CAPÍTULO I

LA CIBERSEGURIDAD Y LA CIBERDEFENSA, LA NECESIDAD DE GENERAR ESTRATEGIAS DE INVESTIGACIÓN SOBRE LAS TEMÁTICAS QUE AFECTAN LA SEGURIDAD Y DEFENSA DEL ESTADO*

Marco Emilio Sánchez Acevedo

* Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto"de la República de Colombia.

1. La investigación como elemento esencial de la política de seguridad digital en Colombia

1.1. La política de seguridad digital colombiana – estructuración desde el entendimiento gráfico

Es pertinente abordar como punto inicial, el objetivo general del contenido en el (numeral 5.1.) del documento *CONPES de seguridad Digital 3854 de 2016*, en el que se señala como tal "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad Digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia". En este sentido, la Política Nacional que se genera, parte de la aceptación de las recomendaciones dadas por la OCDE a fin de que se creen condiciones para la participación de las múltiples partes interesadas, en palabras de la OCDE:

> (I) estar apoyada desde el más alto nivel de gobierno; (II) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social; (III) estar dirigida a todas las partes interesadas; y (IV) ser el resultado de un enfoque intragubernamental, coordinado, abierto y transparente, donde participen las múltiples partes interesadas (OCDE, 2015),

Tal y como se ha señalado en investigaciones anteriores[1], el documento *CONPES de seguridad Digital* establece que es necesario reforzar

1 Véase Sánchez Acevedo, M.E. (2018). Estrategia Jurídica para la Gestión, Análisis y ciberseguridad de la Información en la Investigación Penal. *Tesis de maestría*. Bogotá: Escuela Superior de Guerra "General Rafael Reyes Prieto".

las capacidades de ciberseguridad con un enfoque de Gestión de Riesgos, así como reforzar las de Ciberdefensa bajo este mismo; también se determina que los esfuerzos de cooperación, colaboración y asistencia, nacionales e internacionales, relacionados con la seguridad Digital, son insuficientes y desarticulados. Ante este panorama se plantea una nueva política, cuyo objetivo general es:

> 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. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (CONPES, 2016, p 47)

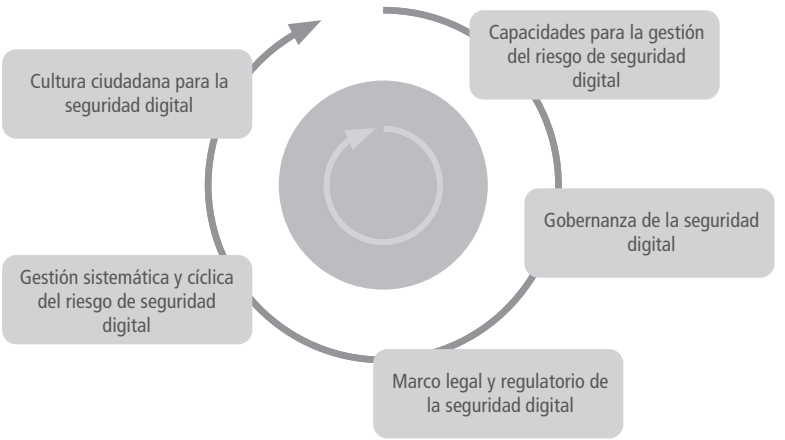
Es precisamente por ello que la política trazada por el documento *CONPES 3854 de 2016* está determinada de la siguiente manera.

Figura 2. Política trazada por el documento CONPES 3854 de 2016

Fuente: Elaboración Propia a partir del documento CONPES 3854 de 2016

Las cinco dimensiones estratégicas sobre las que se adopta el enfoque que garantice la seguridad Digital desde la participación de las múltiples partes interesadas se define de la siguiente manera gráfica para mayor comprensión.

Figura 3. Las cinco dimensiones estratégicas del documento CONPES 3854 de 2016



Fuente: Elaboración propia partir del documento CONPES 3854 de 2016

Estas dimensiones estratégicas han establecido un conjunto de acciones tendientes al desarrollo en los siguientes términos:

a. Dimensión estratégica 1. Establecer un marco institucional para la seguridad digital consistente con un enfoque de Gestión de Riesgos.

Entre los elementos destacables del documento CONPES en referencia está la creación de la figura de coordinador nacional de seguridad Digital, el cual tendrá entre sus funciones:

> Dirigir la implementación de la política nacional de seguridad Digital y hacer seguimiento continuo de la misma; llevar a cabo la coordinación interinstitucional e intersectorial en temas de seguridad Digital; garantizar que

el alcance de la seguridad Digital en el país incluya la prosperidad económica y social; así como la ciberseguridad, para enfrentar nuevos tipos de crimen, delincuencia, y otros fenómenos que afecten la seguridad nacional; y la Ciberdefensa (CONPES, 2016, p. 50)

De igual modo este coordinador debe propender por:

Garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, o de quien haga sus veces, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos; recomendar nuevas acciones en colaboración con las múltiples partes interesadas, en vista de la rápida tasa de desarrollo de la tecnología y los escenarios de ataques cibernéticos; coordinar con la comisión Nacional Digital y de Información Estatal, y con las múltiples partes interesadas, los informes respecto del cumplimiento de los lineamientos de orientación superior establecidos para la implementación de la política nacional de seguridad digital en el marco de sus principios fundamentales (CONPES, 2016, p 50).

