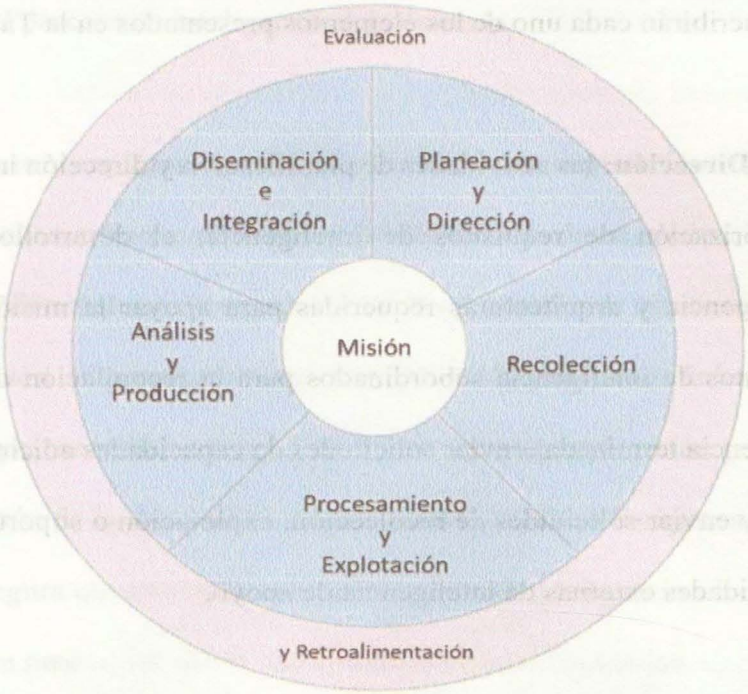


Figura 10. Proceso de Inteligencia Conjunta. Fuente: Joint Chiefs of Staff, (2013)

Tabla 12. Descripción Categorías del Proceso de Inteligencia. Fuente: elaboración propia a partir del análisis de la información expuesta en el documento Joint 2.0. Joint Chiefs of Staff, (2013)

Categorías	Descripción
Planeación y Dirección	Desarrollo de planes de inteligencia y la gestión continua de su ejecución.
Recolección	La recopilación incluye aquellas actividades relacionadas con la adquisición de datos necesarios para satisfacer los requisitos especificados en la estrategia de recopilación.
Procesamiento y explotación	Durante el procesamiento y la explotación, los datos recopilados sin procesar se convierten en formularios que pueden ser fácilmente utilizados por los comandantes, los encargados de tomar decisiones en todos los niveles, los analistas de inteligencia y otros consumidores.
Análisis y producción	Durante el análisis y la producción, la inteligencia se produce a partir de la información recopilada por las capacidades de recopilación asignadas o vinculadas a la fuerza conjunta y del refinamiento y compilación de la inteligencia recibida de unidades subordinadas y organizaciones externas.
Diseminación e integración	Durante la difusión e integración, la inteligencia es entregada y utilizada por el consumidor.
Evaluación y retroalimentación	La evaluación y la retroalimentación ocurren continuamente durante todo el proceso de inteligencia y como una evaluación del proceso de inteligencia como un todo.

A continuación se describirán cada uno de los elementos presentados en la Tabla 12.

Planeación y Dirección: las actividades de planificación y dirección incluyen, entre otras: identificación y priorización de requisitos de inteligencia; el desarrollo de conceptos de operaciones de inteligencia y arquitecturas requeridas para apoyar la misión del comandante; asignación de elementos de inteligencia subordinados para la recopilación de información o la producción de inteligencia terminada; enviar solicitudes de capacidades adicionales a las oficinas centrales superiores; y enviar solicitudes de recolección, explotación o soporte de producción de todas las fuentes a entidades externas de inteligencia de apoyo.

Recolección: los gerentes de recolección desarrollan y coordinan la guía de empleo de sensores, ejercen un control autorizado de operaciones de recolección específicas, revisan las actividades de recolección según sea necesario, monitorean la satisfacción general de los requisitos y evalúan la efectividad del plan de recolección para satisfacer las necesidades de inteligencia originales y en evolución. Los recolectores, ya sea que realicen reconocimiento y vigilancia a través de medios técnicos o humanos, obtienen los datos necesarios para satisfacer los requisitos de información dentro de los requisitos de recolección que se les asignan. Los datos recopilados se distribuyen a través de medios / circuitos adecuadamente clasificados a elementos de procesamiento y explotación. Los gerentes de recolección monitorean continuamente los resultados no solo de la recolección de inteligencia, sino también el procesamiento y la explotación, y el reporte de información para determinar si los requerimientos están siendo satisfechos. Los gerentes de recolección evalúan continuamente la efectividad del plan de recolección para cumplir con los requisitos como parte de la parte de evaluación y

retroalimentación del proceso de inteligencia del comando.

Procesamiento y explotación: el procesamiento y la explotación incluyen la explotación de imágenes de la primera fase, conversión y correlación de datos, traducción de documentos y medios, y descifrado de señales, así como informar los resultados de estas acciones a los elementos de análisis y producción. El procesamiento y la explotación pueden ser federados o realizados por el mismo elemento que recopiló los datos. La planificación de explotación generalmente se realiza durante la planificación de la operación conjunta basada en el rendimiento analítico anticipado de una sola fuente y asegura que la arquitectura de sistemas de inteligencia adecuada esté en su lugar para enrutar datos sin procesar a nodos de explotación predeterminados.

Análisis y producción: toda la información procesada disponible se integra, evalúa, analiza e interpreta para crear productos que satisfagan lo requerimientos del comandante. Los productos de inteligencia se pueden presentar de muchas formas. La producción de inteligencia para operaciones conjuntas es realizada por unidades y organizaciones. Mientras que la recolección, el procesamiento y la explotación son realizados principalmente por especialistas de una de las principales disciplinas de inteligencia, el análisis y la producción se realizan principalmente por analistas de todas las fuentes que fusionan información de todas las disciplinas de inteligencia. El producto del esfuerzo de fusión multidisciplinar es la inteligencia de todas las fuentes.

Diseminación e integración: la difusión se facilita por una variedad de medios. Los medios están determinados por las necesidades del usuario y las implicaciones y la criticidad de la

inteligencia. Las transferencias de datos personales, en red y de bases de datos son todos medios de difusión. La diversidad de rutas de difusión refuerza la necesidad de comunicaciones e interoperabilidad de sistemas informáticos entre fuerzas conjuntas y multinacionales, comandos de componentes, organizaciones y la comunidad interinstitucional.

Evaluación y retroalimentación: el personal de inteligencia en todos los niveles debe evaluar la ejecución de las tareas de inteligencia que realizan y medir sus impactos. La evaluación y la retroalimentación requieren un diálogo colaborativo entre los planificadores de inteligencia, los gerentes de colección, los coleccionistas, los analistas únicos y de todas las fuentes, y los arquitectos de sistemas de inteligencia para identificar deficiencias en el proceso de inteligencia.

También requiere una consulta con los consumidores de inteligencia para determinar si se cumplen los requisitos de inteligencia. Las aplicaciones inmediatas de evaluación y retroalimentación pueden incluir, entre otras, la reformulación de un requisito de inteligencia para mayor claridad, la reasignación dinámica de un sensor, el redireccionamiento de datos a un nodo de explotación alternativo o la revisión de un informe de información o un Producto de inteligencia terminado. El objetivo de la evaluación y la retroalimentación es identificar los problemas lo antes posible para minimizar las brechas de información y mitigar las deficiencias de capacidad.

7.3. Centro Nacional de Inteligencia - CNI España

El Centro Nacional de Inteligencia CNI como órgano responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones necesarias para prevenir y evitar

cualquier peligro, amenaza o agresión, ha desarrollado un ciclo de inteligencia con el cual, como se observa en la Figura 11, se obtiene información, se transforma en inteligencia y se pone a disposición de los usuarios. Este consta de cuatro fases descritas en la Tabla 13: Dirección, Obtención, Elaboración y Difusión y como característica particular, el proceso busca unificar el modelo de proceso para todas las agencias de seguridad del Estado (Centro Nacional de Inteligencia, 2015).

Figura 11. Ciclo de Inteligencia del Centro Nacional de Inteligencia de España. Fuente: Centro Nacional de Inteligencia, (2015)

Tabla 13. Fases del Ciclo de Inteligencia del Centro Nacional de Inteligencia de España. Fuente: elaboración propia a partir de la información del CNI (Centro Nacional de Inteligencia, 2015)

Fases	Descripción
Dirección	Durante la fase de dirección se determinan las necesidades de inteligencia, se prepara un plan para su obtención, se organizan los medios y se efectúa el mando, coordinación y control de todos ellos. En esta fase cobran especial relevancia las denominadas funciones directivas, que son las siguientes: planificación, organización, motivación, mando, coordinación y control, manteniéndose las cuatro últimas durante el desarrollo de todo el ciclo.

Fases	Descripción
Obtención	En esta fase se realiza la explotación de las fuentes de información por los órganos de obtención y la entrega de esta información al correspondiente equipo de elaboración para la producción de inteligencia.
Elaboración	La elaboración es la fase del Ciclo de Inteligencia en la que se produce la transformación de la información en inteligencia al someterla a un proceso apropiado, mediante la valoración de la pertinencia, oportunidad, fiabilidad y exactitud de las noticias e informaciones recibidas sobre cada una de las actividades seguidas, el análisis de estas, la integración con la inteligencia disponible y la interpretación del conjunto. Esta fase se divide en cuatro sub-fases: - Valoración. - Análisis. - Integración. - Interpretación.
Difusión	Es la fase en la que se efectúa la distribución segura y oportuna de la inteligencia en la forma adecuada y por los medios apropiados a aquellos que la necesitan. La difusión es la fase final del Ciclo de Inteligencia.

7.4. Centro Nacional de Inteligencia – CNI México

El CNI es una institución de inteligencia de México, que tiene como objetivo generar inteligencia orientada a conocer con profundidad todos los aspectos relacionados con los fenómenos que representan amenazas y riesgos a la seguridad nacional; como lo son las posibles manifestaciones de los mismos, su probabilidad de ocurrencia e impacto, las variables que los componen y la relación causal entre las mismas (Centro Nacional de Inteligencia de Mexico, 2020).

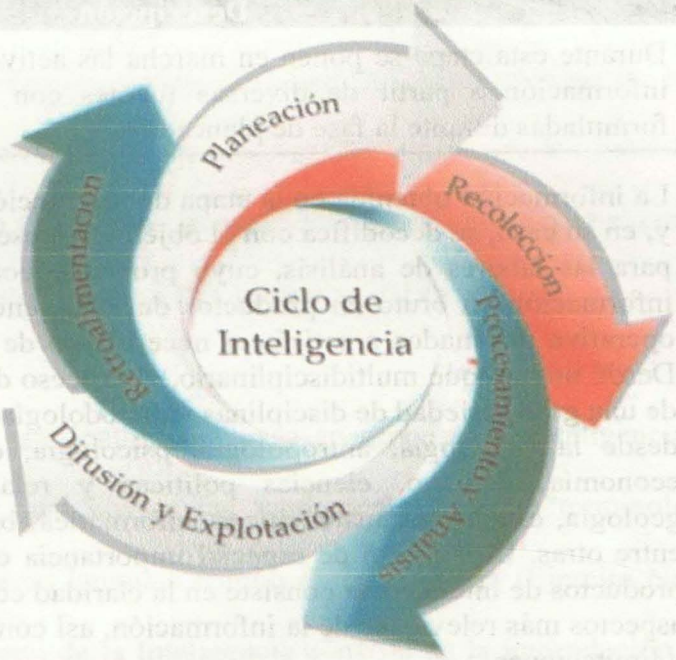


Figura 12. Ciclo de Inteligencia del Centro Nacional de Inteligencia de Mexico. Fuente: Centro Nacional de Inteligencia de Mexico, (2020)

Para esta institución como se observa en la Figura 12, el "ciclo de inteligencia" es el proceso que orienta las acciones de recolección y procesamiento de información con el propósito de integrarlas en productos de inteligencia para los procesos de toma de decisiones. Comprende las etapas descritas en la Tabla 14: Planeación, Recolección, Procesamiento y Análisis; Difusión y Explotación; y Retroalimentación.

Tabla 14. Etapas del Ciclo de Inteligencia del Centro Nacional de Inteligencia de México. Fuente: elaboración propia a partir de la información del CNI (Centro Nacional de Inteligencia de Mexico, 2020)

Etapas	Descripción
Planeación	Los riesgos y amenazas previstos en la Ley de Seguridad Nacional, así como en la Agenda Nacional de Riesgos y demás instrumentos de política pública en la materia, constituyen el marco de referencia donde se establecen las prioridades de los requerimientos de información de inteligencia, en sus vertientes estratégica, táctica y operativa, los cuales se traducen en planes de recolección que detallan las estrategias a seguir para cada caso.

Etapas	Descripción
Recolección	Durante esta etapa se ponen en marcha las actividades de recolección de información a partir de diversas fuentes con base en las solicitudes formuladas durante la fase de planeación.
Procesamiento y análisis	La información obtenida en la etapa de recolección se depura, estandariza y, en su caso, se decodifica con el objeto de presentarla en un formato útil para las labores de análisis, cuyo propósito consiste en transformar la información en bruto en productos de inteligencia estratégica, táctica u operativa destinados a satisfacer necesidades de información específica. Desde un enfoque multidisciplinario, el proceso de análisis recurre al uso de una gran variedad de disciplinas y metodologías especializadas que van desde la sociología, antropología, psicología, demografía, lingüística, economía, derecho, ciencias políticas y relaciones internacionales, geología, estadística, matemáticas, informática, biología, física, química, entre otras. Un aspecto de especial importancia en la elaboración de los productos de inteligencia consiste en la claridad con la que se exponen los aspectos más relevantes de la información, así como detectar sus alcances y limitaciones.
Difusión y explotación	El carácter confidencial de la información de inteligencia, así como la importancia de remitirla oportunamente a las personas indicadas, hacen que esta etapa sea de especial relevancia. Con el fin de garantizar la seguridad de la información y evitar que caiga en manos equivocadas, los productos de inteligencia son objeto de una serie de procesos y medidas de seguridad con el propósito de evitar riesgos durante su traslado y entrega. Asimismo, durante esta etapa, se pone especial atención en hacer llegar la información con oportunidad a las personas indicadas antes de que sea demasiado tarde para los procesos de toma de decisiones.
Retroalimentación	Un aspecto de gran relevancia para el ciclo de inteligencia consiste en determinar el grado en que la información de inteligencia proporcionada atendió las necesidades de los procesos de toma de decisiones, o, en su caso, si las personas a las que se les entregó la información requieren precisar o ampliar la información sobre un tema en especial. Lo que en consecuencia, inicia las actividades de planeación y a comenzar nuevamente en la primera fase del ciclo de inteligencia.

7.5. Ejército Nacional de Colombia

El Ejército Nacional visualiza este proceso de inteligencia como un modelo que describe y

facilita el entendimiento de la situación, apoyando de esta forma la toma de decisiones. Asimismo, establece que este da un marco común para que los profesionales de la Fuerza guíen sus pensamientos, debates, planes y evaluaciones y genera información, productos y conocimiento sobre el enemigo, el terreno y el clima y las consideraciones civiles para el comandante y el estado mayor/plana mayor. (Ejercito Nacional de Colombia, 2017)

Es de anotar que esta institución, basa su proceso de inteligencia en el "Proceso de Inteligencia Conjunta" el cual provee los fundamentos para la terminología y desarrollo de procedimientos en aras de un lenguaje común de Inteligencia (Ejercito Nacional de Colombia, 2016). Este proceso conjunto de la Inteligencia consiste en la interrelación de seis categorías de las operaciones de inteligencia:

1. Planeamiento y dirección.
2. Recolección.
3. Proceso y explotación.
4. Análisis y producción.
5. Difusión e integración.
6. Evaluación y retroalimentación.

Aunque, debido a las características únicas de las operaciones del Ejército, el proceso de Inteligencia difiere del proceso de inteligencia conjunta (Ejercito Nacional de Colombia, 2016), pero aun así, este cuenta con cada una de las categorías del proceso de este y consta de cinco pasos como se muestra en la Figura 13:

Figura 13. Proceso de Inteligencia del Ejército Nacional. Fuente: Ejercito Nacional de Colombia, (2017)

Los pasos que conforman el proceso de inteligencia del Ejecito Nacional de Colombia se describen la Tabla 15.

Tabla 15. Descripción pasos Proceso de Inteligencia del Ejército Nacional. Fuente: elaboración propia a partir de la información registrada en el Manual Fundamental de Referencia del Ejercito (2017)

Pasos	Descripción
Planeamiento y dirección	Los analistas de inteligencia deben preparar tanto para el comandante como al estado mayor productos de planeamiento detallado que permita la emisión de órdenes y la conducción de operaciones. - Preparación de Inteligencia para el campo de combate. - Planeamiento de requerimientos y análisis de recolección. - Generación de conocimiento (inteligencia). - Comunicación e integración interagencial.
Recolección de información	La recolección se sincroniza para proveer información crítica en momentos claves a lo largo de las fases de una operación y durante la transición de una operación a otra. - Recolección de información. - Operaciones de inteligencia. - Operaciones de seguridad. - Reconocimiento. - Vigilancia.

Pasos	Descripción
Procesamiento	Desarrollo de inteligencia a través del tratamiento de la información recolectada. - Tratamiento de la información recolectada. - Integración de la información. - Facilitar el entendimiento de la situación y la toma de decisiones. - Sincronización del esfuerzo de producción de inteligencia.
Difusión y retroalimentación	Los comandantes deben recibir información de combate e inteligencia en el momento y formato adecuado para facilitar el entendimiento situacional y apoyar la toma de decisiones. - Canales de comando. - Canales de estado mayor. - Canales técnicos.
Análisis y Evaluación	Analizar y evaluar son dos actividades continuas que se desarrollan durante todo el proceso de inteligencia (en cada uno de sus pasos) y le dan forma. Los comandantes de todos los niveles realizan análisis para ayudar a tomar decisiones. Como tal, el análisis se produce en diversas etapas a lo largo del proceso de inteligencia y es esencial para el entendimiento de la situación. Esto permite enmarcar el problema, definirlo y resolverlo. Para efectos específicos de inteligencia, la evaluación, el continuo monitoreo y la evaluación de la situación actual hacen referencia particularmente a las actividades de la amenaza y los cambios en el ambiente operacional. La evaluación de la situación comienza al recibir la misión y continúa durante todo el proceso de inteligencia. Esta permite a los comandantes, al personal y a los líderes asegurar la sincronización de inteligencia.

Finalizada la revisión de los ciclos de inteligencia, se pudo evidenciar que la Dirección Nacional de Inteligencia (DNI) y la Unidad de Información y Análisis Financiero en Colombia, no presenta en sus publicaciones oficiales un modelo de ciclo de inteligencia por lo cual no se tendrán en cuenta en la presente investigación.

7.6. Ciclo de inteligencia en la Policía Nacional de Colombia

Las necesidad de que cada Estado tenga una estructura de inteligencia propia que desarrolle las actividades acordes con sus funciones y que, fundamentalmente, sirva para consolidar cada una

de las fases del Ciclo de la Inteligencia (Navarro, 2004), desde la obtención de información a su análisis crítico, estudio en profundidad y extracción de conclusiones, ha sido entendida por la Policía Nacional de Colombia, y como objeto de la presente investigación, a continuación se hará una contextualización de como este ha sido implementado en la institución a través del tiempo.