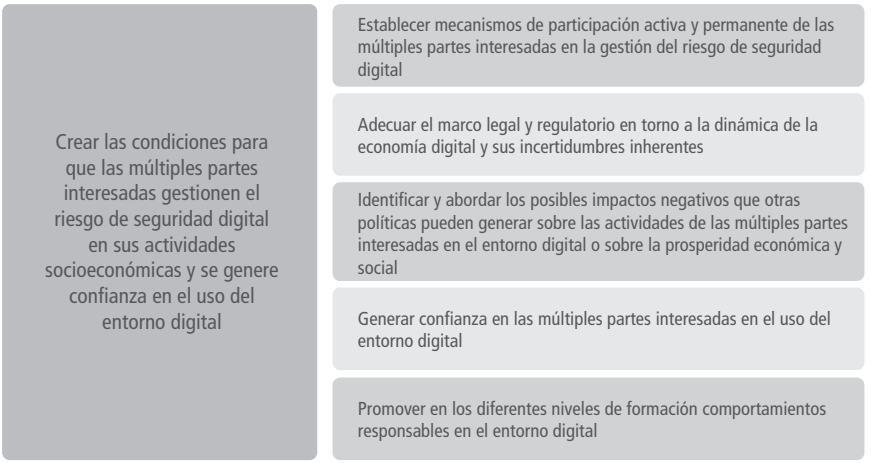
Figura 4. Dimensión estratégica 1. Establecer un marco institucional para la seguridad Digital consistente con un enfoque de Gestión de Riesgos

Fuente: Elaboración propia adoptada del CONPES 3854 de 2016

b. Dimensión estratégica 2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad Digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital

Dentro de los elementos estratégicos que se deben resaltar al respecto, se encuentran los concernientes al establecimiento de mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital; la adecuación del marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes; la identificación y abordaje de los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas o sobre la prosperidad económica y social en el entorno digital, y la generación de confianza a las múltiples partes interesadas en el uso del entorno digital; por último la promoción de comportamientos responsables en el entorno digital (CONPES, 2016, p. 48).

Figura 5. Dimensión estratégica 2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital

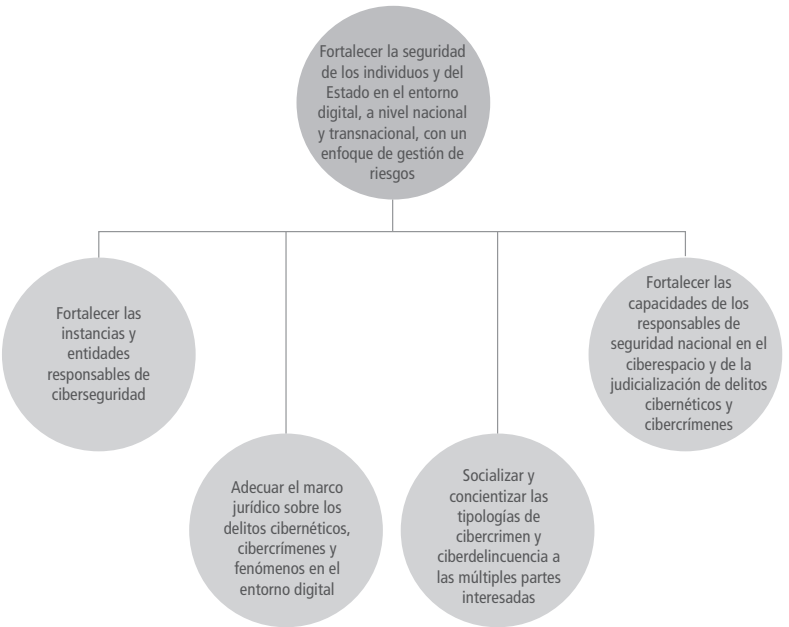


Fuente: Elaboración propia a partir del CONEPS 3854 del 2016

c. Dimensión estratégica 3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de Gestión de Riesgos

Es necesario empoderar a los ciudadanos y al Estado con relación a los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la seguridad Nacional en este espacio. Para esto es imperativo fortalecer a las entidades responsables de ciberseguridad; adecuar el marco jurídico referente a los cibercrímenes y ciberdelincuencia, así como socializar y concientizar acerca de estos a las múltiples partes interesadas; también hay que fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y la de judicialización de este tipo de conductas.