Para el ámbito de inteligencia policial, el ciclo de inteligencia ha conservado la esencia del ciclo tradicional que proviene de las esferas militares y de acuerdo con la literatura disponible, cuenta con más de 70 años de creación aproximadamente. La primera conceptualización del ciclo de inteligencia en la Dirección de Inteligencia Policial, como se muestra en la Figura 14, corresponde al primer manual de inteligencia para la Policía Nacional (1992) en el que fue definido como una secuencia de pasos (Dirección, Obtención, Producción y Difusión) universales que transforman información en inteligencia. Este documento sentó las bases de conceptos como la producción de inteligencia y los principios de oportunidad, seguridad, pertinencia y conveniencia en la difusión de información de inteligencia.

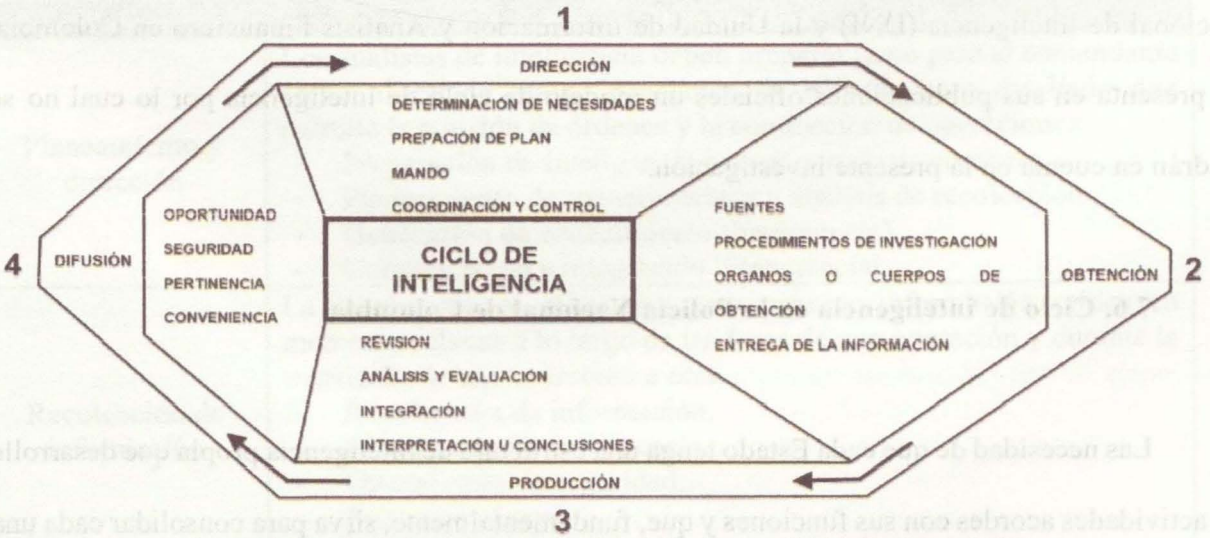


Figura 14. El ciclo de Inteligencia Policial de 1992. Fuente: Policía Nacional, (1992)

En 1999, El documento Reflexiones de Inteligencia No. 5 (Policia Nacional de Colombia, 1999) profundizó sobre el concepto establecido tres años antes, no obstante, expresó los primeros antecedentes de la inclusión de conceptos de administración y gerencia en las actividades misionales de la DIPOL, al incorporar como se observa en la Figura 15, el concepto de planeación en un "ciclo de inteligencia expresado en capacidad", priorizando la actividad de análisis de inteligencia. No obstante, esta modificación tuvo esencialmente un enfoque doctrinal debido a que el acto administrativo del manual no fue modificado.

Figura 15. Ciclo de inteligencia expresado en capacidad. Fuente: Policia Nacional de Colombia, (1999)

Después de 8 años se realizó la primera modificación al Manual de Inteligencia (2005) y consecuentemente a la conceptualización del ciclo. La definición de las fases fue modificada de la siguiente manera:

1. Selección del objetivo,
2. Selección de fuentes,
3. Proceso de la información,
4. Difusión,
5. Formulación de nuevos requerimientos.

Esta nueva visión profundizó en el enfoque gerencial de administración del servicio de inteligencia, y amplió la doctrina referente a la actividad de recolección al examinar conceptos como la administración de fuentes. El proceso de la información formuló el TEA: tratamiento, evaluación y análisis como la metodología de inteligencia policial para elaborar un producto de inteligencia terminado y avanzó en los principios de cada una de estas actividades. La actividad de difusión fue depurada pasando de cuatro principios a tres: pertinencia, oportunidad y seguridad. Esta concepción del ciclo de inteligencia expuesta en la Figura 16, fue la primera en enfocarse en como reiniciar el ciclo al proponer la formulación de nuevos requerimientos de inteligencia.

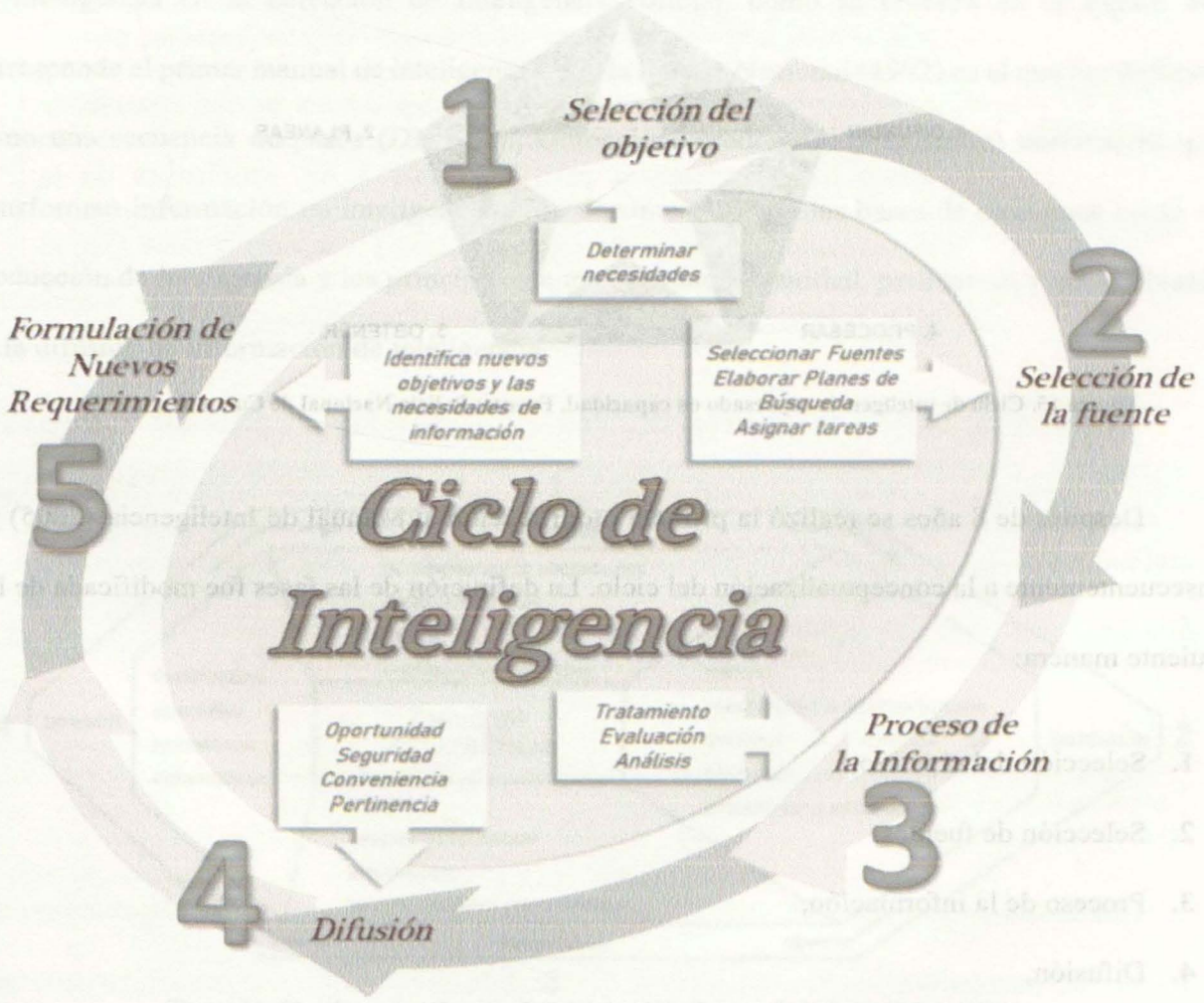


Figura 16. Ciclo de inteligencia Policial 2005. Fuente: Policía Nacional, (2005)

En el marco del 20° aniversario de la Dirección de Inteligencia Policial, luego de la expedición de la ley estatutaria 1621 de 2013[1], se reglamentó un nuevo manual de inteligencia y contrainteligencia para la Dirección de Inteligencia de la Policía Nacional (Policía Nacional de Colombia, 2014). Esto representó una nueva oportunidad para reformular "la metodología para la obtención y procesamiento de la información para la producción de inteligencia y contrainteligencia policial" a través de las siguientes fases expuesta en la Figura 17: Planear y dirigir, Recolectar, Tratar, Analizar, Comunicar e integrar, y Evaluar y retroalimentar, conceptos que habían sido modificados desde el año 2011.

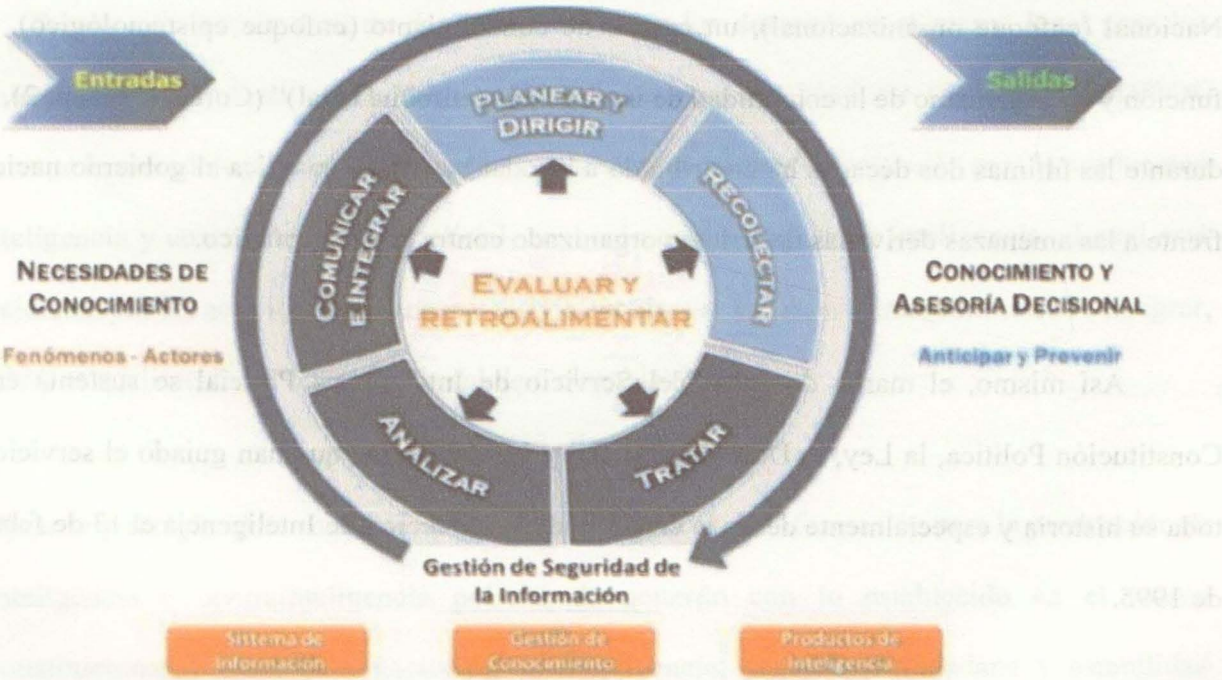


Figura 17. Ciclo de Inteligencia Policial. Fuente: (Policía Nacional de Colombia, 2014)

[1] Ley 1621 del 17 de abril de 2013 "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

Según Cardoso y Rozo (2011), este ciclo transitó de la caracterización de procesos lineales a la descripción en detalle del proceso de inteligencia a través de la "gestión del conocimiento innovador que permitirá la caracterización de los fenómenos y la anticipación del comportamiento futuro de un actor o un fenómeno" (p.8). Esta visión de ciclo respondería a la Ley de Inteligencia y Contrainteligencia, las nuevas políticas de gobierno e institucionales y los requerimientos de la ciudadanía, debido a que fue concebido como un "modelo de inteligencia para la seguridad ciudadana". Este es el ciclo de inteligencia que permanece como la base doctrinal de las actividades de inteligencia y contrainteligencia en la Dirección de Inteligencia Policial al año 2018.

Aunado a lo anterior, la inteligencia policial en Colombia "es una modalidad de la Policía Nacional (enfoque organizacional), un campo de conocimiento (enfoque epistemológico), una función y un organismo de la comunidad de inteligencia (enfoque legal)" (Cortés, 2015, p. 2), que durante las últimas dos décadas ha contribuido a brindar ventaja estratégica al gobierno nacional frente a las amenazas derivadas del crimen organizado contra el orden público.

Así mismo, el marco doctrinal del Servicio de Inteligencia Policial se sustenta en la Constitución Política, la Ley, la Doctrina Policial y los principios que han guiado el servicio en toda su historia y especialmente desde la creación de la Dirección de Inteligencia el 13 de febrero de 1995.

Por otra parte, la doctrina de inteligencia y contrainteligencia policial indica que el procesamiento de la información conduce a la obtención de conocimiento, el cual es empleado para orientar la toma de decisiones en los ámbitos estratégico, operacional y para el Servicio de

Policía, aportando valor significativo a la formulación de estrategias, cuya articulación permite identificar y contrarrestar amenazas a la seguridad pública (Policía Nacional de Colombia, 2014).

Igualmente, a partir de la Ley 1621 de 2013, se define la función de inteligencia y contrainteligencia como aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información (Congreso de la República, 2013), siendo esta definición la primera aproximación al ciclo de inteligencia policial del cual se debe partir, para identificar la estructuración del modelo de ciberinteligencia para la Policía Nacional.

Por lo anterior, en aras de dar cumplimiento a los descrito en el marco legal para los organismos de inteligencia, en el 2014 mediante la resolución 01446 del 16 de abril la DIPOL documenta la metodología para la obtención y procesamiento de la información para la producción de inteligencia y contrainteligencia policial, conocido como el ciclo de inteligencia, el cual está direccionada por las actividades: planear y dirigir, recolectar, tratar, analizar, comunicar e integrar, evaluar y retroalimentar (Policía Nacional de Colombia, 2014), así:

- **Planear y dirigir:** determina las necesidades específicas de información para la producción de inteligencia y contrainteligencia policial de acuerdo con lo establecido en el marco constitucional y legal para garantizar la convivencia, seguridad ciudadana y estabilidad institucional, definiendo objetivos y asignando responsabilidades para el cumplimiento de la misión del Servicio de Inteligencia Policial.

- **Recolectar:** esencialmente se refiere a la recopilación, compendio y obtención de datos sobre personas, organizaciones, objetos y hechos, de acuerdo con las necesidades de información, requeridas para la producción de inteligencia y contrainteligencia policial, a partir del despliegue de actividades específicas que se realizan de manera pública o reservada, acudiendo a medios técnicos o humanos.

La recolección de información requiere de capacitación, calificación y experiencia de los funcionarios que desarrollen esta actividad de inteligencia y contrainteligencia policial, a partir de la aplicación de métodos de obtención y consulta de información, empleando herramientas técnicas y tecnológicas, así como la administración de fuentes humanas.

- **Tratar:** es un procedimiento sistemático que consiste en convertir los datos en insumos disponibles para el análisis de inteligencia y contrainteligencia, a partir de las actividades de organización, clasificación, valoración preliminar y registro.

- **Analizar:** estudio meticuloso, profundo y ordenado de toda la información disponible que responde a los objetivos formulados y a los requerimientos y necesidades de inteligencia y contrainteligencia. Esta actividad implica la distinción y separación de las partes de toda la información, hasta llegar a conocer los principios o elementos de la situación que se presenta.

Tiene como finalidad integrar e interrelacionar la información a partir de la descomposición de los elementos provenientes de las actividades de recolección y tratamiento de información, para llegar a formular hipótesis congruentes con la dinámica y mutación de

los fenómenos que afectan la convivencia y seguridad ciudadana, y así plantear las estrategias más pertinentes para afrontar los problemas de seguridad.

- **Comunicar e integrar:** la actividad de comunicar e integrar, conjuga una serie de acciones que tiene como finalidad difundir información y productos de inteligencia y contrainteligencia al receptor a través de un medio seguro, aportando las herramientas indicadas para el cifrado correspondiente, garantizando la confidencialidad del contenido, el envío oportuno y pertinente.

- **Evaluar y retroalimentar:** esta actividad incorpora la realización de la trazabilidad, medición e impacto de los productos de inteligencia y contrainteligencia, incluyendo actividades de seguimiento, verificación y evaluación de los resultados, considerando desde la planificación del trabajo de inteligencia y contrainteligencia, hasta la toma de las decisiones o la ejecución de las acciones implementadas a partir de los productos de inteligencia y contrainteligencia comunicados.

8. Análisis de los elementos constitutivos del ciclo de inteligencia

Con base a la información presentada en la sección anterior, se puede evidenciar que los diferentes organismos de inteligencia de carácter gubernamental implementan un ciclo de inteligencia, aunque en algunas agencias lo denominan proceso y pueden llamar a sus elementos como fases, pasos, actividades o etapas.

A continuación, en la Tabla 16 se presenta el resumen de los ciclos de inteligencia de los organismos gubernamentales que fueron analizados previamente, con cada uno de los elementos que lo conforman y el nombre que le dan a cada uno de estos:

Tabla 16. Elementos de los ciclos de inteligencia de organismos gubernamentales. Fuente: elaboración propia, (2020)

Organismo de Inteligencia	País	Nombre del ciclo	Nombre de las actividades	Elementos del Ciclo					
Agencia Central de Inteligencia - CIA	Estados Unidos	Ciclo	Fase	Planeación y Dirección	Recolección	Procesamiento	Análisis y Producción	Diseminación	-
Estado Mayor Conjunto de los Estanos Unidos	Estados Unidos	Proceso	Actividad	Planeación y Dirección	Recolección	Procesamiento y explotación	Análisis y Producción	Diseminación e Integración	Evaluación y retroalimentación
Centro Nacional de Inteligencia - CNI	España	Ciclo	Fase	Dirección	Obtención	Elaboración		Difusión	-
Centro Nacional de Inteligencia - CNI	México	Ciclo	Etapas	Planeación	Recolección	Procesamiento y Análisis		Difusión y explotación	Retroalimentación
Ejército Nacional de Colombia	Colombia	Proceso	Pasos	Planeamiento	Recolección de Información	Procesamiento		Difusión y retroalimentación	Análisis y Evaluación

Organismo de Inteligencia	País	Nombre del ciclo	Nombre de las actividades	Elementos del Ciclo					
				Planear y Dirigir	Recolectar	Tratar	Analizar	Comunicar e Integrar	Evaluar y Retroalimentar
Policía Nacional de Colombia	Colombia	Ciclo	Actividades						

Así mismo, al revisar los elementos que conforman los diferentes ciclos de inteligencia se identificaron como se muestra en la Tabla 17, los más significativos, aquellos que a pesar de tener nombres distintos tienen similitudes en su estructura funcional:

Tabla 17. Elementos constitutivos del ciclo de inteligencia. Fuente: elaboración propia, (2020)

Organismo de Inteligencia	Elementos Constitutivos del Ciclo de Inteligencia						
	Planeación	Recolección	Procesamiento	Análisis	Diseminación	Evaluación	Retroalimentación
Agencia Central de Inteligencia -CIA	X	X	X	X	X		
Estado Mayor Conjunto de los Estanos Unidos	X	X	X	X	X	X	X
Centro Nacional de Inteligencia -CNI España	X	X	X	X	X		
Centro Nacional de Inteligencia -CNI México	X	X	X	X	X		X
Ejército Nacional de Colombia	X	X	X	X	X	X	X
Policía Nacional de Colombia	X	X	X	X	X	X	X

Como se puede observar, el análisis se hizo a partir de siete (7) elementos principales: planeación, recolección, procesamiento, análisis, diseminación, evaluación y retroalimentación, los cuales pueden variar su denominación dependiendo del ciclo de inteligencia. Asimismo, se observa que en algunas agencias unifican dos elementos en uno, como es el caso de procesamiento y análisis, o evaluar y retroalimentar, las cuales para el presente análisis se tomaron de forma separada con el fin de detallar las diferencias entre cada uno de los modelos.