Figura 6. Dimensión estratégica 3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de Gestión de Riesgos



Fuente: Elaboración propia adaptada del documento *CONPES 3854 de 2016*

d. Dimensión estratégica 4. Fortalecer la Defensa y soberanía nacional en el entorno digital con un enfoque de Gestión de Riesgos

Es fundamental desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y Defensa para garantizar los fines del Estado, así como mejorar la protección, preservar la integridad y la resiliencia de la Infraestructura Crítica Cibernética Nacional; para lo cual es necesario fortalecer las instancias y entidades responsables de la Defensa Nacional en el entorno digital, adecuar el marco jurídico para abordar la protección y Defensa del mismo; generar una Estrategia de Protección y Defensa de la Infraestructura Crítica Cibernética Nacional, fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas, y fortalecer las capacidades de los responsables de garantizar la Defensa Nacional en el entorno digital.

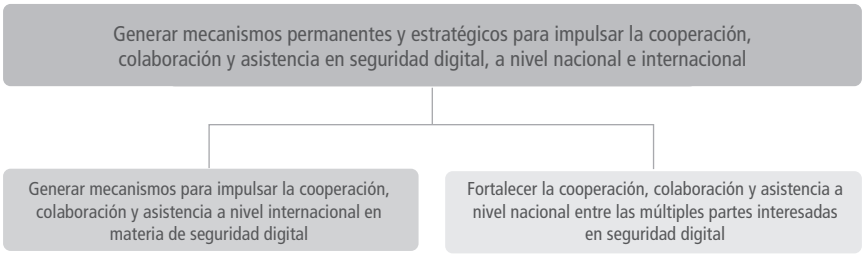
Figura 7. Dimensión estratégica 4. Fortalecer la Defensa y soberanía nacional en el entorno digital con un enfoque de Gestión de Riesgos

Fuente: Elaboración propia adaptada del documento CONPES 3854 de 2016

e. Dimensión estratégica 5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional

La cooperación nacional entre las múltiples partes interesadas y la cooperación internacional en materia de seguridad Digital resultan ser esenciales, para ello se deben generar mecanismos para impulsarlas, así como fortalecer la cooperación, colaboración y asistencia entre bloques de países.

Figura 8. Dimensión estratégica 5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad Digital, a nivel nacional e internacional



Fuente: Elaboración propia adaptada del documento CONPES 3854 de 2016

1.2. Conceptualización

1.2.1. Ciberseguridad

Para abordar la ciberseguridad y Ciberdefensa debemos señalar el concepto de ciberespacio, entendiéndose por este el espacio artificial creado por el conjunto de sistemas de la información y telecomunicaciones que utilizan las TIC, es decir de redes de ordenadores, 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, ha sido creado por el hombre para su servicio (Min. Defensa España y IEEE, 2012).

> El ciberespacio es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan. (CARI, 2013, p. 4)

> La Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 que resuelve adicionar al Artículo 1.8 de la Resolución CRT 1740 de 2007, algunas definiciones y aunque a pesar de que estas disposiciones han sido derogadas, los conceptos siguen vigentes en la actualidad entre ellos:

> C**iberseguridad:** 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. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno […] **Ciberespacio:** es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

La Asociación de Auditoría y Control sobre los Sistemas de Información —*Information Systems Audit and Control Association* (en adelante: Isaca)— define la ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Audea.com, 2016, párr. 3).

Para S. Koch (2015) la ciberseguridad "se entiende que es la situación de ausencia de amenazas realizadas por medio de, o dirigidas a las tecnologías de la comunicación y de la información y a sus redes" (p. 89).

Adicionalmente, para comprender qué es seguridad de la información se debe entender como la preservación de la confidencialidad, integridad y disponibilidad de la información, donde confidencialidad se entiende como una propiedad, a saber, que la información no sea puesta a disposición de otros sin autorización; integridad, por su parte, es la

propiedad de mantener la exactitud y *completitud* de la información; y disponibilidad es la propiedad de que la información sea accesible y utilizable ante el requerimiento de una entidad autorizada (Kosutic, 2012).

En palabras de la Unión Internacional de Telecomunicaciones (en adelante: UIT), se puede definir así:

> El objetivo de la ciberseguridad es contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos. La finalidad de la seguridad informática es conseguir que ningún perjuicio pueda poner en peligro su perpetuidad. Para ello se tratará de reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable. (UIT, 2007, p. 5)

Así mismo el documento *CONPES 3854 de 2016* señala que:

> Seguridad Digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (I) la gestión del riesgo de seguridad Digital; (II) la implementación efectiva de medidas de ciberseguridad y (III) el uso efectivo de las capacidades de Ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Así las cosas, ciberseguridad es la seguridad de la información en el ciberespacio; en otras palabras, cuando se busca proteger la información contenida en el *hardware*, redes, *software*, infraestructura tecnológica o servicios, se está hablando en el ámbito de la seguridad informática o *ciberseguridad* (Audea. com, 2016).

1.2.2. Ciberdefensa

Los Estados organizan la Defensa de la seguridad mediante el establecimiento de una Estrategia Nacional; de acuerdo con las amenazas y los consiguientes riesgos se planean y definen unas estrategias de Defensa abordando diferentes frentes como el territorial, aéreo, fronterizo,

económico y el del ciberespacio, razón por la cual tiene que existir una Ciberdefensa que garantice la ciberseguridad (Min. Defensa España, IEEE, 2012).

Ciberdefensa es, entonces, el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la Defensa con el objeto de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que Fuerzas enemigas los utilicen para cumplir los suyos.

Se ha planteado que el proceso de la Ciberdefensa inicia por la Inteligencia informática con el ciberespacio como ambiente, para poder obtener los elementos descriptores de los escenarios que permitan parametrizar las amenazas y dimensionar los riesgos, para así posibilitar el diseño de los instrumentos de Defensa (CARI, 2013).

La ciberdefensa se efectúa en términos de la defensa activa y pasiva del centro de operaciones y los medios de información que posee la institución con el fin de resistir los ataques cibernéticos que sufra la entidad, cuya arma rectora son las comunicaciones militares que coadyuvan en la protección cibernética de la infraestructura crítica del país. Lo anterior en el ámbito de lo dispuesto por las Fuerzas Militares de Colombia (FF. MM. y Ejército Nacional, 2015).

> A partir de lo mencionado, [la defensa activa es una] estrategia determinada en adquirir una capacidad de defensa del ciberespacio, combinando la protección interior de los sistemas, la vigilancia permanente de redes sensibles y la respuesta rápida en caso de ataque, contrarrestando las amenazas ciberespaciales y garantizando acceso al ciberespacio; [y la defensa pasiva es] la estrategia para la protección de los activos relacionados con los sistemas de información a través de controles detectivos, correctivos, disuasivos que contrarresten las posibles amenazas. (FF. MM. y Ejército Nacional, 2015, p. 5)

En este punto es importante reseñar que en el país se cuenta con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (en adelante: Colcert), el cual tiene como responsabilidad central la coordina-

ción nacional de la ciberseguridad y ciberdefensa, la cual estará enmarcada dentro del proceso misional de gestión de la seguridad y Defensa del Ministerio de Defensa Nacional.

Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad (Colcert, 2013).

De acuerdo con Colcert, el CSIRT de la Policía Nacional de Colombia registró menos incidentes cibernéticos en 2012 que en 2011; esto lo ubica, junto con Chile, como uno de los pocos países latinoamericanos con esa distinción.

No obstante, no es claro si esto se debió a una reducción real en el número de incidentes o a una mejor gestión de la seguridad por parte de las agencias gubernamentales atendidas por estos equipos nacionales de respuesta a incidentes de seguridad cibernética, como son los CSIRT, o a la implementación de políticas que cambiaron la cobertura de la asistencia prestada por los equipos de respuesta de Colombia (OEA, 2013).

También está el Sistema de Información del Centro de Operaciones del Ejército Nacional (en adelante: SICOE); mediante esta herramienta las Unidades operativas mayores y menores del Ejército reportan todos y cada uno de los eventos y situaciones operacionales que se presentan en todo el territorio nacional.

Su objetivo primordial consiste en promover la información en el momento requerido, permitiendo realizar análisis cuantitativos y cualitativos de cualquier situación operacional bajo los niveles de seguridad que garanticen la integridad y la reserva de la información (OEA, 2013).

Además, está el Sistema de Información Geográfica del Ejército (en adelante: SIGE), esta herramienta ha sido diseñada para la captura, almacenamiento, manipulación, análisis, modelación y presentación de datos militares referenciados; el SIGE brinda información geográfica detallada para facilitar el proceso militar en todas las decisiones y es direccionado desde el Comando Conjunto Cibernético (en adelante: CCOC), (FF. MM. y Ejército Nacional, 2015).

1.3. La incorporación de la ciberseguridad en la política nacional desde el entendimiento de la política internacional

Es del caso hacer una referencia de cómo los distintos Estados han adoptado e incorporado el concepto de ciberseguridad desde la política tal como en adelante se describe.

La primera referencia es la Estrategia de Ciberseguridad Europea, nacida como un conjunto de acciones encaminadas a solventar y mejorar el espacio en la red. El documento nació asistido por una serie de órganos, instituciones y políticas que ya se habían estado trabajando alrededor de las diversas dimensiones de la seguridad desde finales de 1990 (Machín y Gazapo, 2016). La Estrategia de ciberseguridad de la Unión Europea establece los planes para prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones de este bloque de países. La UE tiene, en este contexto, una extraordinaria importancia, no solo porque agrupa a 28 países industrializados -que en la economía digital mundial juegan un papel relevante-, sino porque en ellos las tecnologías digitales son el paradigma sobre la economía y la sociedad en su conjunto, mucho más que en otro lugar.

Además, en el Viejo Continente proporcionalmente están más amenazados que en otras partes; como se ha visto con los crecientes ciberataques dirigidos por bandas internacionales conectadas entre sí y que operan con un elevado nivel técnico. Ante esta perspectiva, la ciberdelincuencia nos lleva a una cruda realidad en países abiertos e interconectados como los de la UE (Izquierdo, 2016).