A continuación, se analizarán los elementos constitutivos del ciclo de inteligencia:

1. **Planeación:** es un elemento que está presente en todos los ciclos de inteligencia revisados. Consiste en determinar las necesidades y las contingencias que se debe tener en cuenta cuando se esté desarrollando una actividad de inteligencia, en todos los casos se establecen factores económicos, lineamientos legales y gerenciales, distribución de personal, definición del objetivo de la actividad de inteligencia, niveles de seguridad, niveles de acceso a información, medios a utilizar y medidas de cooperación si se requieren.

2. **Recolección**: este elemento está incluido en todos los ciclos de inteligencia de las agencias analizadas. Es conocido también como obtención y consiste en la adquisición y reunión de información, del objetivo planteado en la planeación. Incluye todas las actividades que se dirigen a obtener la materia prima (los datos) que precisan los analistas para satisfacer las necesidades de conocimiento. En este elemento es donde se utilizan las disciplinas de inteligencia como HUMINT, SIGINT, IMINT, OSINT, entre otras.

   Para este elemento, la identificación de fuentes y la selección de los mecanismos

de obtención de información son lo más importante, ya que a partir de esto se da paso al siguiente componente, pero a su vez es el que requiere mayor presupuesto, al necesitar medios especializados para su ejecución.

3. **Procesamiento:** es denominado también elaboración o tratamiento. Para algunas agencias en este elemento está incluido el análisis, aunque para el presente análisis el procesamiento hará referencia al tratamiento que se realiza a los datos para transformarlos en información.

   En este elemento se suelen aplicar las actividades de organización del conocimiento con el fin de preparar la información para su análisis definitivo. Comúnmente se intenta dar respuesta a los siete (7) elementos de la información: ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué? y ¿para qué?, ya que al identificar vacíos de información, se puede solicitar ampliar la recolección y de esta forma dar inicio al análisis.

4. **Análisis:** igual que elemento anterior está presente en todos los ciclos de inteligencia analizados, con la particularidad de que suele ser incluido en el procesamiento o elaboración. Este tiene por objeto, extraer de la información recolectada y tratada todos los datos de interés que respondan a las necesidades de inteligencia, por lo cual requiere que los analistas actúen metódicamente, estudiando en profundidad la información recibida y contrastándola continuamente con la inteligencia que ya poseen en sus archivos.

   Este elemento marca la diferencia entre dato, información e inteligencia, al hacer la integración e interpretación de toda la información recolectada y procesada dándole un

sentido, con lo cual se orientará la toma de decisiones del mando institucional o en su caso se implementarán cursos de acción.

5. **Diseminación:** también conocido como difusión. Este elemento es considerado en algunos ciclos como la fase final, en el cual se hacer llegar de forma oportuna la inteligencia como producto al receptor.

   En esta se consideran e implementan los criterios de seguridad relacionados con la confidencialidad, integridad y disponibilidad de la información, así como la oportunidad y la pertinencia.

6. **Evaluación:** este elemento no está incluido en los ciclos de inteligencia de la CIA y el CNI de México y España, pero para las otras agencias es una fase transversal del ciclo, en la cual se verifican y evalúan los resultados, considerando desde la planificación hasta la toma de decisiones o la ejecución de las acciones a implementar, con el fin de identificar la lecciones aprendidas y buenas prácticas de inteligencia. Este elemento en muchas ocasiones es unificado con la retroalimentación.

7. **Retroalimentación:** este elemento consiste en informar en tiempo real las lecciones aprendidas y debilidades evidencias en la evaluación, con el fin de realizar los ajustes que se requieran y evitar de esta forma fracasos en la obtención de la información o en el asesoramiento del decisor, llevando a que sus actividades sean mucho más contundentes a la hora de tomar decisiones y garantizar la mejora continua y la gestión del conocimiento.

Por otra parte, en algunos ciclos la retroalimentación se encuentra unificada con la evaluación y es transversal a los demás elementos, pero no está incluido en los ciclos de inteligencia de la CIA y el CNI de España

Como se observa en la información anteriormente expuesta, los elementos constitutivos analizados están presente en el ciclo de inteligencia usado por la Policía Nacional de Colombia, lo cual hace posible que sea utilizado como base para la definición del modelo de ciberinteligencia, que se busca diseñar en la presente investigación, aunque deberá ser adaptado a las necesidades del ciberespacio.

Así mismo, se hace necesario revisar al interior de la Policía Nacional las capacidades y componentes que tiene la institución en materia de ciberseguridad y ciberinteligencia que podrían ser incorporados al modelo, aspecto que será abordado en el siguiente capítulo en donde se contextualizará y analizará desde la parte doctrinal y operativa, que actividades se realizan en pro de la ciberseguridad de los ciudadanos en el ciberespacio.

CAPITULO III

IDENTIFICACIÓN DE LAS CAPACIDADES Y COMPONENTES QUE TIENE LA POLICÍA NACIONAL PARA LA CONSTRUCCIÓN DEL MODELO DE CIBERINTELIGENCIA

En el capítulo anterior, como fase inicial de la investigación se analizaron las características teóricas y conceptuales que conlleva un modelo de ciberseguridad y ciberinteligencia en términos específicos y su relación con el ciclo de inteligencia, que permitieron validar la inclusión de este último en el modelo a proponer.

Posterior a esto, en el presente capítulo se procederá a identificar a partir de una revisión doctrinal y operacional las capacidades de la Policía Nacional para garantizar la ciberseguridad de los ciudadanos, de tal forma que se puedan incluir en el ciclo de inteligencia y por ende de modelo de ciberinteligencia, aprovechando de esta forma las capacidades ya existentes en la institución.

1. Contextualización capacidades y componentes de ciberseguridad y ciberinteligencia

> *"Con el objeto de fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia, el Gobierno Nacional mediante el CONPES 3854 de 2016, le asigna a la Policía Nacional la*

responsabilidad de fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos" (Ministerio de Tecnologías de la Información y las Comunicaciones et al., 2016, p. 47).

Por lo anterior, en cumplimiento a la Política de Seguridad Digital, la Policía Nacional a través del Centro Cibernético Policial de la DIJIN, ha venido consolidando las capacidades que le permitirán contribuir en el desarrollo de algunos propósitos que encierra esta política (Policía Nacional de Colombia, 2019), como son:

- Fortalecer las instancias y entidades responsables de ciberseguridad.
- Adecuar el marco jurídico sobre los delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital.
- Socializar y concientizar las tipologías de cibercriminal y ciberdelincuencia a las múltiples partes interesadas.
- Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de una judicialización de delitos cibernéticos y cibercrímenes.

De esta forma y en concordancia con el proceso de modernización y transformación institucional que actualmente adelanta la Policía Nacional, en lo que respecta al robustecimiento tecnológico para la seguridad y convivencia ciudadana, la Institución consideró pertinente ampliar el enfoque de la Estrategia contra los Delitos Informáticos - EINFO, con el fin de dar respuesta a la evolución de los fenómenos, las expresiones de criminalidad y la conflictividad social, permitiendo de esta manera satisfacer las necesidades de los cibernautas en materia de

ciberseguridad (Policía Nacional de Colombia, 2019).

Bajo este direccionamiento, se modificó la nominación de la estrategia EINFO por el de Estrategia Integral de Ciberseguridad ESCIB; esta última, más acorde con el propósito de fortalecer la ciberseguridad de los Individuos y del Estado en el entorno digital a nivel nacional, con un enfoque de gestión de riesgos y bajos componentes fundamentales de prevención, articulación interinstitucional y judicialización (Policía Nacional de Colombia, 2018), a través del desarrollo de las siguientes iniciativas las cuales se plantean en la Directiva Operativa Transitoria No. 38 (2019):

1. Desplegar las capacidades de la Policía Nacional, para contrarrestar los fenómenos que atenúan contra la convivencia ciudadana en el ciberespacio bajo un enfoque de ciberseguridad.
2. Desarrollar las acciones necesarias para alinear la seguridad ciberseguridad como fuente fundamental para la economía digital y el comercio electrónico en Colombia, fomentando el acceso a las tecnologías de la información y las comunicaciones en un entorno seguro.
3. Articular las capacidades del Estado, para realizar las actividades relevantes que contribuya a un desarrollo integral de los Niños, Niñas y Adolescentes de Colombia, estableciendo los mecanismos idóneos de protección en entornos digitales y contribuyendo en la formación de estos.
4. Garantizar la estabilidad del estamento gubernamental e institucional, a través del fortalecimiento de las capacidades de prevención y anticipación frente amenazas informáticas.
5. Actualizar los mecanismos y capacidades de la Policía Nacional para el conocimiento y

acercamiento y satisfacción del ciudadano como víctima del cibercrimen, logrando el esclarecimiento de los actos delictivos para contribuir con la consecución de una paz estable y duradera.

6. Desarrollar acciones de impacto que contribuyan a la prevención del ciberdelito y a la educación ciudadana y de los entes de Policía y gubernamentales para la consolidación de una cultura de ciberseguridad.
7. Fortalecer la alianza de cooperación policial con agencias y entidades internacionales para una articulación efectiva en el cumplimiento de objetivos estatales en la fomentación de las Tecnología de la información y las comunicaciones TIC's.

Esta estrategia cuenta con tres dimensiones como se muestra en la Figura 18: Participación Internacional, Articulación Interinstitucional y Articulación de capacidades C4.

Figura 18. Dimensiones de la Estrategia Integral de Ciberseguridad - ESCIB. Fuente: elaboración propia a partir de la información descrita en la Directiva Administrativa Transitoria No. 38 (Policía Nacional de Colombia, 2019) y el Modelo de Planeación y Gestión Operacional del Servicio de Policía (Policía Nacional de Colombia, 2018)

Para presentar con un poco más de detalle las dimensiones, podemos decir que la de "Participación Internacional", hace referencia a los mecanismos de cooperación de la Policía Nacional con homólogos en otros países y agencias de ley a nivel mundial, tales como: la Organización Internacional de Policía Criminal (INTERPOL), la Oficina Federal de Investigaciones de los Estados Unidos (FBI), la Administración para el Control de Drogas de los Estados Unidos (DEA), el Centro Europeo Contra el cibercrimen (EC3), la Comunidad de Policías de América (AMERIPOL), la Agencia Internacional de Cooperación Coreana (KOICA), la Agencia Nacional contra el crimen del Reino Unido (NCA), el Grupo de Trabajo Americano de delitos Tecnológicos del INTERPOL (GLDTA) y el Programa de Asistencia Antiterrorismo de Estados Unidos (ATA). Esto, con el fin de combatir el cibercrimen desde diferentes blancos (CONPES 3854, 2016, p. 16)

Por su parte, la dimensión de "*Articulación Institucional*" plantea la cooperación con entidades de sector público y Sector Privado de carácter nacional, como el Comando Conjunto Cibernético, la Fiscalía General de Nación, el Ministerio de Tecnologías de la Información y Comunicaciones, CSIRT Gobierno, bancos, proveedores de servicios TICs, comercio electrónico, entre otras.

Finalmente, la tercera dimensión "Articulación de capacidades C4" define la articulación de capacidades internas con las que cuenta la Policía Nacional, entre las que destaca el Centro de Capacidades para la Ciberseguridad de Colombia – C4, el CSIRT PONAL liderado por la Oficina de Telemática de la Dirección General, y demás unidades. Por otra parte, la Estrategia Integral de Ciberseguridad define también como se observa en la Figura 19, tres componentes para su

despliegue (Policía Nacional de Colombia, 2019):

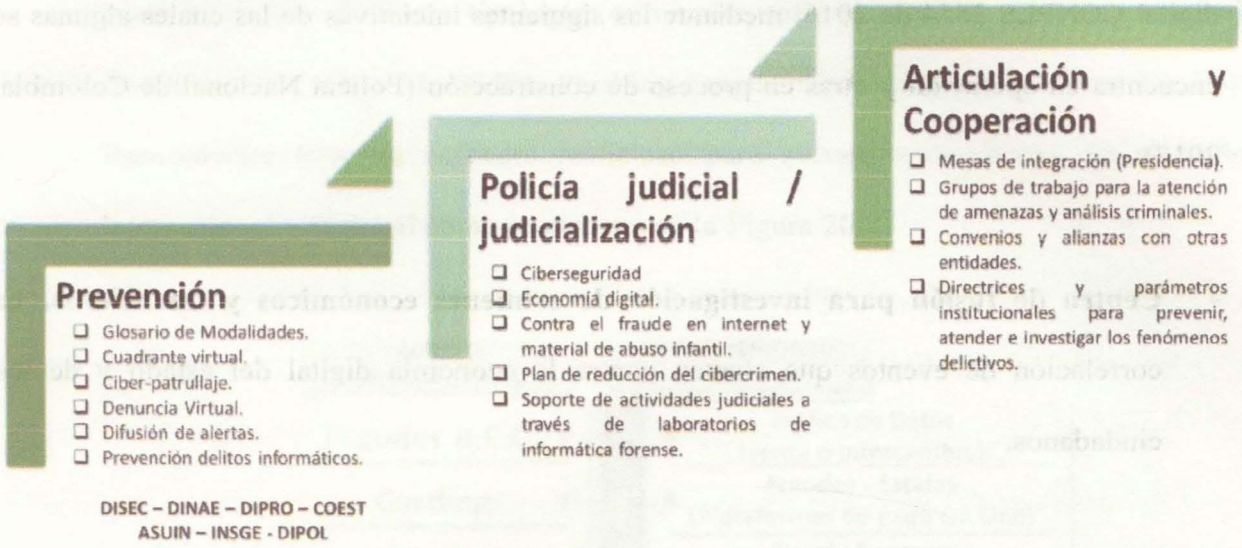


Figura 19. Componentes de la ESCIB. Fuente: elaboración propia a partir de la información descrita en la Directiva Administrativa Transitoria No. 38 (Policía Nacional de Colombia, 2019)

1. **Prevención:** en este componente de la estrategia, se identifican las modalidades del cibercrimen, se definen cuadrantes virtuales, se realiza análisis de fuentes abiertas y ciber-patrullajes 24/7, se implementan el sistema de gestión de incidentes y la plataforma para las denuncias virtuales, se generan difusión de alertas para la prevención de delitos informáticos e informes de cibercrimen y se definen las líneas de trabajo para las Direcciones y Oficinas de la Policía Nacional, que de acuerdo a su misionalidad pueden aportar a la prevención, para este caso, designa a la Dirección de Seguridad Ciudadana (DISEC), la Dirección de Inteligencia Policial (DIPOL), la Dirección Nacional de Escuelas (DINAE), la Dirección de Protección y Servicios Especiales (DIPRO), la Oficina de Comunicaciones Estratégicas (COEST), la Oficina de Asuntos Internacionales (ASUIN) y la Inspección General (INSGE).

Al interior de este componente, se contempla el fortalecimiento de las capacidades del Centro Cibernético Policial, alineando estos esfuerzos con la política pública de seguridad digital CONPES 3854 de 2016, mediante las siguientes iniciativas de las cuales algunas se encuentra en operación y otras en proceso de construcción (Policía Nacional de Colombia, 2018):

- **Centro de fusión para investigación de crímenes económicos y financieros.** La correlación de eventos que atenten contra la economía digital del estado y de los ciudadanos.

- **Centro de Capacidades para la Ciberseguridad de Colombia C4.** Representa la centralización de todas las capacidades de ciberseguridad de Colombia para contribuir a la ciberseguridad de Colombia y posterior despliegue a nivel nacional.

- **Observatorio de crímenes y delitos en el entorno digital.** Centro de análisis de nuevos comportamientos y tendencias de cibercrimen.

- **Cuadrante Virtual.** Capacidad para fortalecer la interacción estado - policía - comunidad – sector privado, en pro de coadyuvar en materia preventiva y atención de delitos que utilicen el ciberespacio y las tecnologías de información y las comunicaciones para afectar la integridad, vida y patrimonio de terceros.

- **Glosario de Modalidades.** Adopción de conceptos de carácter trasnacional de varias

agencias investigativas, laboratorios de malware y empresas productoras de antivirus quienes han establecido definiciones para asociar las modalidades a través de las cuales materializan las diferentes tipologías criminales, tal es el caso de Smishing (mensajes fraudulentos a través de SMS), Phishing (copia ilegal de páginas online legales) y Ransomware (uso de software malicioso para secuestro de datos), en el ámbito internacional y regional como se muestra en la Figura 20.

Figura 20. Ámbitos de los ciberdelitos - afectación ciudadana. Fuente: (Policía Nacional de Colombia, 2018)

- **Análisis fuentes abiertas / Ciber-patrullaje.** El uso de software especializado que mediante la utilización de etiquetas busca en tiempo real y asincrónico información relevante y conducente para el desarrollo de procesos investigativos, así como para la construcción de medidas de prevención como tal es el caso de pornografía infantil y otros abusos a niños, niñas y adolescentes en internet.

- **Difusión de alertas.** Construcción y divulgación de material gráfico e interactivo que permite alertar a la ciudadanía y sectores estatal y privado sobre la aparición, incidencia, atomización y mutación de amenazas emergentes en el ciberespacio que atentan de

manera directa intereses individuales y colectivos bajo enfoques de cibercrimen y ciberterrorismo.

- **Prevención delitos informáticos.** Política institucional direccionada a la prevención de delitos informáticos que desde y hacia Colombia atenten contra la ciberseguridad. Lo anterior a través de planes focalizados con entes públicos y privados que coadyuvan de manera integral como: fraude bancario (INCOCREDITO), criptodivisas (ASOBANCARIA) y pornografía infantil (ICBF), entre otros.

- **Informes de Cibercrimen.** Presentación del estado del arte del cibercrimen, a través de la caracterización de mismo que permite contextualizar sobre tipologías, modalidades, técnicas, amenazas, puntos de concentración, zonas de injerencia que atentan contra la seguridad de la información y los activos de la nación uy del sector privado.

- **Unificación de procedimientos.** A través de la contextualización de información en mesas de trabajo con expertos del cibercrimen desde la partes investigativa, pericial y analítica, se definen las líneas de acción que orientan la estandarización.

- **Creación Manual de Doctrina.** Iniciativa para la unificación de todos los elementos históricos y presentes que contribuyan a la desarticulación de organizaciones criminales y a la ciberseguridad.

- **Capacitaciones.** Incrementar el grado de sensibilización y conciencia, socializando las nuevas tendencias de cibercrimen y generando alianzas estratégicas.

- **Mesas de trabajo criptomonedas y fraude en comercio electrónico**. Articulación con entidades como ASOBANCARIA, La Unidad de Información y Análisis Financiero UIAF, INCOCREDITO, pasarelas de pago, la Superintendencia Financiera, para contrarrestar nuevos fenómenos de cibercrimen como los que emplean criptomonedas para fraude, estafas, extorsiones y lavado de activos.

- **Sistema Gestión de incidentes.** Desarrollo tecnológico a la medida que permite la interacción directa entre el ciudadano y la Policía Judicial para la atención de incidentes informáticos, a través del portal web https://caivirtual.policia.gov.co/.

A modo de resumen, como se observa en la Tabla 18 se realizó una clasificación de las iniciativas mencionadas anteriormente por tipo (estratégico, gestión y tecnología) y estado (activa o no activa) el cual hace referencia si está o no en ejecución por parte de algún actor o unidad de la Policía Nacional.

Tabla 18. Clasificación de las iniciativas por tipo y estado. Fuente: elaboración propia a partir de la información descrita en la ESCIB (Policía Nacional de Colombia, 2018)

INICIATIVAS	TIPO DE INICIATIVA			ESTADO	
	Estratégico	Gestión	Tecnología	Activa	No activa
Centro de fusión para investigación de crímenes económicos y financieros		X	X	X	
Centro de Capacidades para la Ciberseguridad de Colombia C4	X	X		X	
Observatorio de crímenes y delitos en el entorno digital		X		X	
Cuadrante Virtual		X	X	X	
Glosario de Modalidades		X		X	
Análisis fuentes abiertas / Ciber-patrullaje		X	X	X	
Difusión de alertas		X		X	

INICIATIVAS	TIPO DE INICIATIVA			ESTADO	
	Estratégico	Gestión	Tecnología	Activa	No activa
Prevención delitos informáticos	X			X	
Informes de Cibercrimen		X		X	
Unificación de procedimientos	X			X	
Creación Manual de Doctrina		X			X
Capacitaciones		X		X	
Mesas de trabajo criptomonedas y fraude en comercio electrónico		X		X	
Sistema Gestión de incidentes		X	X	X	
	21%	**86%**	**29%**	**93%**	**7%**

De lo anterior, se evidencia que de las 14 iniciativas propuestas entorno a la Estrategia Integral de Ciberseguridad, el 93% se encuentran activas, es decir que tienen algún tipo de despliegue y seguimiento y solo la creación del manual de doctrina no está en ejecución, aunque está en proceso de construcción.

Por otra parte, el 20% de las iniciativas presentadas, que equivalen a dos, son de carácter estratégico, sin embargo, se observa que el 86% están enfocadas en la gestión y el 29% al tecnológico, lo cual demuestra que el fortalecimiento de las capacidades de la Policía Nacional de Colombia se está dando en el ámbito de gestión, siendo esto un punto de atención al requerirse generar una nivelación con las capacidades tecnológicas, a partir de la adopción de nuevas tecnologías que permitan la recolección y procesamiento de grandes volúmenes de datos presentes en el ciberespacio.

Finalmente, en relación con el componente estratégico se evidencia que solo el 21% de las iniciativas se orientan hacia este, siendo necesario generar un fortalecimiento de las capacidades estratégicas con las que cuenta la Policía Nacional, teniendo en cuenta que son

las que permiten dar un propósito, intencionalidad y sentido a la arquitectura de negocio de la institución.

2. **Policía Judicial / Judicialización**: este componente es exclusivo de la Dirección de Investigación Criminal e Interpol (DIJIN), siendo el Centro Cibernético Policial como dependencia anexa a esta unidad, la responsable de liderar las actividades de la ESCIB, relacionadas con la ciberseguridad, economía digital, afectación a las estructuras criminales, reducción del delito (Policía Nacional de Colombia, 2018), todo a través de la investigación criminal y policía judicial.

Así mismo, se considera que este componente hace alusión a la parte reactiva de la estrategia, contrario al componente de la prevención que se enfoca en evitar que se presenten incidentes; es decir, el componente de policía judicial opera sobre incidentes informáticos y delitos cibernéticos que se presentan y los cuales afectan la integridad de las personas y la disponibilidad, confidencialidad e integridad de la información, debiéndose ejecutar procesos investigativos y operaciones de carácter nacional e internacional, con el fin de judicializar a los responsables (Policia Nacional de Colombia, 2015).

Dentro de este componente se encuentran definidos los siguientes grupos de trabajo:

- Contra el fraude en internet.
- Contra el abuso de las criptomonedas.
- Contra el material de abuso infantil.
- Protección institucional.

- Acción efectiva Operacional.
- Plan de reducción de cibercrimen.
- Conexidad de procesos a nivel nacional.
- Soporte actividades judiciales a través de laboratorios de informática forense.

Igualmente, el modelo de investigación de los delitos cibernéticos (Figura 21) para este componente corresponde a la definición de los estándares internacionales establecidos en la convención de Budapest, con la adopción de un modelo nacional de frentes de investigación que comprende los delitos que afectan la información y los datos (Ley 1273/2009), y los delitos que utilizan los medios tecnológicos para su materialización, y que corresponden a otras legislaciones para reducir el fenómeno en las ciudades de mayor influencia. (Policía Nacional de Colombia, 2018).

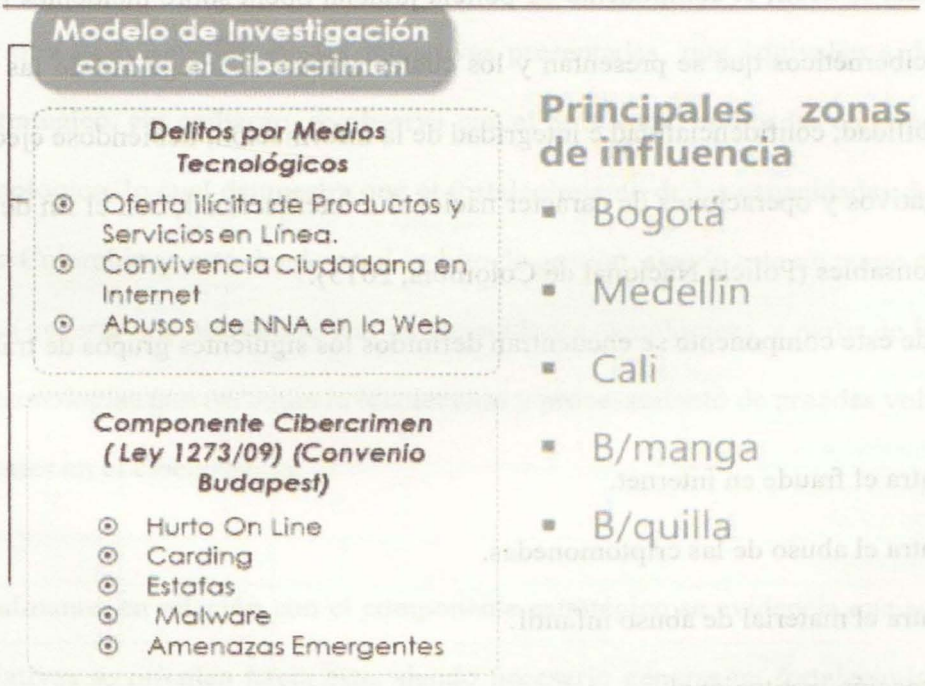


Figura 21. Modelo de Investigación contra el Cibercrimen. Fuente: Policía Nacional de Colombia, (2018)

La tarea investigativa se complementa con el trabajo conjunto de la Fiscalía General de la Nación, con una fiscalía especializada para temas cibernéticos, y las diligencias de policía judicial como apoyo a la investigación. Igualmente se soporta con la utilización de fuentes internas (PANDORA, Sistema de Investigación Criminal Antifraude - SICAF, OSINT), y externas de información, con la automatización y sistematización bajo los conceptos de Big Data y minería de datos, que permiten la correlación de actores y fenómenos delincuenciales transversales a otros ejes de investigación (Policía Nacional de Colombia, 2018).

El modelo se soporta bajo el eje transversal de informática forense, y se despliega en el nivel desconcentrado con las Unidades de Investigaciones Tecnológicas - UDITE, las cuales dependen de las seccionales de investigación criminal SIJIN bajo la coordinación y apoyo del nivel central. Adicional, se cuenta con ocho 8 laboratorios de informática forense en las regiones de Policía, para dar soporte y apoyo a la investigación criminal en aspectos técnicos, y el tratamiento de la evidencia digital (Policía Nacional de Colombia, 2018).

3. **Articulación y Cooperación:** en cumplimiento a este componente, el CCP ha venido liderando el desarrollo de mesas de integración, entre otros con, Presidencia de la República de Colombia donde se han implementado grupos de trabajo para la atención de amenazas y análisis criminales. Igualmente, se han desarrollado convenios y alianzas con otras entidades del estado (Policía Nacional de Colombia, 2019).

Con este componente se complementa la actividad preventiva e investigativa, actuando

bajo los principios de articulación y cooperación interinstitucional, con el fin de compartir información y contrarrestar la actividad criminal. Es por ello que el 2018 se consolida el proyecto de Centro de Capacidades para la Ciberseguridad de Colombia – C4 con una inversión superior a los $ 5.000.000.000 millones de pesos en tecnología, en el que se articulan las capacidades del Estado para la atención de los fenómenos criminales que afectan la seguridad cibernética del país (Policía Nacional de Colombia, 2018).

Dentro de las prioridades de este componente se destacan: mesas de trabajo con organismos y entidades de las múltiples partes interesadas en ciberseguridad, incremento de la participación de la Policía Nacional en el contexto internacional, implementación de grupos de trabajo y fuerzas de tarea cibernética, mesas de crisis para la atención de amenazas y fenómenos criminales emergentes, vinculación con la academia para capacitación entrenamiento, transferencia de conocimiento, desarrollo de alianzas y convenios con sector público y privado, intercambio de información para la investigación criminal y la articulación de capacidades institucionales (Policía Nacional de Colombia, 2018).

Por lo anterior, y con el fin de realizar el despliegue de la Estrategia Integral de Ciberseguridad la Policial Nacional mediante la Directiva Operativa Transitoria No. 030 de 2018 y No. 038 de 2019, ha fijado las directrices y parámetros instituciones para la implementación efectivas de esta y propiciar de esta forma escenarios seguros para el acceso a las tecnologías de la información y las comunicaciones a los ciudadano, así como prevenir, atender e investigar los fenómenos delictivos que afecta la Convivencia y Seguridad Ciudadana en el ciberespacio, bajo un enfoque de ciberseguridad y de corresponsabilidad con

las demás instituciones comprometidas, de la siguiente forma (Policía Nacional de Colombia, 2019):

Dirección de Seguridad Ciudadana – DISEC

- Coordina con la DIJIN, la implementación, seguimiento y evaluación de las acciones que son responsabilidad de las policías Metropolitanas y Departamentos de Policía en el marco de la Estrategia.
- Diseña y Difunde en coordinación con la DIJIN un plan para la estandarización del proceso de prevención en el ámbito cibernético para que sea aplicado a través del portafolio de servicio institucional.
- Coordina con la DIJIN la generación y/o actualización de lineamientos que guíen la actuación de las Direcciones Operativas y de los funcionarios del MNVCC, frente a la atención de los ciberdelitos.
- Dispone en las policías Metropolitanas y Departamentos de Policía, la implementación del plan de capacitación proyectado por la Dirección Nacional de Escuelas en coordinación con la DIJIN, respectos a las herramientas de actuación policial frente a los ciberdelitos.

Dirección de Investigación Criminal e Interpol – DIJIN

- Gerencia, supervisa y direcciona las actividades institucionales que garanticen la continuidad y sostenibilidad en materia de despliegue de la Estrategia Integral de Ciberseguridad – ESCIB, debiendo desarrollar acciones para su cumplimiento y

consolidación, garantizando la participación de las direcciones comprometidas en la mitigación de los delitos informáticos y el uso del ciberespacio como medio del despliegue de fenómenos criminales.

- Define las actividades que deberán desarrollar los funcionarios designados para integrar el Centro de Capacidades para la Ciberseguridad de Colombia - C4.
- Dispone del Centro Cibernético Policial y de la Unidad de Seguimiento Operacional, para supervisar y controlar el desempeño de las Seccionales de Investigación Criminal en el marco del despliegue de la Estrategia ESCIB.
- Dispone del fortalecimiento y continuidad de los funcionarios de la Unidad de Seguimiento Operacional y del Centro Cibernético Policial con competencias en la administración de información y análisis operacional y conocimiento en materia judicial, con el fin de orientar, retroalimentar, controlar y evaluar de manera integral las actividades que deben realizar las unidades policiales comprometidas con la ESCIB.
- Coordina el fortalecimiento de las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes a través de la creación y consolidación del Centro de Fusión para la Investigación de Crímenes Económicos y Financieros, el Centro C4, el Observatorio de crímenes y los delitos en el entorno digital.
- Realiza ciber-patrullaje 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 circula en el ciberespacio.

- Lidera bimestralmente mesas de trabajo con diferentes sectores corresponsables en la problemática (proveedores de internet, RedPapAz, MINTIC, Microsoft, CCIT, Asobancaria), con el fin de evaluar los alcances y resultados de la estrategia.
- Desarrolla en coordinación con la Fiscalía General de la Nación, las investigaciones judiciales de carácter trasnacional, orientadas a la identificación y desarticulación de organizaciones criminales dedicadas al cibercrimen y al uso del ciberespacio como medio delictivo.
- Consolida el C4 como parte del Centro Cibernético Policial, para focalizar alertas y emitirlas. Igualmente como medio para realizar análisis de información y articular con el Gobierno Nacional la atención, investigación, reacción, contención, despliegue, y gestión de incidentes informáticos.
- Administra el Sistema de Investigación Criminal Antifraude – SICAF y fija parámetros de uso, empleo, registro y validación de la información que deberá ser insertada en el sistema, con enfoque a las acciones de prevención para contrarrestar el fenómeno del cibercrimen a nivel nacional.
- Fortalece los canales de prevención y atención ciudadana, para la atención efectiva de incidentes cibernéticos mediante el CAI virtual, desde donde se realiza el acompañamiento a la ciudadanía con un servicio ininterrumpido, adoptando los protocolos de tratamiento de evidencia digital y su trámite ante la autoridad competente.
- Garantiza la capacitación, formación, actualización de herramientas tecnológicas, fortalecimiento de los laboratorios de informática forense del personal encargado del despliegue de la estrategia en cada uno de los procesos.

- Desarrolla banco de proyectos para el fortalecimiento del Centro Cibernético Policial y de esta forma alinear la institución con la Política de Seguridad Digital del Estado.
- Implementa un modelo investigativo frente a los delitos que afectan la ciberseguridad de los ciudadanos y del sector público y privado, en coordinación con la Fiscalía General de la Nación, que permita la priorización de actividades de Policía Judicial.

Dirección de Inteligencia Policial – DIPOL

- Desarrolla mecanismos para el monitoreo de medios digitales, análisis de fuentes abiertas, seguimiento y análisis de redes sociales, análisis situacional de contenidos, identificación de articuladores mediáticos, para contribuir a la disminución de fenómenos delictivos que impactan la Ciberseguridad de Colombia.
- Lidera los CI3-APSD "Centros Integrados de Información de Inteligencia para la Atención y Prevención de la Seguridad Digital" consolidando las memorias, plasmando los cursos de acción y realizando el seguimiento de los compromisos.
- Realiza trabajo articulado con la DIJIN, en el marco del ciber-patrullaje 24/7 en la web, con el propósito de contrarrestar amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y defensa de la nación.
- Informa a la DISEC y DIJIN, sobre la identificación de actores y fenómenos que permitan generar alertas tempranas en materia de Ciberseguridad.
- Articula con el CSIRT (Computer Security Incident Response Team), liderado por la Oficina de Telemática, la identificación y caracterización de ataques realizados a la plataforma tecnológica de la Policía Nacional y los dominios "gov.co".

- Coordina son su Seccionales de Inteligencia Policial, para que desde su misionalidad en conjunto con la Investigación Criminal realicen la identificación de estructuras relacionadas con el cibercrimen, así mimos, fortalece las actividades de inteligencia para obtener información estratégica y operacional que permita aportar productos de Inteligencia a la estrategia.
- Presenta el plan de trabajo propuesto por la DIJIN ante las instancias del CLACIP y EUROPOL, para la recolección de información estratégica ante objetivos de alto valor en las organizaciones delictivas dedicadas al Cibercrimen.
- Coordina con la Oficina de Telemática, los aportes para la implementación de nuevas tecnologías en pro de mejorar la capacidad y el despliegue en anticipación, prevención y detección, para la contención de ataques informáticos que pongan en peligro la seguridad de la información y desestabilicen el Estado Colombiano, presentando iniciativas a través de proyectos de desarrollo tecnológico de manera trimestral.
- Identifica, anticipa y previene amenazas que afecten la estabilidad gubernamental e institucional recolectando insumos que permitan aportar y orientar acciones investigativas, penales y disciplinarias de los actores.

Dirección Antisecuestro y Antiextorsión – DIASE

- Coordina con la DIJIN, las acciones requeridas en materia de prevención para propender por un ambiente que garantice la reducción del cibercrimen en delitos de secuestro y extorsión. Esta actividad es reportada por intermedio del enlace de esta Dirección en el C4.

- Entrega reporte de las extracciones del Laboratorio de Informática Forense, resultado de los apoyos a las diferentes investigaciones de los GAULA.

Dirección de Protección y Servicios Especiales – DIPRO

- Elabora un plan de trabajo con acciones preventivas y de anticipación dirigidas a la población de niños, niñas y adolescentes que hacen uso de las tecnologías de la información y comunicación (Programa abre tus ojos, bloque temático encaminado a la virtualización del programa para llegar a cualquier parte del país).
- Coordina, acompaña y estructura la realización del material para las campañas preventivas y educativas en planteles e instituciones escolares, donde se vinculen a los padres de familia, docentes y estudiantes a fin de sensibilizar y prevenir delitos como abuso sexual con menores de edad y pornografía infantil referenciando el uso responsable de las tecnologías y las comunicaciones.
- Coordina con la DIJIN, el intercambio de información efectivo en relación con delitos por medios informáticos como es la distribución de contenido de abuso infantil, informándolas acciones adelantadas y contenido identificado para un accionar integral, a través del funcionario que se encuentra como enlace en el C4.

Dirección Nacional de Escuelas – DINAE

- Incluye en el Plan Anual de Educación de la Institución, la oferta académica de la Estrategia Integral de Ciberseguridad ESCIB previa validación del contenido temático con asesores

(CCP, CSIRT, ESTIC, DIPRO, DIASE, DIPOL y DISEC) y certifica al personal una vez culminen los eventos académicos.

- Promueve en coordinación con la DIJIN la realización de convenios con universidades nacional y/o extranjeras, que permitan actualizar y potenciar el conocimiento del talento humano de la Policía Nacional designado para cumplir funciones en materia de Ciberseguridad en Colombia.

Oficina de Comunicaciones Estratégicas – COEST

- Estructura con la DIJIN y el CAI – VIRTUAL, la activación comunicacional para el despliegue de la estrategia.
- Difunde la Estrategia Integral de Ciberseguridad a través del "cuadrante virtual", utilizando el hashtag #Ciberseguridad e involucrando el portal web institucional www.policia.gov.co.
- Diseña y difunde en coordinación con la DIJIN, un plan de medios que permite comunicar las acciones institucionales de prevención, así como los resultados obtenidos referentes a Ciberseguridad.