En cuanto a lo mencionado, cabe traer a colación la más reciente Directiva del Parlamento Europeo y del Consejo de la UE encaminada a determinar las medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información, a fin de mejorar el funcionamiento del mercado interior, (PE y Consejo, 2016, p. 1). Esta contiene las siguientes prerrogativas:

> a) Establece obligaciones para todos los Estados miembros de adoptar una Estrategia Nacional de seguridad de las redes y sistemas de información; b) Crea un Grupo de cooperación para apoyar y facilitar la cooperación

> estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos; c) Crea una red de equipos de respuesta a incidentes de seguridad informática a (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz; d) Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales; e) Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información. (PE y Consejo, 2016, pp. 11-12)

Esta regulación establece las reglas de seguridad cibernética (o conjuntos de controles de seguridad) para las empresas que suministran servicios a la sociedad que se han categorizado como esenciales (OEA 2018). Allí se establecen un conjunto de sectores, referenciados como estratégicos para las actividades sociales y económicas de la Unión Europea. Se relacionan el sector de la energía, de los transportes, el sector financiero, el de los servicios de agua y salud, motores de búsqueda, operadores de servicios digitales, entre otros. Así mismo, se establece la obligación de los Estados para determinar y delimitar de manera clara quiénes, de las organizaciones públicas o privadas de cada uno de los miembros son operadores de servicios esenciales.

La Estrategia china en la *Ley Nacional de seguridad Cibernética* adoptada por el Parlamento chino en noviembre de 2016, que entró plenamente en vigencia el 31 de diciembre de 2017, establece a lo largo de siete capítulos y 79 artículos, los compromisos más importantes de las agencias del Estado, así como de quienes prestan servicios de Internet y por último de los usuarios de este. De forma inicial se establece la obligación frente a la adopción, por parte de las compañías para garantizar que Internet funcione, y para ello le obliga a la adopción de medidas técnicas y humanas, dar frente a los incidentes de seguridad y la prevención de actividades en el ciberespacio. La política establece un régimen de vigilancia, inspección y auditoría, para garantizar la reducción de riesgos.

Estados Unidos, si bien no ha adoptado un esquema regulatorio claro, sí ha hecho un llamado para que las organizaciones y la industria adopten los estándares, metodologías, procedimientos y procesos, que garanticen la seguridad de la información, a partir los enfoques políticos, de negocios y de tecnología del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para abordar los riesgos cibernéticos. En el año 2014 fue publicado el marco para mejorar la seguridad cibernética de Infraestructura Crítica que ayuda a las organizaciones a evaluar, administrar y responder al riesgo de seguridad cibernética. Sin embargo, ataques como WannaCry y NotPetya han demostrado que ello no es suficiente.

Luego de la Cumbre Mundial sobre la Sociedad de la Información del año 2003, un conjunto de 170 países determinó la necesidad de que se pudiera beneficiar de las oportunidades de las TIC para acceder a la infraestructura, a la información y al conocimiento, la seguridad en el uso de las TIC; desarrollo y ampliación de aplicaciones TIC; y alentar la cooperación internacional y regional (World Summit on the Information Society, 2003).

Precisamente por ello, en 2004, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), y su Programa de Seguridad Cibernética, inició el desarrollo de su agenda. La Organización de Estados Americanos (en adelante: OEA) ha estado trabajando para fortalecer las capacidades de seguridad cibernética entre sus Estados miembros desde principios de la década de 2000. Con los años se ha convertido en un líder regional en asistencia a los países para fortalecer la capacidad técnica y de seguridad cibernética en cuanto a políticas para garantizar un ciberespacio seguro y resiliente. El Programa de seguridad Cibernética de la OEA apoya las iniciativas sobre la base de un análisis en profundidad y la comprensión de la magnitud de las amenazas (OEA, 2015).

En 2004, los Estados miembros de este organismo aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, que abogaba por un esfuerzo coordinado de múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio y proporcionaba un referente inicial para cultivar y guiar tal enfoque.

Los Estados miembros fueron extraordinariamente previsivos cuando adoptaron tal estrategia, ya que se ha mejorado la protección de la infraestructura de las TIC con el fortalecimiento de la capacidad de los gobiernos para responder y mitigar incidentes cibernéticos. Estos compromisos se han reafirmado y fortalecido con los años a partir de la adopción de numerosas declaraciones oficiales, incluyendo la más reciente relacionada con el papel y las responsabilidades de la OEA y sus Estados miembros en la promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica (OAS, 2016).

Para el año 2007, la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas (ONU), publicó una Estrategia para la Cooperación y la Colaboración con y entre las partes, ello a partir del desarrollo unos pilares estratégicos así: "I) Medidas legales; II) Medidas técnicas y procedimentales; III) Estructuras organizacionales; IV) Desarrollo de capacidades; y V) Cooperación internacional" (Agencia Especializada sobre Tecnologías de Información y Comunicación de las Naciones Unidas, ITU, 2014). Esto seguido de la Guía de ciberseguridad Nacional de la UIT en 2011, y en 2014, la UIT lanza el Índice de ciberseguridad Global (GCI, por sus siglas en inglés) con el objetivo de medir los programas de ciberseguridad.