Oficina de Telemática – OFITE

- Coordina con la DIJIN, DIPOL y DISEC, la formulación y diseño de los desarrollos tecnológicos para el despliegue de la ESCIB.
- Adquiere y suministra soporte técnico y tecnológico requerido para el desarrollo de la estrategia, previa coordinación con el gerente de esta.

- Dispone del equipo de respuesta a incidentes de seguridad informática de la Policía Nacional CSIRT, para el despliegue de la ESCIB.
- Garantiza la conectividad permanente del ancho de banda adecuado, de acuerdo con la misionalidad de las instalaciones del C4.

Área de Relaciones y Cooperación Internacional Policial de la Dirección General – ASUIN

- Fortalece los canales de cooperación internacional policial con las entidades homólogas a fin de combatir las amenazas de ciberseguridad en Colombia.
- Coordina con la DIJIN y DIPOL, la elaboración de un plan de trabajo que permita contrarrestar las amenazas de ciberseguridad en Colombia, el cual será ejecutado por el personal que se encuentra asignado por la Policía Nacional en EUROPOL.
- Asesora la DIJIN en la formulación de nuevos acuerdos interinstitucionales internacionales, que fortalezca el trabajo mancomunado y el intercambio de experiencia y de información en temas de ciberseguridad.

Grupo de Respuesta a Incidentes de Seguridad – CSIRT

Este grupo pertenece a la Ofician de Telemática y se encarga de la atención a incidentes informáticos de la Policía Nacional, cumpliendo las siguientes funciones (Policia Nacional de Colombia, 2013):

- Detectar, reportar y solucionar, vulnerabilidades, amenazas e incidentes informáticos que afectan la disponibilidad, confidencialidad e integridad de la información en la Policía Nacional, a su vez verificar, monitorear y auditar la plataforma de antivirus de la institución, generando reportes y estadísticas.
- Realizar la difusión, concientización y prevención de las políticas de seguridad de la información.
- Alertar y advertir los incidentes de seguridad de la información, para mantener informado a las unidades de la Policía Nacional.
- Realizar el tratamiento de incidentes de seguridad de la información, para garantizar su protección y minimizar los riesgos de seguridad de la información.
- Apoyar y dar respuesta a los incidentes de seguridad de la información que se presenten en la institución, para evitar daños en la infraestructura tecnológica.
- Supervisar la actualización y aplicación de parches de seguridad de la información para controlar la seguridad de la información.
- Coordinar con COEST, el diseño de campañas de concientización sobre seguridad de la información en la Institución.
- Aplicar mecanismos de detección de intrusos y externos sobre la red institucional.
- Implementar y hacer seguimiento a la Estrategia Nacional para la protección del ciberespacio a fin de contribuir a la sensibilización del ciber-ciudadano sobre la importancia de la seguridad de la información.
- Realizar acuerdos de colaboración y convenios con diferentes organismos nacionales e internacionales, que permita construir una red mundial de apoyo en ciberseguridad.

Igualmente, como parte de su capacidad tecnológica en ciberseguridad, cuenta con un portal web (https://cc-csirt.policia.gov.co) en el cual ofrece los siguientes servicios:

- SANDBOX: permite verificar archivos o URL Maliciosas.
- APK: analizador de aplicaciones móviles.
- CTF: juego de seguridad informática (Captura la bandera)

Aunado a lo anterior, el CSIRT PONAL hace parte del CSIRT gobierno el cual es liderado por el Ministerio de Tecnologías de la Información y Comunicaciones.

Centro Cibernético Policial – 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 (Policia Nacional de Colombia, 2015).

Actualmente, es la responsable de desarrollar la capacidad de detección, prevención, investigación, análisis, correlación, convergencia tecnológica, procedimientos de respuesta frente a las situaciones de crisis informática, planes de contingencia específicos y judicialización de las amenazas que afectan la ciberseguridad en el ámbito nacional criminal (Policia Nacional de Colombia, 2015) .

Así mismo, lidera los 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, así como, aquellas organizaciones que realizan ciberterrorismo que atenta contra la integridad de las personas (Policia Nacional de Colombia, 2015).

En razón al fortalecimiento a la ciberseguridad, el CCP es responsable también de desarrollar soluciones tecnológicas que permitan generar capacidades institucionales mediante aplicaciones o software que contribuyan al uso seguro de la web por parte de los cibernautas, así como, fortalecer el conocimiento, 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 ESCIB (Policia Nacional de Colombia, 2015).

Finalmente, le corresponde al CCP atender los incidentes cibernéticos reportados por los ciber-ciudadanos a través de los canales de comunicación oficiales, como el CAI virtual, adoptando los protocolos de tratamiento de la evidencia digital y su trámite ante la autoridad competente, complementando esta actividad con el desarrollo ciber-patrullaje 24/7, el cual es realizado por funcionarios de la institución y que tiene como propósito identificar amenazas desde y hacia Colombia en contra de la ciberseguridad ciudadana, desarrollado la capacidad de identificación y detección de factores comunes en los incidentes de su conocimiento, así como la vulneración a los principios de la seguridad de la información en el ciberespacio (Policia Nacional de Colombia, 2015).

Por otra parte, para el fortalecimiento de sus capacidades de ciberseguridad el CCP se apoya en el Laboratorio de Informática Forense, con el fin de realizar los exámenes, análisis o estudios de los elementos materiales probatorios solicitados por autoridades judiciales, o policía judicial dentro de un proceso penal, emitiendo los respectivos dictámenes.

Este laboratorio cuenta con 10 peritos, los cuales se encargan de dar respuesta a incidentes cibernéticos, adquirir datos volátiles y realizar imágenes forenses, así como realizar auditorías a bases de datos, análisis de malware y equipos terminales, contando de igual forma con un laboratorio móvil. Asimismo, dentro de sus capacidades tecnológicas se encuentra la plataforma para el análisis dinámico de software malicioso, los softwares de Forense NUIX y Forense AXIOM, la solución para la extracción de información y análisis de dispositivos móviles UFEAD 4PC y un sistema SANDBOX.

Centro de Capacidades para la Ciberseguridad de Colombia –C4

Es un centro en el cual se centralizan todas las capacidades de ciberseguridad de Colombia, que tiene como propósito contribuir a la ciberseguridad de los ciudadanos. Entre sus principales objetivos se encuentra el de consolidar las alertas de cibercrimen, así como focalizar la atención de ciberdelitos, coordinando durante las 24 horas del día los 7 días de la semana, la identificación de amenazas cibernéticas a partir de la convergencia tecnológica especializada.

Actualmente entre sus principales funciones se encuentra la Difusión de Alertas por

Redes Sociales, la generación de boletines, el ciber-patrullaje de amenazas en internet y el análisis en Deep Web y Darknet.

El C4 cuenta con 10 operadores y 22 analistas los cuales se distribuyen en los 32 puestos de trabajo, una oficina de coordinación y una sala de crisis, las cuales son utilizadas por miembros de diferentes instituciones del estado que aportan desde su misionalidad a la ciberseguridad. En la Figura 22 se muestra la distribución física del C4:

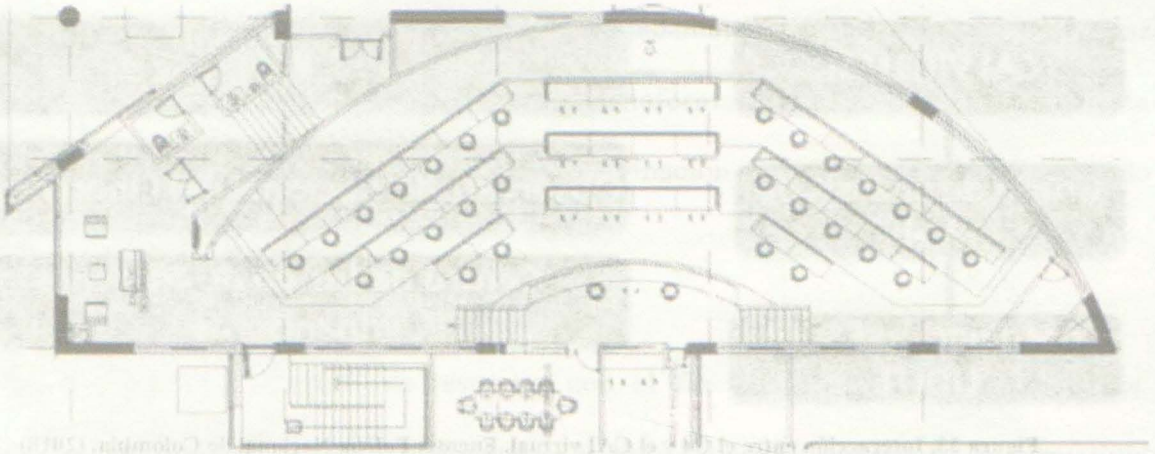


Figura 22. Distribución física del C4. Fuente: Policía Nacional de Colombia, (2018)

Frente a la proyección de investigación, actualmente en el C4 se ubica el Centro Cibernético Policial el cual cuenta con 25 investigadores, 11 analistas de prevención, 8 peritos de Informática forense quienes se enfocan principalmente en los delitos relacionados con el abuso sexual infantil en internet, acceso abusivo a sistemas informáticos, oferta ilícita de productos (drogas) en la web, fraude y hurto informático, convivencia ciudadana en internet (redes sociales) y software malicioso (Policía Nacional de Colombia, 2018).

Así mismo, en las instalaciones del C4 se ubica el CAI virtual, el cual actualmente está conformado por 32 funcionarios, quienes están encargados de atender y gestionar 24/7 los incidentes cibernéticos, realizar análisis de fuentes abiertas de información, generar alertas, desarrollar boletines y ciber-patrullaje, esta última apoyada mediante el software FOCAL-INFO. Igualmente realiza el bloqueo de páginas con material de abuso infantil, realiza análisis WEB, participa en la coordinación de la ESCIB y realiza coordinaciones con el C4 como se muestra en la Figura 23.

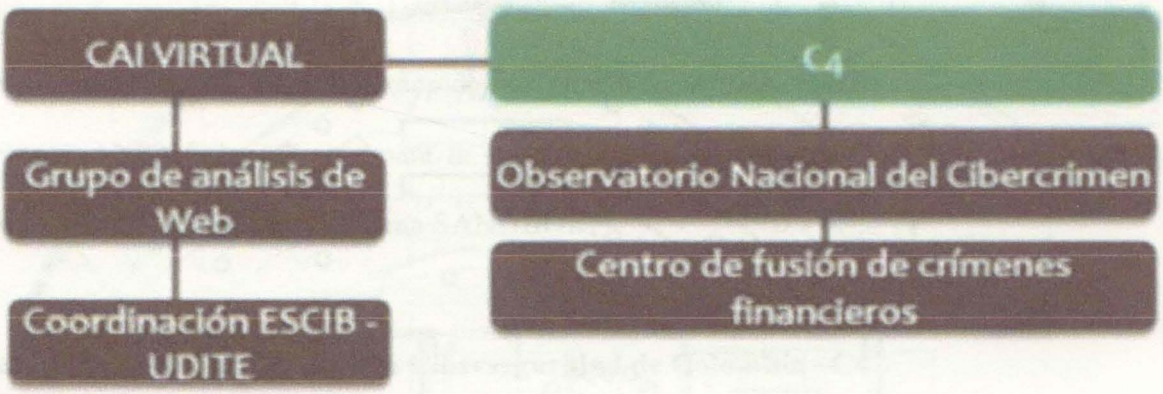


Figura 23. Interacción entre el C4 y el CAI virtual. Fuente: Policía Nacional de Colombia, (2018)

2. Análisis de las capacidades y componentes de ciberseguridad - Policía Nacional

A partir de la información anterior, se puede evidenciar las responsabilidades que son asignadas a cada una de las unidades policiales y cómo la mayoría de estas, están orientadas a generar actividades de coordinación con la DIJIN y el CCP, al ser quienes lideran la Estrategia de Ciberseguridad.

Igualmente, se evidencia que las otras unidades solo tienen la responsabilidad de designar el personal que participará desde su misionalidad como actores, ya sea para apoyar la prevención, procesos investigativos o la generación de canales de cooperación, la DIPOL apoya las actividades de ciber-patrullaje y caracterización de fenómenos; DIASE todo lo relacionado con incidentes relacionados con secuestro y extorsión; DIPRO las actividades que involucren niños, niñas y adolescentes; DINAE aporta desde su misionalidad, la implementación de capacitaciones para fortalecer las competencias de los funcionarios que trabajan en torno a la ciberseguridad; ASUIN realiza las gestiones para la generación de convenios con entidades de carácter internacional; COEST apoya la comunicación de información a la ciudadanía; OFITE brinda el soporte necesario para garantizar el funcionamiento correcto de la plataforma tecnológica y DISEC facilita el personal requerido para participar en programas de formación y atención a incidentes cuando es requerido.

Por lo anterior y a modo de resumen, con el fin de identificar las capacidades de ciberseguridad con las que cuenta actualmente la Policía Nacional, a partir de la normatividad, actores y responsabilidades (elementos) descritos en los componentes de la ESCIB los cuales conforman el ecosistema de ciberseguridad de esta institución, se realizó el siguiente análisis utilizando el proceso de ciberinteligencia propuesto por Blanco (2018), teniendo en cuenta que une el ciclo de inteligencia y el modelo de ciberseguridad de NIST necesarios para la presente investigación, por lo cual los resultados obtenidos en la Tabla 19 son dados en términos de detección, análisis y respuesta, y en adición el factor de coordinación.

Tabla 19. Análisis de las capacidades de detección, análisis, respuesta y coordinación de la PONAL a partir de la valoración de la normatividad, componentes de la estrategia y actores. Fuente: elaboración propia a partir de la información descrita en la Directiva Administrativa Transitoria No. 38 (Policía Nacional de Colombia, 2019), el Modelo de Planeación y Gestión Operacional del Servicio de Policía (Policía Nacional de Colombia, 2018) y el proceso de ciberinteligencia propuesto por Blanco con base al modelo NIST (Blanco, 2018, p. 24)

	TIPO DE INICIATIVA			ECOSISTEMA	COMPONENTES	ELEMENTOS	ELEMENTOS DEL MODELO			
							Detección	*Análisis*	*Respuesta*	*Coordinación*
Capítulo II: Identificación de capacidades PONAL	Estratégico			**Normas**	CONPES 3854	1	-	-	-	1
	Estratégico				Direc. Opera. Trans	1	-	-	-	1
	Estratégico				Res. Estra. Org	1	-	-	-	1
	Estratégico			**Estrategia**	Prevención	1	1	1	-	-
	Estratégico				Judicialización	1	-	1	1	-
	Estratégico				Cooperación	1	-	-	1	1
		Gestión		**Actores**	DISEC	4	-	-	1	3
	Estratégico	Gestión			DIJIN	14	2	4	4	4
		Gestión			DIPOL	9	3	1	-	5
		Gestión			DIASE	2	1	-	1	-
		Gestión			DIPRO	3	2	-	1	-
		Gestión			DINAE	2	-	-	-	2
		Gestión		**Actores**	COEST	3	1	-	2	-
		Gestión			ASUIN	3	-	-	1	2
		Gestión	Tecnología		OFITE	4	-	-	1	3
		Gestión	Tecnología		CSIRT	10	3	-	3	4
		Gestión	Tecnología		CCP	13	2	4	4	3
		Gestión	Tecnología		C4	6	4	2	-	-
			Total	**3**	**18**	**79**	**19**	**13**	**20**	**30**
			Distribución porcentual				24%	16%	25%	38%

Como se evidencia en la Tabla 19, el 38% de los elementos del ecosistema de ciberseguridad de la Policía Nacional, se centran en actividades de coordinación entre unidades de la institución, con otras entidades públicas y privadas de Colombia y organizaciones internacionales.

Por su parte, el 25 % de los elementos se orientan a dar respuesta a incidentes cibernéticos y delitos informáticos, los cuales tienen como principales actores la DIJIN y el CCP como responsables de realizar actividades de investigación y judicialización, seguidos del CSIRT como encargado de atender los incidentes que se presentan al interior de la Policía Nacional.

Estas actividades son realizadas mediante la utilización de herramientas sandbox, software de correlacionador de eventos para la detección y priorización de ciberamenazas (QRADAR), equipos de detección electrónica de dispositivos (Orion), software para de análisis de datos (ARBUTUS, IDEA y ACL) y una solución forense para dispositivos móviles como celulares, GPS, portátiles y tabletas (Cellebrite Ufed Touch Ultimate).

Aunado a lo anterior, los elementos de detección corresponden a un 24%, en los cuales se despliegan actividades de ciber-patrullaje y análisis de fuentes abiertas (software FOCALINFO), así como la realización de campañas de sensibilización y difusión de boletines y aleras de seguridad, por parte del C4, la DIPOL y el CSIRT.

Así mismo, el 16% de los elementos corresponden al análisis, lo cual demuestra que actualmente existe una debilidad en el estudio de fenomenologías que afectan la ciberseguridad. Dentro de este elemento, se encuentra el Centro de Fusión para la investigación de Crímenes Económicos y financieros y Observatorio de crímenes y los delitos en el entorno digital, los cuales se encuentran en proceso de maduración, por lo cual aún no generan el impacto deseado.

Por otra parte, se evidencia que las iniciativas tecnológicas están centradas en el CCP, C4

y CSIRT PONAL, siendo responsabilidad de las otras unidades coordinar y cooperar con estos la ejecución de actividades.

Igualmente, se observa que la mayoría de las responsabilidades son de gestión y que el componente tecnológico con el que cuenta la Policía Nacional en torno a la ciberseguridad está orientado a la investigación y judicialización de delitos informáticos e incidentes cibernéticos. Por su parte, la prevención está limitada en este aspecto, ya que la recolección de información se realiza mediante patrullaje manual por funcionarios de la PONAL, apoyándose solamente de las denuncias que realiza la ciudadanía mediante el CAI virtual y la utilización de la herramienta FOCAL-INFO para la recolección y análisis de información de fuentes abiertas.

Es importante mencionar, que lo anterior es una falencia que ya es evidente por parte de la Dirección de Inteligencia Policial, quien, en cumplimiento a las responsabilidades asignadas en el marco de la ESCIB, se encuentra en proceso de adquisición de un "Sistema de ciberinteligencia basado en inteligencia artificial", el cual se encuentra publicado en la página de Colombia Compra eficiente en el Sistema Electrónico de Contratación Púbica, con el código PN DIPOL SA 049-2020.

Así mismo, es importante destacar que existen muchos convenios de cooperación con entidades de carácter nacional e internacional, que han permitido fortalecer las capacidades de la Policía Nacional relacionadas con la ciberseguridad, por ejemplo, el tema de las capacitaciones al talento humano, la participación en congresos y eventos de ciberseguridad y el intercambio de información.

En complemento a lo anterior, como se observa en la Figura 24 la Policía Nacional se centra principalmente en realizar actividades que permiten la coordinación con otras entidades y unidades para el fortalecimiento de las capacidades de ciberseguridad de la institución y en la respuesta a los incidentes cibernéticos que se asocian a delitos informáticos, siendo esto un factor de atención que genera la necesidad de reforzar y potencializar los elementos de detección y análisis en la propuesta del modelo de ciberinteligencia a estructurarse en la presente investigación, de tal forma que se cuente con mecanismos que permitan generar la anticipación, prevención y análisis y caracterización de los fenómenos que afectan la ciberseguridad en el ciberespacio.

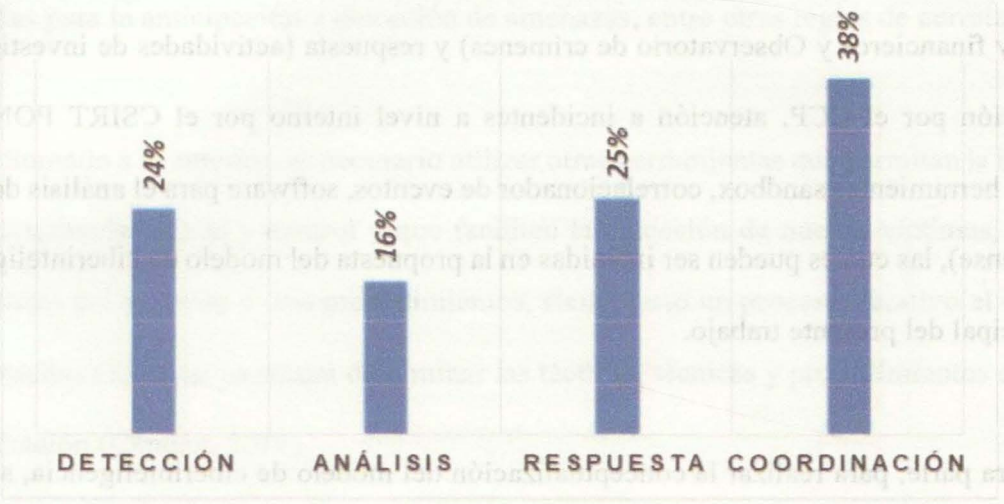


Figura 24. Distribución porcentual de las capacidades actuales de ciberseguridad de la PONAL. Fuente: Elaboración propia a partir de los resultados del análisis de capacidades de la PONAL, (2020)

Finalmente, con la información obtenida del análisis realizado en el presente capítulo, se logró identificar las capacidades de ciberseguridad y ciberinteligencia que tiene la Policía Nacional, las cuales aunadas a los elementos constitutivos y al ciclo de inteligencia revisados en el capítulo II, permite que en la siguiente sección se proceda a realizar la propuesta del modelo de ciberinteligencia y describir cada uno de los componentes que lo conformarán.

CAPITULO IV

CONCEPTUALIZACIÓN DEL MODELO DE CIBERINTELIGENCIA PARA LA POLICÍA NACIONAL ADAPTADO AL CICLO DE INTELIGENCIA

A partir de la información presentada en el capítulo anterior, se logró evidenciar que actualmente la Policía Nacional de Colombia cuenta con capacidades en el ámbito de ciberseguridad relacionadas con: detección (CAI virtual, ciber-patrullaje 24/7 y análisis de fuente abiertas – software FONCALINFO), análisis (Centro de Fusión para la investigación de Crímenes Económicos y financieros y Observatorio de crímenes) y respuesta (actividades de investigación y judicialización por el CCP, atención a incidentes a nivel interno por el CSIRT PONAL y utilización de herramientas sandbox, correlacionador de eventos, software para el análisis de datos y análisis forense), las cuales pueden ser incluidas en la propuesta del modelo de ciberinteligencia, objetivo principal del presente trabajo.

Por otra parte, para realizar la conceptualización del modelo de ciberinteligencia, se debe entender que su papel dentro de la generación de ciberseguridad es la de mejorar las capacidades de anticipación, detección y respuesta, a través de la vigilancia y el análisis, utilizando herramientas y personal capacitado, siendo su propósito principal generar información relevante para apoyar y facilitar la toma de decisiones en cuestiones relativas al ciberespacio (Candau, 2017).

Aunado a lo anterior, la revisión del Ciclo de Inteligencia de la Policía Nacional de

Colombia permitió evidenciar que sus actividades (planear, recolectar, tratar, analizar y comunicar e integrar), mantienen su validez, siempre y cuando se respeten las características propias del ciberespacio: 1) rapidez en la elaboración, debido al corto espacio de tiempo en el que esta información es válida y 2) la utilización en gran medida de fuentes técnicas, aunque la obtención de fuentes humanas sigue teniendo un valor trascendental (Candau, 2017)..

Así mismo, se evidenció que para la generación de ciberinteligencia es necesario utilizar herramientas que permitan la recolección y almacenamiento de grandes volúmenes de datos de los diferentes dispositivos conectados a internet y su correlación avanzada, basadas en reglas o en anomalías para la anticipación y detección de amenazas, entre otras reglas de correlación.

Sumado a lo anterior, es necesario utilizar otras herramientas que permitan la identificación de estructuras de mando y control y que faciliten la detección de nuevas víctimas, así como las capacidades del atacante y sus procedimientos, siendo esto un proceso iterativo el cual aplicado sobre muchas víctimas, permitirá determinar las tácticas, técnicas y procedimientos del atacante y su motivación (Candau, 2017)

De allí que el aporte de las tecnologías a la inteligencia sea relevante, en la recolección, tratamiento, análisis y difusión de información de valor, al permitir que estas actividades se desarrollen de manera más sencilla, eficiente y eficaz, por lo cual y partiendo de que el modelo de ciberinteligencia para la Policía Nacional debe alinearse con el ciclo de inteligencia ya definido en la doctrina institucional, este se deberá adaptarse a los fenómenos que ocurren en el ciberespacio.

1. Inclusión de elementos ciberseguridad en el ciclo de inteligencia.

Desde el marco de ciberseguridad propuesto por el Instituto Nacional de Estándares y Tecnología – NIST (2018) el cual se relacionó en el capítulo dos, se revisó como este interactúa con el ciclo de inteligencia y se transforma en un ciclo de ciberinteligencia, siendo necesario para la definición del modelo revisar cada una de las funciones propuestas en este framework y cruzarlas con las actividades del ciclo de inteligencia y determinar cuáles de estas deben ser incluidas en este último, como se muestra en la Tabla 20.

Tabla 20. Actividades del ciclo de inteligencia y funciones del modelo de ciberseguridad NIST. Fuente: elaboración propia a partir de la información descrita en el Manual de Inteligencia de la Policía Nacional (2014) y el Marco de Seguridad NIST (2018)

Actividades Ciclo de Inteligencia Policial	Funciones del Modelo NIST	Elementos
Planear	Identificar	- Gestión de activos. - Revisión del entorno. - Gobernanza. - Evaluación de riesgos. - Métodos prospectivos. - Vigilancia tecnológica.
Recolectar	Detectar	- Anomalías y eventos. - Monitoreo continuo de la Seguridad. - Procesos de detección. - Evaluación de riesgos.
Tratar	Responder	- Filtrado, evaluación, clasificación e integración de la información
Analizar		- Análisis de los eventos de ciberseguridad. - Definición de medidas de anticipación, prevención y atención a incidentes. - Análisis de Big Data - Machine Learning, algoritmos avanzados, redes neuronales, Inteligencia Artificial.
Difundir y Comunicar	Recuperar	- Actividades de anticipación, prevención y mitigación. - Receptores de inteligencia. - Resultados de los análisis.
Evaluar y Retroalimentar	No aplica	- Lecciones aprendidas - Oportunidades de mejora - fortalecer y maximizar la eficiencia de las actividades
No aplica	Proteger	- Controles de seguridad de la información. - Concientización y Capacitación.

Apoyados en lo presentado en la Tabla 20, se describen las siguientes actividades del ciclo de inteligencia:

1.1. Planear

Esta actividad hace referencia a la función identificar, en la cual se relaciona todo el proceso de planeación, soportado en el marco legal y en la gestión de riesgos mediante el cual se proyecta priorizar las actividades del ciclo de ciberinteligencia. Asimismo, con base al requerimiento de inteligencia, se procede a determinar el alcance, plazos y recursos precisos. Posteriormente, se lleva a cabo un plan para la parametrización de las fuentes y palabras claves sobre las herramientas de detección automatizada que se puedan utilizar, de manera que los sistemas queden preparados para la monitorización automática (Blanco, 2018).

Igualmente, dentro de este elemento se debe contemplar la implementación de métodos prospectivos que permitan la construcción de escenarios futuros para mejorar la asignación de recursos (humanos, técnicos y económicos) y la ejecución de actividades de vigilancia tecnológica, con las cuales la Policía Nacional pueda estar en la vanguardia y entender también que tecnología usa o puede ser usada por los ciberdelincuentes.

Está actividad cuenta con los siguientes elementos los cuales deben ser documentados mediante una "Misión de Trabajo" conforme a lo establecido en el artículo 14 de la ley 1621 de 2013:

- **Gestión de activos:** se realiza la identificación de las plataformas y sistemas a verificar (Instituto Nacional de Estándares y Tecnología, 2018), siendo necesario que la Policía Nacional

cuente con un inventario de los activos de información que tienen valor en la generación de ciberseguridad, como es el caso de las plataformas de redes sociales, sistemas de entidades públicas y demás sitios de internet en los cuales las personas desarrollan algún tipo de actividad socioeconómica.

- **Revisión del entorno:** en este elemento se entienden y priorizan los objetivos, el motivo de la recolección, las partes interesadas y las actividades a realizar, informando los roles y responsabilidades y decisiones a tomar en caso de identificarse o presentarse riesgos que puedan afectar la ciberseguridad (Instituto Nacional de Estándares y Tecnología, 2018).
- **Gobernanza:** se definen las políticas, procedimientos, los requisitos legales y regulatorios para el desarrollo de actividades de inteligencia, así como la gestión de riesgos. Igualmente en esta actividad, se coordina que los roles y responsabilidades a nivel de la institución se alineen con las entidades que brindaran algún tipo de cooperación para el desarrollo de las actividades a realizarse.
- **Evaluación de riesgos:** en relación con la ciberseguridad, se identifican y se documentan las vulnerabilidades y amenazas (internas y externas) de los activos de información relacionados previamente, determinando los riesgos con su respectivo impacto y probabilidad de materialización, esto con el fin de priorizar las respuestas a los mismos (Instituto Nacional de Estándares y Tecnología, 2018).
-
- **Estrategia de gestión de riesgos:** los actores del modelo establecen, gestionan y acuerdan los procesos para la gestión de riesgos, determinado la tolerancia de estos (Instituto Nacional de

Estándares y Tecnología, 2018) y las actividades de tratamiento en caso de que se llegasen a materializar.

1.2. Recolectar

Esta actividad hace referencia a la función detectar, en la cual se realiza la recolección de información mediante sistemas tecnológicos que han sido parametrizados y puestos en operación de acuerdo con la actividad anterior, los cuales se encargarán de recopilar información para la detección y anticipación de potenciales eventos de ciberseguridad y su posterior análisis por parte de los operadores y analistas del servicio (Blanco, 2018).

De igual forma, es de anotar que la actividad de recolectar se realizará a través del ciberespacio, con el fin de aportar elementos de información que confluyan en la web, prevenir y anticipar situaciones y fenómenos que puedan afectar el régimen democrático, constitucional y legal, la seguridad y defensa nacional.

Dentro de esta actividad se encuentran los siguientes elementos:

- **Anomalías y eventos:** en este elemento se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas, igualmente se recopilan los eventos detectados y se correlacionan con múltiples fuentes de información, estableciéndose su posible impacto y sus umbrales de alerta (Instituto Nacional de Estándares y Tecnología, 2018).

- **Monitoreo Continuo de la Seguridad:** se realiza el monitoreo del ciberespacio para anticipar, prevenir y detectar posibles eventos de ciberseguridad, amenazas y vulnerabilidades, así como fenómenos o conductas que promueven o incitan al delito o a la comisión de acciones que no se tipifican como tal, pero que de alguna forma afectan la seguridad y convivencia ciudadana, las cuales se gestan y replican haciendo el uso de las redes sociales.

  Actualmente la Policía Nacional cuenta con el CAI virtual y funcionarios que realizan ciber-patrullaje 24/7, apoyando esta última actividad en el software FOCALINFO; es de anotar que estas actividades serán incluidas en el modelo, pero sigue siendo necesario que la institución implemente nuevas fuentes de datos, ya sea mediante la adquisición de nuevas herramientas tecnológicas o convenios de cooperación con entidades públicas o privadas. Igualmente, el monitoreo realizado incluye el escaneo de vulnerabilidades, de código malicioso, entre otros factores, siendo necesario comunicar la información de los eventos detectados para su tratamiento y análisis (Instituto Nacional de Estándares y Tecnología, 2018).

- **Procesos de detección:** en este elemento se mantienen y se aprueban los procesos y procedimientos de detección para verificar el conocimiento de los eventos de ciberseguridad, que a su vez cumplen con los requisitos (Instituto Nacional de Estándares y Tecnología, 2018) para generar una anticipación y prevención efectiva.

1.3. Tratar

En esta actividad se realizan tareas de filtrado, evaluación, clasificación e integración de la información que ha sido recolectada. Teniendo en cuenta que el cumulo de información puede llegar a corresponder a BIG DATA, se requerirá herramientas tecnológicas que permitan a los

funcionarios que realicen esta actividad agilizar y sistematizar sus tareas. Es importante resaltar que hace parte de la función responder.

1.4. Analizar

Es la actividad principal de la función responder, teniendo en cuenta que se lleva a cabo el análisis de los eventos de ciberseguridad, para identificar su posible impacto y las medidas de anticipación, prevención a implementar, y en los casos que se materialice algún incidente se realiza un análisis forense (Instituto Nacional de Estándares y Tecnología, 2018) que permita identificar lecciones aprendidas. Igualmente, como actividad preventiva se definen las estrategias para responder a las vulnerabilidades o amenazas que puedan materializar algún tipo de riesgo.

Así mismo, se realiza el estudio e interpretación de la información, utilizando disciplinas que incrementan las capacidades del analista, ante las dificultades cuantitativas y cualitativas derivadas de la cantidad masiva de datos recolectados como son: análisis semántico, Big Data, minerías de datos, Machine Learning, algoritmos avanzados, ingeniería de sistemas de decisión, redes neuronales, entre otros (Blanco, 2018).

Es importante mencionar, que la Policía Nacional presenta un déficit en esta actividad porque no cuenta con los suficientes recursos tecnológicos y personal capacitado en temas de análisis de ciberinteligencia, puesto que como se ha descrito anteriormente todos los esfuerzos se centran en la investigación criminal, aunque los software que actualmente utilizan para el análisis de datos (ARBUTUS, IDEA y ACL) podrían ser incluidos dentro del modelo, no son suficientes para generar un correcto análisis, siendo necesario como primera medida, que la institución

adquiera sistemas de inteligencia artificial que permitan valorar y cuantificar a través de métodos probabilísticos múltiples tendencias de las variables; segundo, coordinar capacitaciones a los funcionarios policiales que serán responsables de ejecutar esta actividad; y tercero, establecer modelos matemáticos que permitan identificar el comportamiento individual y colectivo de las variables.

Igualmente, las actividades de análisis pueden apoyarse del Observatorio de Crímenes y Delitos en el Entorno Digital, como fuente de información para fortalecer la caracterización de fenómenos en el ciberespacio, debiendo la Policía Nacional, implementar conexiones cruzadas a datos de diversas fuentes en tiempo real, para que el analista o los sistemas que se implementen puedan tener mayor visión del ciberespacio.

1.5. Comunicar e Integrar

Los resultados del análisis son comunicados a los receptores de información de inteligencia quienes a partir de las conclusiones y recomendaciones deberán adoptar las medidas oportunas o necesarias (Blanco, 2018). Igualmente, se coordinan las actividades de anticipación, prevención o mitigación con los actores responsables de garantizar ciberseguridad en Colombia, respetando el principio de confidencialidad y reserva legal.

1.6. Evaluar y Retroalimentar

Esta actividad es transversal al ciclo de ciberinteligencia. Hace referencia a incorporar en las actividades mencionadas anteriormente lecciones aprendidas, procesos de recuperación y resultados obtenidos del análisis. Dentro de esta actividad, se llevan a cabo periódicamente

ejercicios para compartir conocimientos, mejorar la calidad de los entregables, disminuir los tiempos de respuesta y abordar oportunidades de mejora. Igualmente, se tratan las desviaciones con el objetivo de fortalecer y maximizar la eficiencia de las actividades (Blanco, 2018).

1.7. Proteger

Esta función aunque no es una actividad del ciclo, se incluirá en el modelo y hará referencia a las tareas de protección que se implementan en el marco del desarrollo de las actividades del ciberinteligencia, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información recolectada, tratada, analizada y difundida mediante las herramientas tecnológicas. Por ello, se gestiona y protegen los accesos físicos y la integridad de la red, se verifican las identidades y usuarios de los funcionarios a los sistemas tecnológicos y se aplican controles de seguridad de la información (Instituto Nacional de Estándares y Tecnología, 2018).

Es de anotar que la Policía Nacional actualmente tiene implementando el Sistema de Gestión de Seguridad de la Información soportado en la norma técnica ISO 27001/2013. Así mismo, este componente incluye el elemento de concientización y capacitación del personal y los actores del modelo de ciberinteligencia, quienes son capacitados para cumplir con sus deberes y responsabilidades, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.

Por lo anterior, en la Figura 25, se presenta el ciclo de ciberinteligencia propuesto por este trabajo, con la inclusión de elementos de ciberseguridad, requeridos para la definición del modelo de ciberinteligencia.

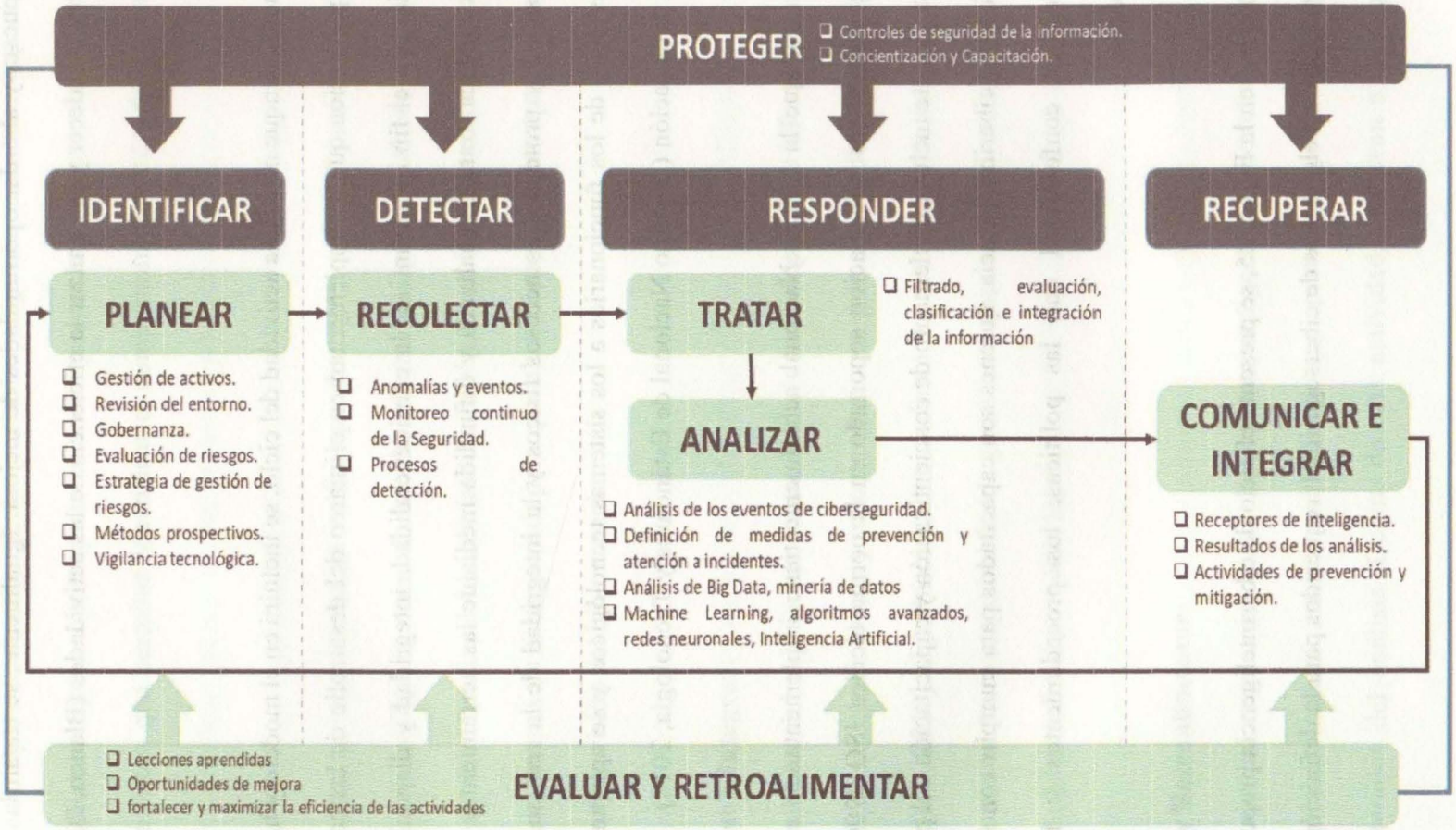


Figura 25. Inclusión de ciberseguridad en el ciclo de inteligencia. Fuente: elaboración propia a partir de la información descrita en el Manual de Inteligencia de la Policía Nacional (2014) y el Marco de Seguridad NIST (2018)

2. Identificación de entradas y salidas del modelo de ciberinteligencia.

En la sección anterior, se identificaron las actividades y elementos que componen el ciclo de ciberinteligencia policial, con los cuales se proyecta realizar la recolección, tratamiento, análisis y difusión de información, aunque no se incluyeron los componentes de entrada y salida que permiten fortalecer el modelo, por lo cual a continuación se realizará una presentación y descripción de estos.