Para el año 2015, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE), adoptó y publicó la Recomendación sobre gestión del riesgo de seguridad Digital para la Prosperidad Económica y Social de la OCDE (OCDE, 2015). El principal aporte en la construcción colectiva es la incidencia sobre la adopción de enfoques desde la Gestión de Riesgos desde el cumplimiento de los principios de:

> (I) sensibilización, adquisición de habilidades y empoderamiento; (II) responsabilidad de los interesados; (III) derechos humanos y valores fundamentales; (IV) cooperación; (V) evaluación del riesgo y ciclo de tratamiento; (VI) medidas de seguridad apropiadas y acordes con el riesgo y la actividad económica y social en juego; (VII) innovación; y (VIII) planificación de la preparación y continuidad. (OCDE, 2015)

Para el año 2018, el Foro Económico Mundial (FEM, 2018, pp. 33-36) ha entregado el Cuaderno de Resiliencia Cibernética para la Colaboración Público-Privada (WEF, 2018), a partir del desarrollo de tres capacidades: solidez, resiliencia y Defensa. La solidez se define como "la capacidad de prevenir, repeler y contener amenazas". La resiliencia se define como "la capacidad de gestionar y solucionar violaciones exitosas". Y la Defensa se define como "la capacidad de adelantarse a interrumpir y responder a ataques" (WEF, 2018).

Las escuelas de formación, los grupos de investigación y en general los técnicos se han involucrado y aportado a la construcción colectiva. Puede observarse cómo, el Instituto Potomac para Estudios de Políticas en 2015 expide el Índice de preparación cibernética y se fundamenta en la preparación de indicadores para determinar mejoras en las categorías: (1) Estrategia Nacional; (2) respuesta a incidentes; (3) delito informático y aplicación de la ley; (4) intercambio de información; (5) inversión en I+D; (6) diplomacia y comercio y (7) defensa y respuesta a crisis[2] (Cyber Readiness Index 2.0).

El Modelo de Madurez de Capacidad de seguridad Cibernética de Oxford (Oxford, 2016), muestra cinco dimensiones: "Política y Estrategia de Seguridad Cibernética; (II) cultura cibernética y sociedad; (III) seguridad cibernética, educación, capacitación y habilidades; (IV) marcos legales y regulatorios y (V) estándares, organizaciones y tecnologías".

El Manual es un instrumento para evaluar el nivel de comprensión de las diversas partes interesadas en la capacidad y madurez cibernética de un país.

También la Academia de Gobierno Electrónico en Estonia lanzó un Índice Nacional de seguridad Cibernética en mayo de 2016, allí se establecen 12 áreas de evaluación de capacidades son:

2 El Cyber Readiness Index 2.0 se basa en el anterior su versión 1.0, marco metodológico para evaluar la preparación cibernética en cinco elementos esenciales: Estrategia Cibernética Nacional, respuesta a incidentes, delito electrónico y capacidad legal, intercambio de información e investigación y desarrollo cibernético. El Cyber Readiness Index 1.0 aplicó esta metodología a un conjunto inicial de treinta y cinco países. Para obtener más información sobre Cyber Readiness Index 1.0, véase: Hathaway (2013). Cyber Readiness Index 1.0. En: Hathaway Global Strategies LLC (2013). Obtenido de http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

(1) Capacidad para desarrollar políticas nacionales de seguridad cibernética; (2) Capacidad para analizar las ciberamenazas a nivel nacional; (3) Capacidad para proporcionar educación sobre seguridad cibernética; (4) Capacidad para garantizar seguridad cibernética de base; (5) Capacidad para proporcionar un entorno seguro para servicios electrónicos; (6) Capacidad para entregar identificación y firma electrónicas; (7) Capacidad para proteger la infraestructuras críticas de la información; (8) Capacidad para detectar y responder incidentes cibernéticos 24/7; (9) Capacidad para gestionar una crisis cibernética a gran escala; (10) Capacidad para luchar contra los delitos cibernéticos; (11) Capacidad para llevar a cabo operaciones militares de defensa cibernética y (12) Capacidad para proporcionar seguridad cibernética internacional. (National Cyber Security Index, 2016)

1.4. Elementos críticos de la política nacional de seguridad digital colombiana y su impacto para la investigación el desarrollo y la innovación

A manera enunciativa me limito en señalar los elementos que se convierten en críticos y que impactan la investigación, el desarrollo y la innovación, así:

I. La elaboración y ejecución de los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas.

II. La elaboración y ejecución del plan de fortalecimiento de las capacidades institucionales, operativas, administrativas, humanas, de infraestructura física y tecnológica del sector Inteligencia.

III. El diseño de un modelo de gestión de riesgos de seguridad digital a nivel nacional.

IV. El ajuste al marco regulatorio del sector de tecnologías de la información y las comunicaciones, teniendo en cuenta aspectos necesarios para la gestión de riesgos de seguridad digital.

V. La creación de una agenda estratégica nacional e internacional en temas de seguridad digital.

VI. La adaptación e implementación de un modelo de Gestión de Riesgos de seguridad digital a nivel nacional (MinTIC, 2015).