Inicialmente, se identificaron dos componentes de entrada: tecnología y talento humano, los cuales impactan directamente en las actividades del ciclo de ciberinteligencia al mejorar su eficiencia y efectividad:

2.1. Tecnología

Este componente de entrada tiene como propósito, ayudar en el desarrollo y despliegue de herramientas y tecnología necesaria para garantizar que el desarrollo de las actividades del ciclo de ciberinteligencia se mantenga a la vanguardia y al día, de tal forma que puedan responder a los cambios constantes de las ciberamenazas.

Como valor agregado, se proyecta que la institución realice vigilancia tecnológica para identificar no solo los avances tecnológicos en temas de ciber, sino también la tecnología usada o que podría ser utilizada por los cibercriminales, de tal forma que se prevean medidas de contención, tratamiento, y respuesta a los riesgos que se lleguen a materializar.

Este componente, puede considerarse el motor tecnológico del modelo de ciberinteligencia, teniendo en cuenta que será donde se garantice la implementación, soporte y mantenimiento de los sistemas que se implementen, verificando de igual forma que estos se adapten a las actividades y contribuyan a mejorar la efectividad en la ejecución de estas.

2.2. Talento humano

Este componente hace referencia a fortalecer la capacitación de los funcionarios que harán parte del modelo y desarrollarán alguna de las actividades descritas en el ciclo de ciberinteligencia, siendo necesario que cuenten con los conocimientos, aptitudes y habilidades para poder entender las actuales ciberamenazas y sepan como contrarrestarlas (Blanco, 2018).

Aunando a lo anterior, la Policía Nacional requiere establecer un plan de carrera, que considere la formación precisa y las condiciones para conservar la curva de aprendizaje que permita a los funcionarios adquirir las capacidades para desarrollar la recolección, tratamiento y análisis de información de ciberinteligencia y la generación de nuevo conocimiento, aún más porque se incluirá la administración de herramientas tecnológicas y de cantidades masivas de datos (Big Data). Por otra parte como componentes de salida se tienen los resultados operativos y las lecciones aprendidas, que también son considerados de entrada al impactar las actividades del ciclo de ciberinteligencia.

2.3. Resultados operativos

Hacen referencia, a los resultados obtenidos al pasar los datos recolectados por el ciclo de ciberinteligencia, los cuales pueden convertirse en entradas como soporte de nuevas actividades de recolección. Asimismo, apoya el componente de la estrategia, que a partir de estos resultados

puede generar modificaciones en la misma. Los resultados operativos, permitirán generar un banco de conocimiento del cual se alimentará el ciclo de ciberinteligencia para generar análisis comparativos y garantizar la mejora continua.

2.4. Lecciones aprendidas

Dentro del modelo se considera el componente clave para generar la mejora continua y conocimiento, ya que las lecciones aprendidas que se obtengan de los resultados del procesamiento de información mediante el ciclo de ciberinteligencia, permitirán identificar desviaciones y oportunidades de mejorar que generaran que el modelo madure y se adapte a las nuevas ciberamenazas y tecnologías emergentes. Como componentes transversales que impactan todo el modelo de ciberinteligencia, se identificaron la estrategia, la cooperación con otras entidades y la articulación entre las unidades de la Policía Nacional de Colombia.

2.5. Estrategia

Como se observó en la identificación de capacidades de la Policía Nacional, esta institución cuenta con la Estrategia Integral de Ciberseguridad, mediante la cual realiza la coordinación y asigna responsabilidades a todas sus unidades, en torno a actividades relacionadas con la gestión de ciberseguridad, al ser la institución designada para esto.

Por lo anterior, se hace necesario que dentro de la ESCIB, se incorporen elementos de ciberinteligencia como capacidad para generar ciberseguridad, la cual conforme a la Ley 1621 de 2013 debe ser liderara por la Dirección de Inteligencia Policial, al ser la única unidad de la PONAL que cuenta con la función de inteligencia.

2.6. Cooperación con otras entidades

Dentro del modelo, la cooperación no es considerada opcional, teniendo en cuenta que todas las medidas no son suficientes sin la posibilidad de compartir información entre las distintas organizaciones, generando confianza mutua y utilizando herramientas comunes que mejoren el conocimiento de las amenazas y de los ataques (Candau, 2017).

Aunado lo anterior, al existir un mayor grado de relación entre las entidades públicas o privadas de carácter nacional o internacional con la Policía Nacional de Colombia, permitirá implementar acciones conjuntas, desarrollar proyectos de investigación, organizar jornadas y talleres, coordinar grupos de expertos para debate, intercambiar buenas prácticas, entre otras (Blanco, 2018). Asimismo, la cooperación permitirá ampliar las fuentes de información que impactarán directamente en las actividades de recolección y análisis que tanto requieren poder tener acceso a datos privilegiados, para mejorar sus capacidades de detección y respuesta.

2.7. Articulación entre unidades

Actualmente las capacidades de ciberseguridad de la Policía Nacional de Colombia se encuentran distribuidas en las diferentes unidades, por lo cual, se hace necesario generar articulación entre las mismas de tal forma que todas aporten e interactúen de forma dinámica en el modelo de ciberinteligencia, por ejemplo, como fuentes de información o analistas de los fenómenos conforme a su misionalidad.

Con base a lo anterior y a partir del ciclo relacionado en la Figura 25, se presenta el modelo de ciberinteligencia para la Policía Nacional de Colombia descrito en la Figura 26, con el cual se proyecta que esta institución gestione las actividades de ciberinteligencia en el ciberespacio, como una capacidad adicional para fortalecer la ciberseguridad del País.

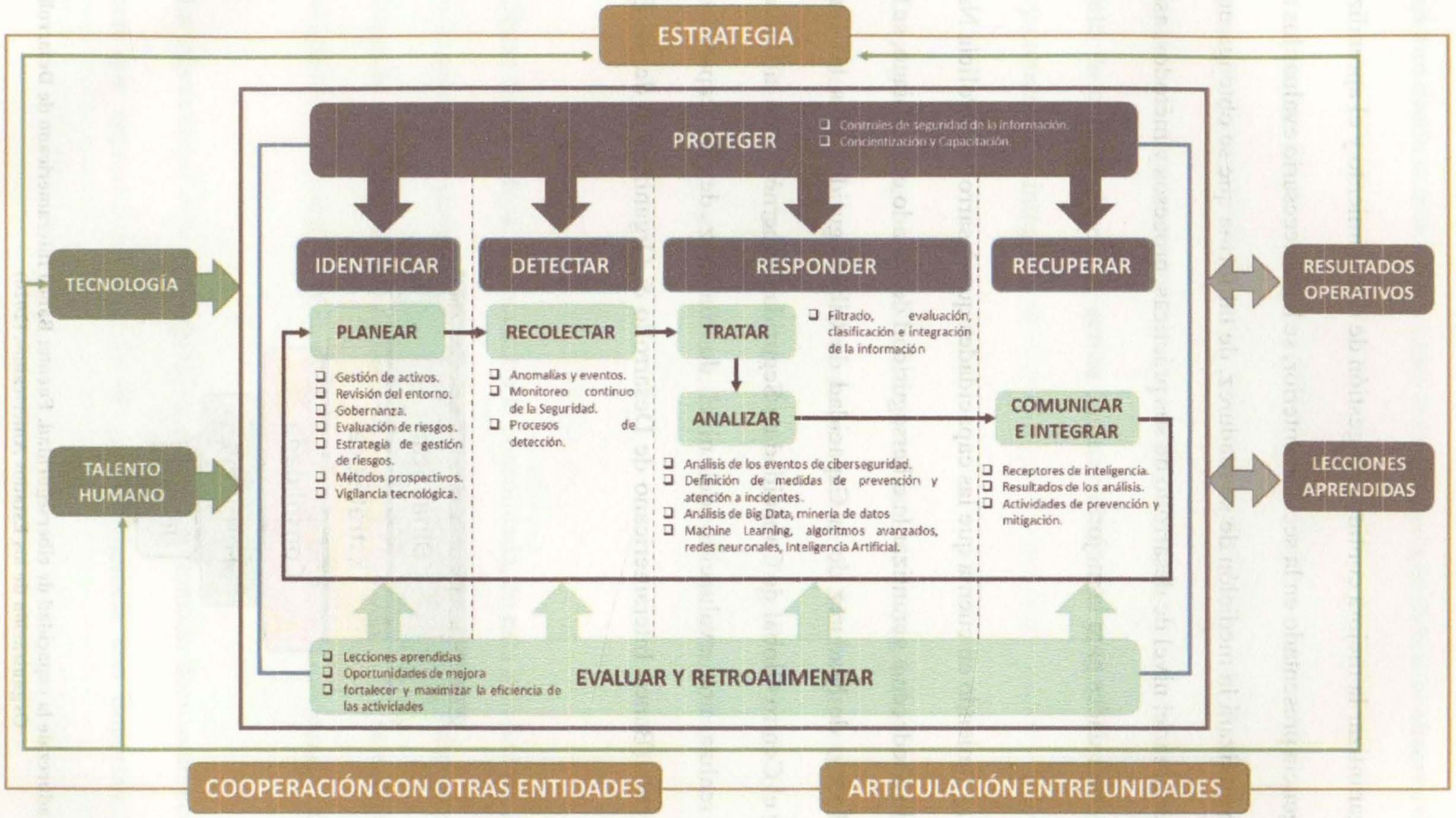


Figura 26. Modelo de ciberinteligencia soportado en el Ciclo de Inteligencia Policial. Fuente: elaboración propia a partir de la información descrita en el Manual de Inteligencia de la Policía Nacional (2014) y el Marco de Seguridad NIST (2018)

3. Línea de madurez del modelo de ciberinteligencia.

Con el fin de garantizar la mejora continua, la gestión de conocimiento y el aprendizaje del modelo de ciberinteligencia presentado en la sección anterior, se hace necesario evaluar los niveles mediante los cuales se realizará la medición de su madurez, de tal forma que se obtenga un punto de referencia para determinar el nivel de desarrollo de sus prácticas, procesos y métodos, así como establecer objetivos y prioridades para la mejora.

Por lo anterior, y teniendo en cuenta que las capacidades que desarrolla la Policía Nacional en torno al ciberespacio obedecen a garantizar la ciberseguridad del estado colombiano, se tomará como referencia el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) propuesto por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford, el cual realiza una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

Figura 27. Etapas de madurez de la capacidad de ciberseguridad. Fuente: Banco Interamericano de Desarrollo & Organización de los Estados Americanos, (2020)

Este modelo plantea cinco etapas: inicial, formativa, consolidada, estratégica y dinámica, las cuales van desde la más básica hasta la más avanzada, como se observa en la Figura 27.

La primera etapa se conoce como inicial, en esta no existe ningún tipo de madurez, pero puede presentarse discusiones sobre el desarrollo de capacidades de ciberseguridad (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020), que para el caso de modelo de ciberinteligencia, serían las actividades de planeación, recolección, tratamiento, análisis y comunicar e integrar.

La segunda etapa es la formativa, en esta se puede haber comenzado a formular las capacidades de ciberinteligencia, pero se encuentran de forma descentralizada, desorganizada, o son nuevas (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020) y todavía no cuentan con el suficiente desarrollo para impactar en el fortalecimiento de la ciberseguridad.

Como tercera etapa, se encuentra la consolidada, en esta a se han tomado las decisiones de incluir indicadores que permitan medir el desempeño del modelo de ciberinteligencia, pero aún no se han asignado recursos, aunque se considera que ya es funcional y se encuentra definido (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

La cuarta etapa es la estratégica, en esta se han tomado decisiones sobre los indicadores y se definen que aspectos del modelo de ciberinteligencia son importantes para fortalecer la

ciberseguridad del estado, reflejándose de que las elecciones se encuentran supeditadas a este factor (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

Como última etapa se encuentra la dinámica, en la cual ya existen mecanismos claros para alterar el modelo de ciberinteligencia en función de la sofisticación tecnológica del entorno de amenazas, el conflicto global, los cambios significativos en temas de delitos informáticos y las amenazas en el ciberespacio, siendo las principales características de esta etapa la rápida toma de decisiones, la asignación de recursos y el amplio conocimiento de los fenómenos que se presentan en el ciberespacio (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

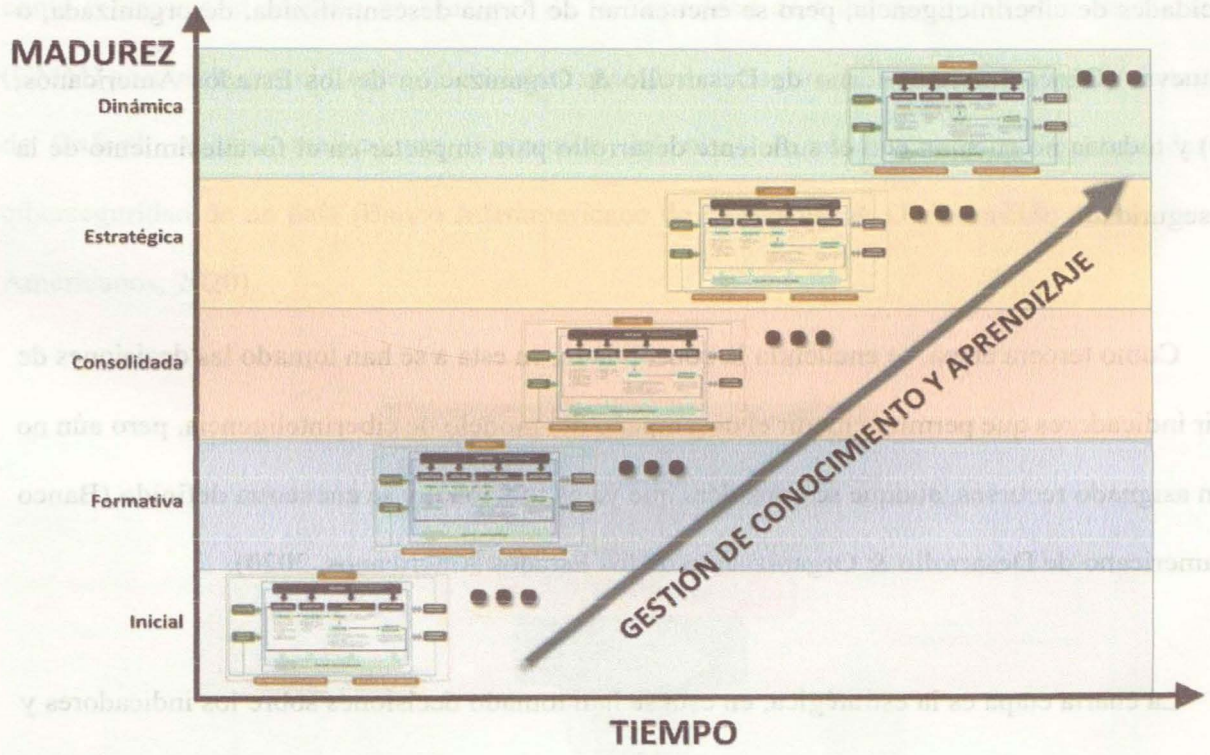


Figura 28. Etapas de la medición de la madurez de modelo de ciberinteligencia. Fuente: Elaboración propia a partir de la información descrita en el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

Con base a lo anterior, en la Figura 28 se presenta la relación gráfica de cómo se realizaría la medición de la madurez del modelo en relación con tiempo de implementación y las etapas descritas previamente.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Teniendo en cuenta que dentro de la investigación se definió utilizar el Ciclo de Inteligencia Policial como base para la propuesta del modelo de ciberinteligencia, se proyecta para su despliegue aplicar la guía 1DS-GU-0004 "Gestión del cambio institucional en la Policía Nacional", utilizado por la institución para identificar, planificar, ejecutar y controlar de forma oportuna aquellos cambios que puedan afectar el cumplimiento de los objetivos estratégicos de la Policía Nacional y de forma estructural los componentes o elementos específicos del Sistema de Gestión Integral de la Institución (Policía Nacional de Colombia, 2019), permitiendo de esta forma establecer la hoja de ruta para incluir en la Estrategia Integral de Ciberseguridad y el Ciclo de Inteligencia todos los elementos identificados en el presente trabajo como valor agregado.

- A partir del desarrollo del presente trabajo se logró evidenciar que el ciclo de inteligencia puede ser utilizando como base para la definición del modelo de ciberinteligencia, el cual debe incluir también capacidades de ciberseguridad para fortalecer sus actividades y adaptarse a las características propias del ciberespacio: 1) rapidez en la elaboración, debido al corto espacio de tiempo en el que esta información es válida y 2) utilización en gran medida de fuentes técnicas, aunque la obtención de fuentes humanas sigue teniendo un valor trascendental.

- Se evidenció en el desarrollo del presente trabajo, que la Policía Nacional realiza actividades de ciberseguridad que se orientan a la investigación judicial, haciéndose necesario fortalecer la prevención y anticipación de ciberamenazas y la conceptualización de fenómenos que se presentan en el ciberespacio, a partir de la implementación de capacidades de recolección, tratamiento, análisis y difusión de información desde el rol de inteligencia.

- El análisis de las capacidades de ciberseguridad de la Policía Nacional permitió identificar que la institución se centra en realizar actividades de coordinación con otras entidades y entre sus mismas unidades, con el objeto de fortalecer sus capacidades y dar respuesta a los incidentes cibernéticos que se asocian a delitos informáticos.

- A partir de la conceptualización de marcos de ciberseguridad como NIST, ISO 27032 y la ISO 27001/2013, aunado al proceso de ciberinteligencia propuesto por Blanco (2018) se logró evidenciar que los componentes del Marco de Ciberseguridad NIST presentan similitudes con las actividades del ciclo de inteligencia, permitiendo a partir de la unión de funciones como la detección con las actividades de planificación y recolección, y respuesta con la difusión, establecer un ciclo de ciberinteligencia, el cual requiere adicionalmente la inclusión de Tecnologías de la Información y Comunicación, que permitan parametrizar y automatizar la obtención y monitorización de la información, así como el análisis mediante la implementación de herramientas de Inteligencia de Negocios, de tal forma que se definan los cursos de acción para mitigar, recuperar, prevenir o anticipar fenómenos que afectan la ciberseguridad de las personas.

- Con base al análisis comparativo entre los componentes del proceso de ciberinteligencia propuesto Blanco (2018), la Estrategia Integral de Ciberseguridad, las unidades que tienen responsabilidad en su despliegue como DIJIN, DIPRO, DIPOL, DIASE, DIPRO, DINAE, COEST, ASUIN, OFITE, CSIRT, CCP y C4 y las iniciativas de tipo tecnológico, estratégico (documentos CONPES, las directicas operativas y resoluciones de estructura orgánica) y de gestión, que conforman a su vez el ecosistema de ciberseguridad de la Policía Nacional, se logró establecer que esta institución cuenta con capacidades de "detección" (ciber-patrullaje y análisis de fuentes abiertas, sistema de gestión de incidentes, CAI virtual), "análisis" (Centro de Fusión para la investigación de Crímenes Económicos y financieros y el Observatorio de crímenes y los delitos en el entorno digital) y "respuesta" las cuales se centran en la investigación y judicialización mediante la utilización de herramientas sandbox, software de correlacionador de eventos, equipos de detección electrónica de dispositivos, software para de análisis de datos y solución forense para dispositivos móviles, las cuales pueden ser incluidas en el modelo de ciberinteligencia. Por otra parte, se evidenció que era necesario incluir también un componente de coordinación en atención a la cooperación que realiza la Policía con otras entidades y articulación entre sus propias unidades para el despliegue de la estrategia; asimismo, se definió que desde el rol de inteligencia se deben implementar actividades relacionadas con la gestión de activos, revisión del entorno, evaluación de riesgos, métodos prospectivos, vigilancia tecnológica y análisis de eventos de ciberseguridad mediante minería de datos, Machine Learning, redes neuronales e inteligencia artificial, que permitan generar una compresión mayor de fenómenos diferentes a los asociados con delitos informáticos y fortalecer la prevención y anticipación de amenazas.

- La redefinición del ciclo de inteligencia policial a partir de la inclusión de funciones del marco de ciberseguridad NIST para la conceptualización del modelo de ciberinteligencia, permitió establecer actividades y capacidades de detección, respuesta y recuperación, que sumadas a las actividades de planeación, recolección, tratamiento, análisis y difusión establecidas en ciclo tradicional, atienden a las necesidades que tiene la Policía para generar mecanismos de anticipación y prevención de amenazas y fenómenos que se presentan en el ciberespacio, las cuales requirieron también, la vinculación de un componente de protección que se orientó a la implementación de controles de seguridad de la información para garantizar la reserva legal dispuesta en la Ley 1621 de 2013. Asimismo, en atención a la Estrategia Integral de Ciberseguridad ya definida por la Policía Nacional de Colombia, dentro del modelo se incluyeron componentes de cooperación con otras entidades homólogas (INTERPOL, el FBI, la DEA, el EC3, AMERIPOL, KOICA, NCA, GLDTA y ATA) y articulación entre unidades de la misma institución, que responden a su respectiva misionalidad, lo cual ayuda a que desde la adquisición de tecnologías de información para el desarrollo de las actividades del modelo y la capacitación del personal, se puedan obtener resultados operativos que se orienten a la misionalidad y la función de inteligencia los cuales se fortalecen desde la identificación y aplicación de las lecciones aprendidas.

Recomendaciones

- Se recomienda que la Policía Nacional establezca un inventario de activos de información, los cuales deben ser considerados dependiendo si tiene o no valor en la generación de ciberseguridad, como es el caso de las plataformas de redes sociales, sistemas de entidades

públicas y demás sitios de internet en los cuales las personas desarrollan algún tipo de actividad socioeconómica.

- Teniendo en cuenta que el fortalecimiento del Talento Humano en temas de ciberseguridad es necesario, se recomienda que la Policía Nacional coordine con las universidades la inclusión de programas de formación que se orienten a la misionalidad de la institución y en los cuales participen los funcionarios que tengan asignada algún tipo de responsabilidad o función frente a ciberseguridad.

- Se recomienda que las actividades de ciberinteligencia se hagan a partir de los resultados obtenidos de una evaluación de riesgos de los activos de información, que permita orientar la recolección y análisis de información hacia la identificación de amenazas y vulnerabilidades.

- Para medir el nivel de madurez del modelo de ciberinteligencia, se recomienda utilizar el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) propuesto por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford, ya que este mide el nivel de madurez de las capacidades de ciberseguridad de un país y esto obedece al rol de la Policía Nacional de garantizar la ciberseguridad del estado colombiano.

BIBLIOGRAFÍA

Agencia Central de Inteligencia. (2013). *The Intelligence Cycle*. https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html#planning-and-direction

Arrojo, M. J. (2015). Los contenidos transmedia y la renovación de formatos periodísticos: la creatividad en el diseño de nuevas propuestas informativas. *Palabra Clave*, *18*(3), 746–787. https://doi.org/10.5294/pacla.2015.18.3.6

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. 204. https://doi.org/http://dx.doi.org/10.18235/0002513

Blanco, C. T. (2017). Potenciando la dimesión proactiva de la ciberinteligencia. *Red Seguridad. Revista Especializada En Seguridad de La Información*, *1695–3991*, 60–61. http://www.redseguridad.com/revistas/red/079/3/#zoom=z

Blanco, J. M. N. (2018). Ciberinteligencia, la vía para la ciberseguridad. *Cuadernos de La Guardia Civil. Revista De Seguridad Pública*, *57*, 6–30. https://biblioteca.guardiacivil.es/cgi-bin/koha/opac-detail.pl?biblionumber=21499

Bradshaw, S., & Howard, P. N. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6/download_file?file_format=pdf&safe_filename=Troops-Trolls-and-Troublemakers.pdf&type_of_work=Report

Bradshaw, S., & Howard, P. N. (2019). *EL orden global de la desinformación inventario global de la manipulación organizada en redes sociales 2019*.

http://www.apoyocomunicacion.com/repositorio/boletin/periodistas/2019/Orden-Global-OXFORD.pdf

Cámara Colombiana de Informática y Telecomunicaciones, & Policía Nacional de Colombia. (2019). *Tendencias Cibercrimen Colombia 2019 - 2020.* https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Candau, J. (2017). Ciberinteligencia, complemento perfecto para la ciberseguridad. *Red Seguridad. Revista Especializada En Seguridad de La Información*, 52–56. http://www.redseguridad.com/revistas/red/079/3/#zoom=z

Cardoso, R y Rozo, L. (2011). *Una renovada producción de inteligencia estratégica y anticipativa para la seguridad de los colombianos* (Policía Nacional de Colombia (Ed.)). https://issuu.com/esdeguecol/docs/218

Carnegie Mellon University. (2013). SEI Emerging Technology Center : Cyber Intelligence Tradecraft Project. Summary of Key Findings Authors. *Carnegie Mellon University, January789*, 22.

Casabona, C. M. R. (2006). *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales* (2006 Granada: Comares (Ed.)).

Centro Nacional de Inteligencia. (2015). *El Ciclo de Inteligencia.* https://www.cni.es/es/queescni/ciclo/

Centro Nacional de Inteligencia de Mexico. (2020). *Ciclo de Inteligencia.* https://www.gob.mx/cms/uploads/attachment/file/535136/Ciclo_Inteligencia.pdf

Cepik, M., & Antunes, P. (2004). Professionalization of intelligence activity in Brazil: criteria, evidence and remaining challenges. In Joint Military Intelligence College (Ed.), *Profesionalismo de Inteligencia en las Américas* (p. 566).

https://books.google.com.co/books?id=K06HAAAAMAAJ&hl=es

CESDEN (Ed.). (2012). *Monografía 126 "El Ciberespacio. Nuevo Escenario de Confrontación."*

Cline, R. S., Berkowitz, B. D., & Goodman, A. E. (1989). Strategic Intelligence for American National Security. *Political Science Quarterly*. https://doi.org/10.2307/2151109

Comisión de Regulación de Comunicaciones. (2009). *RESOLUCIÓN 2258 DE 2009 - "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".* 4–9. http://legal.legis.com.co/document/Index?obra=legcol&document=legcol_76d551c6723f602ce0430a010151602c

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 infor. 2009*(4). http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República. (2013). *Ley Estatutaria 1621 "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras di.*

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*. 26. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Constitución Política de Colombia. (1991). Constitución de Colombia de 1991. *Congreso de La República de Colombia.*

Corte Constitucional. (2005). *Sentencia C-1194.* https://www.corteconstitucional.gov.co/relatoria/2005/C-1194-05.htm

Corte Constitucional. (2012). *Sentencia C-540.* https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

Cortés, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. In *Revista de Derecho Comunicaciones y Nuevas Tecnologías.* https://dialnet.unirioja.es/servlet/articulo?codigo=7496888

Departamento Nacional de Seguridad de España. (2013). *Estrategia de Seguridad Nacional.* Departamento Nacional de Seguridad de España. http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

Ejercito Nacional de Colombia. (2016). *RESOLUCIÓN NÚMERO 01649 DE 2016 Por la cual se aprueba el "MANUAL FUNDAMENTAL DEL EJÉRCITO INTELIGENCIA."* https://www.cemil.mil.co/centro_educacion_militar/examenes_competencia/manuales_fundamentales_ejercito/mfe_2_0_inteligencia_407445

Ejercito Nacional de Colombia. (2017). *Manual Fundamental de Referencia del Ejercito.* https://www.cedoe.mil.co/centro_doctrina_ejercito_nacional_colombia/doctrina/manuales_fundamentales_referencia_458641/mfre_2_0_inteligencia

Fojón, J. E., & Sanz, A. F. V. (2010). Ciberseguridad en España: una propuesta para su gestión. *Boletín Real Instituto Elcano*, *126*, 8. https://core.ac.uk/download/pdf/42966556.pdf

Gallegos, R. (2007). *Tecnologías apropiadas de la comunicación.*

Gastón Sack, P., & Ierache, J. S. (2015). *Controles de seguridad propuesta inicial de un framework en el contexto de la ciberdefensa. 1*, 1–11.

http://sedici.unlp.edu.ar/handle/10915/50588

Gertrudis Casado, M., Gértrudix Barrio, M., & Álvarez García, S. (2016). Competencias informativas profesionales y datos abiertos: Retos para el empoderamiento ciudadano y el cambio social. *Comunicar: Revista Científica Iberoamericana de Comunicación y Educación*, *47*, 39–47.

Herman, M. (1996). *Intelligence Power in Peace and War* (Cambridge University Press (Ed.)). https://books.google.com.co/books/about/Intelligence_Power_in_Peace_and_War.html?id=zb0LAQAAQBAJ&redir_esc=y

Hernández, R. S., Fernández, C. C., & Baptista, M. del P. L. (2014). *Metodología de la Investigación* (6th ed.).

Hilsman, R. (1952). Intelligence and Policy-making in Foreign Affairs. *World Politics*.

Holzmann, P. G., & Gallardo, C. M. (1997). La función del sistema nacional de inteligencia en un estado democrático. *Política. Revista de Ciencia Política*, *35*, 97–130. https://revistapolitica.uchile.cl/index.php/RP/article/view/55040

INSA. (2015). *CiberInteligencia: Preparando el talento de hoy para las amenazas del mañana*. 20. https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf

Instituto Nacional de Estándares y Tecnología. (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas*. https://doi.org/10.6028/NIST.CSWP.04162018

Instituto Nacional de Normas Técnicas y Certificación - ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requsitos.*

International Organization for Standardization - ISO. (2012). *International Standard ISO/IEC*

27032. Information technology - Security techniques - Guidelines for cybersecurity. 2008, 58.

Jimenez, R. V. (2018). Tipos de Inteligencia | Global Strategy - Universidad de Granada. *Centro Nacional de Inteligencia y Seguridad Internacional de La Universidad de Granada.*, 1–22. https://global-strategy.org/tipos-de-inteligencia/

Joint Chiefs of Staff. (2013). Joint Intelligence 2.0. *U.S. Defense Planning*, *October*, 144. https://doi.org/10.4324/9780429269684-7

Kent, S. (1986). *Inteligencia estratégica: para la política mundial norteamericana* (1986 Pleamar (Ed.); 4th ed.).

Kornmaier, A., & Jaouen, F. (2014). Beyond technical data-a more comprehensive situational awareness fed by available intelligence information. *International Conference on Cyber Conflict, CYCON*. https://doi.org/10.1109/CYCON.2014.6916400

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingenieria de Software*, *3*(4), 161. https://doi.org/10.18294/relais.2015.161-176

Loubet del Bayle, J. L. (1992). *La police. Approche socio-politique* (Montchrestien Colección Clefs Politiques (Ed.); 1st ed.).

Lowenthal, M. M. (1992). Tribal tongues: Intelligence consumers, intelligence producers. *Washington Quarterly*, 157–168. https://doi.org/10.1080/01636609209550084

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy* (CQ Press (Ed.); 5th ed.). https://books.google.com.co/books/about/Intelligence_From_Secrets_to_Policy.html?id=xNBbYNt3JJ0C&redir_esc=y

Martin, E. I. (2016). Los retos de la ciberinteligencia. *Cuadernos de La Guarcia Civil: Revista de*

Seguridad Pública, *53*, 53–67. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2016/GC_Cuadernos_Num.53-2016.pdf#page=78%0Ahttp://www.intervencionoperativapolicial.com/doc/CUADERNOS GC N 52 2016.pdf#page=155

Measuring the information society report. Vol. 2. (2018). In *ITU Publications* (Vol. 2). https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf

Meyrowitz, J. (2008). Nómades globales en la llanura digital. *Revista Chilena de Comunicación*, *8*(9), 105–115.

Ministerio de Defensa Nacional. (2019). Política marco de convivencia y seguridad ciudadana. In *Ministerio de defensa nacional*. https://id.presidencia.gov.co/Documents/191220-Politica-Marco-Convivencia-Seguridad-Ciudadana.pdf

Ministerio de Interior y de Justicia, Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de Seguridad, Departamento Nacional de Planeación, & Fiscalía General. (2011). CONPES 3701 - Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. *Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación*, 43. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Dirección Nacional de Inteligencia, & Departamento Nacional de Planeación. (2016). CONPES 3854 - Política Nacional de Seguridad Digital. *Consejo Nacional De*

Política Económica Y Social República De Colombia Departamento Nacional De Planeación.

Mintzberg, H., Ahlstrand, B. W., Ahlstrand, B., & Lampel, J. (2005). *Strategy Bites Back: It is a Lot More, and Less, Than You Ever Imagined.* Pearson Education.

Miró, L. F. (2011). La oportunidad en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, *07*, 13–17. http://criminet.ugr.es/recpc

Navarro, D. B. (2004). El ciclo de inteligencia y sus límites. *Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol*, *48*, 51–66.

Navarro, D. B., & Velasco, F. (2009). *EL ALMA DE LA VICTORIA: Estudios sobre inteligencia estratégica* (P. y Valdés (Ed.)).

Office of the Director of National Intelligence. (2014). *The National Intelligence Strategy of the United States of America 2014*. 24. https://www.dni.gov/files/documents/2014_NIS_Publication.pdf

Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. Á. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *Revista Iberoamericana Para La Investigación y El Desarrollo Educativo*, *8*(16), 847–870. https://doi.org/10.23913/ride.v8i16.371

Policia Nacional de Colombia. (1999). *Reflexiones de Inteligencia 5. El análisis en el marco de la inteligencia y el conocimiento* (Policía Nacional de Colombia (Ed.)).

Policia Nacional de Colombia. (2013). *Resolución No. 02536 del 08 de julio de 2013 "Por la cual se define la estrucutura orgánica interna de la Oficina de Telemática, se determinan*

sus funciones y se derogan unas disposiciones" (p. 14).

Policia Nacional de Colombia. (2015). *Resolución 05839 del 31 de diciembre de 2015 "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"* (p. 43).

Policía Nacional de Colombia. (1992). *Resolución No. 10033 del 13 noviembre de 1992 "por la cual se expide el Manual de Inteligencia para la Policía Nacional y se deroga la resolución 8513 de 1989."*

Policía Nacional de Colombia. (2005). *Resolución No 00199, Manual de Inteligencia.*

Policía Nacional de Colombia. (2014). *Resolución No. 01446 del 16 de abril de 2014 "Manual de Inteligencia y Contrainteligencia para la Dirección de Inteligencia de la Policía Nacional."*

Policía Nacional de Colombia. (2017). *Balance Cibercrimen en Colombia 2017.* https://caivirtual.policia.gov.co/contenido/informe-balance-del-cibercrimen-2017

Policía Nacional de Colombia. (2018). *Análisis del Estado de la Ciberseguridad.* 18. https://ratsel.com.co/wp-content/uploads/2019/07/Análisis-del-Estado-de-la-Ciberseguridad-en-Colombia-2018-2.pdf

Policía Nacional de Colombia. (2019). *Directiva Operativa Transitoria No. 038 / DIPON - DIJIN "Parámetros de actuación Policial para el despliegue de la Estrategia Integral de Ciberseguridad."*

Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the high ground. *International Conference on Cyber Conflict, CYCON.* https://doi.org/10.1109/CYCON.2014.6916409

Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen : particularidades en su investigación y enjuiciamiento. *UOC -Universitat Oberta de Catalunya*, 209–234. http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Real Acedemia de la lengua. (2014). *Diccionario de la lengua española.* https://dle.rae.es/?w=inteligencia

Rodríguez, G., Gil, J., & García, E. (1996). Tradición y enfoques en la investigación cualitativa. In *Metología de la investigación cualitativa*. http://www.albertomayol.cl/wp-content/uploads/2014/03/Rodriguez-Gil-y-Garcia-Metodologia-Investigacion-Cualitativa-Caps-1-y-2.pdf

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal. *Cibercrimen y Delitos Informáticos: Los Nuevos Tipos Penales En La Era de Internet*, 7–32. http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Sainz de la Peña, J. A. (2012). Inteligencia Táctica. *Revista UNISCI, (28)*, 213–232. https://revistas.ucm.es/index.php/UNIS/article/download/38473/37212

Sancho, C. H. (2017). Ciberseguridad. Presentación del dossier. *Revista Latinoamericana de Estudios de Seguridad*, 16. http://hdl.handle.net/10469/12197

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. *Cibercrimen y Delitos Informáticos: Los Nuevos Tipos Penales En La Era de Internet*, 49–68. http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Unión Internacional de Telecomunicaciones. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. *Unión Internacional de Telecomunicaciones*, *1205*, 66.

Uribe, J. E. (2016). El cambio mediático de la televisión: Netflix y la televisión en teléfonos

inteligentes. *Revista Palabra Clave*, *19*(2), 358–364. https://doi.org/10.5294/pacla.2016.19.2.1

Velasco, F., Bonilla, D. N., & Martín, R. A. (2010). *Introducción: convergencia disciplinar y diversidad como necesidad en los estudios de Inteligencia* (Ministerio de Defensa; Plaza y Valdés (Ed.)).

Villalba, A. F., & Corchado, J. M. R. (2017). Análisis de las ciberamenazas. *Cuadernos de Estrategia*, *185*, 97–138. https://dialnet.unirioja.es/servlet/articulo?codigo=6115622

Yar, M. (2006). Cybercrime and society. In *Cybercrime and Society*. https://doi.org/10.4135/9781446212196

ANEXOS

Un CD el cual contiene la copia virtual en formato PDF de la presente monografía.