1.5. La investigación de la ciberseguridad y la ciberdefensa como elemento de la política nacional

Son precisamente estas dimensiones las que centran el actuar de la presente investigación, específicamente la *dimensión estratégica 2* que señala la necesidad de "Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital", de manera particular se establece que el "el Ministerio de Tecnologías de la Información y las Comunicaciones creará y pondrá en marcha un tanque de pensamiento con las múltiples partes interesadas para abordar la gestión de riesgos de seguridad digital mediante la investigación, el desarrollo y la innovación". En este orden corresponde en virtud del rol de la academia establecer la identificación de las partes que participan y están vinculadas con la investigación, el desarrollo y la innovación en temáticas asociadas a la seguridad Digital, así como la identificación de las temáticas a ser investigadas y las metodologías para ello.

Es precisamente este lineamiento de actuación el que enmarca el presente documento, al establecer una aproximación al estado actual en el que se encuentra la ciberseguridad y Ciberdefensa, en cada uno de los sectores que involucran a las diversas partes interesadas y con ello aportar a la construcción de la dimensión estratégica en referencia.

2. Las diversas partes interesadas del ecosistema de seguridad digital como actores principales de la investigación

2.1. El entendimiento de una estrategia de ciberseguridad y ciberdefensa nacional por las diversas partes interesadas

El *CONPES de seguridad Digital 3854 de 2016* ha entendido que las múltiples partes interesadas son en el Esquema Nacional de seguridad Digital, el Gobierno nacional y los territoriales, las organizaciones públicas

y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades (CONPES 3854 de 2016). En ese contexto resulta fundamental entender los elementos que incorpora, para todos y cada una de las partes interesadas, una Estrategia de ciberseguridad para su organización.

a. Gobernanza. La "buena gobernanza" según lo presenta (Cerrillo Martínez, 2007) se erige con base en los principios de participación, eficacia, coherencia, transparencia y rendición de cuentas, (último término conocido como *accountability*); dichas directrices marcan la pauta para las diferentes políticas públicas caracterizadas por un trato más cooperativo y consensuado hacia la ciudadanía, según lo señalé en mi texto de doctorado. Bajo este concepto, es necesario el desarrollo, desde el nivel estratégico de las organizaciones, sean públicas o privadas, de un conjunto de principios, normas y valores, que enmarquen la política de ciberseguridad. Allí se deberá establecer, además, quién es la autoridad que ejercerá el liderazgo, la estructura de la organización; las formas, procesos y procedimientos de coordinación al interior y al exterior de esta.

b. Desarrollo de capacidades especiales. La estrategia debe incorporar un conjunto de medidas tendientes a la creación, mantenimiento y fortalecimiento de cuatro grupos: uno de prevención de riesgos; en segundo lugar, otro de gestión de riesgos; en tercera instancia, un grupo especial de reacción defensiva frente a escenarios de confrontación; por último, un grupo de cibercriminalidad, cuyo objetivo esencial es la investigación de ataques a la infraestructura crítica del Estado.

c. Formación. La estrategia debe contar con un plan a corto, mediano y largo alcance que permita la formación, en los distintos niveles -básico, técnico, profesional, especializado y experto- del conjunto de

servidores de la organización. De la misma manera, deben existir unos elementos mínimos de formación para los usuarios o ciudadanos que se relacionan con la organización. Dicho plan de capacitaciones debe tener como principios la integralidad, transversalidad, permanencia, la prospectiva y la responsabilidad.

d. Esquema para prevención del riesgo, gestión de incidentes y defensa de la infraestructura crítica. En la estrategia será necesaria la incorporación de tres elementos específicos, señalándose en cada uno de ellos los procesos, procedimientos, responsables, responsabilidades, y esquemas de reacción que tengan que ver con los elementos que a continuación se relacionan. En primera instancia, la prevención de los riesgos, esto es, todas las medidas humanas, técnicas, institucionales, personales, económicas y políticas, necesarias para la prevención de los riesgos; En segundo lugar, tenemos la gestión de incidentes; se deben establecer las técnicas, procesos y procedimientos que se tendrán que desarrollar frente a un escenario en el que se vea comprometida la infraestructura física y lógica de la entidad; Por último, se encuentra el conjunto de normas, procesos y procedimientos en caso de verse comprometida la Infraestructura Crítica de la organización, es decir, la capacidad de reacción y sus límites en un escenario de confrontación. Así las cosas, existe un elemento transversal que es señalar que la infraestructura física y lógica de la entidad es el corazón y cuáles son las capas en que se permite su intrusión y los niveles correspondientes.

e. Marco legal. Siendo este uno de los elementos esenciales de la estrategia, en el desarrollo de esta se debe identificar los elementos estructurales de regulación como pueden ser, identificación electrónica, servicios misionales, gestión de riesgos, gestión de incidentes, obligaciones, condición de infraestructura crítica, entre otros.

f. Marcos de cooperación y diplomacia. La estrategia debe contener los elementos esenciales de cooperación, relación y trabajo, en conjunto con situaciones de prevención y gestión de los riesgos; pero al mismo

tiempo tiene que incluir el esquema de cooperación nacional e internacional frente a escenarios de conflicto.

g. Investigación, desarrollo e innovación. Uno de los elementos más importantes que deberá abordar la Estrategia de ciberseguridad y Ciberdefensa en una organización, es la creación de un centro de investigación, desarrollo e innovación que se encuentre alineado con la política de I+D+I Nacional y la generación de investigación desde la participación activa de las diversas partes interesadas. Partes que están definidas a continuación.

2.2. Las diversas partes interesas en la gestión de riesgos de seguridad digital

2.2.1. Consideraciones Preliminares

El concepto de grupo de interés o partes interesadas[3] proviene de la consolidación de la Responsabilidad Social Empresarial (en adelante: RSE) o Responsabilidad Social Corporativa (en adelante: RSC) como área de estudio y aplicación por parte de las entidades del sector productivo. En este contexto se busca la identificación de aquellas colectividades u organizaciones a quienes influencia la actividad de una corporación o empresa, ya sea de manera directa o indirecta, y como tal, según Strandberg (2010), tienen derecho a ser escuchadas más no a que la empresa u organización satisfaga todos sus requerimientos.

En el campo de la RSE, por ejemplo, pueden identificarse grupos de interés observando el desarrollo de la línea de negocios como tal, esto es, desde las actividades que generan productores, proveedores, distribuidores o consumidores, si se toma al sector de transformación.

Otro modo, *a priori*, de detectar grupos de interés en este ámbito es a través de la determinación de Áreas de Influencia Directa (en adelante: AID) y Áreas de Influencia Indirecta (en adelante: AII) de una actividad

3 "Se entiende por *stakeholder* cualquier individuo o grupo de interés que, de alguna manera — explícita o implícita; voluntaria o involuntaria— tenga alguna apuesta hecha — *to stake*, poner algo en juego— en la marcha de la organización" (OCDE, 2015).

industrial, extractiva o de infraestructura que, de cualquier forma, tienen impacto social y medio ambiental, para así encontrar a los interesados dentro de estas áreas.

Una similitud que se observa en cuanto a los grupos de interés en la RSE y en los que se dan en las relaciones de la producción académico científica, consiste en que lo que se genera en tales círculos ofrece resultados con finalidades específicas y con diferentes grados de impacto en diversas esferas de la sociedad; otra característica en común es la necesidad de buscar sinergia y realimentación entre la organización y sus grupos de interés, en concordancia con Strandberg (2010), quien señala que:

> El desarrollo de compromisos con los grupos de interés puede conllevar beneficios, pero si se establecen con grupos equivocados o se plantean de manera errónea pueden llevar a un desaprovechamiento de los recursos y distraer a la organización de otras prioridades más urgentes. Por ello, es importante considerar los objetivos estratégicos de la empresa (**o del proyecto, o del departamento en cuestión**) a la hora de plantearse por qué establecer una colaboración. (p. 11) [negrillas fuera del original]

Ahora bien, si se extrapola el tema 'grupo de interés' del terreno corporativo al de la investigación académica aplicada, los objetivos de ésta deben confluir con los de los grupos de interés hacia los que van dirigidos los resultados de tal producción científica, lo cual tendría que redundar en beneficio no solo de determinadas empresas y sectores sino de la nación en su conjunto.

Igualmente, una de las principales diferencias en cuanto al compromiso con los grupos de interés en la RSE y aquellos que se puedan establecer desde producción científica, concebida en la academia, es el grado de compromiso en este último caso; por ende, en principio, sí se tendrían que cumplir los requerimientos de los grupos de interés que se beneficien con lo producido a partir de una línea de investigación como esta; pero ello solo debería darse sobre la base de acuerdos claros y medibles en cuanto a lo que se puede y debe brindar, de ahí la importancia de determinar adecuadamente cuáles son los grupos de interés.

2.2.2. Modelos para Identificar Grupos de Interés en La RSE

Según Strandberg (2010), la organización AccountAbility sugiere tener en cuenta las dimensiones para identificar partes interesadas o grupos de interés, de acuerdo con el grado en que se presenten las siguientes circunstancias con ciertos colectivos: "Responsabilidad […] Influencia […] Tensión […] Dependencia […] Perspectivas diversas (identificación de oportunidades)" (p. 11).

Entonces, aquellos con quien se llegue a dar estas circunstancias, identificadas como dimensiones, son quienes harán parte de los grupos de interés. Adicionalmente, el mencionado autor, refiere que la Global Reporting Initiative menciona que la **proximidad de los grupos** y la **representación de organizaciones** son otros factores para tener en cuenta al determinar a las partes interesadas; estos factores son patentes cuanto se habla de AID y AII, según se mencionó en acápites anteriores.

Por su parte, Granda Revilla y Trujillo (s.f.) además de mencionar varias de las dimensiones y factores aludidos por Strandberg; pero enmarcados como perspectivas; añaden que por temas de economía es necesario realizar un proceso de **priorización** (donde se agrupen grupos con intereses similares) y previamente a esto se debe hacer "un ejercicio de agrupación de los stakeholders [sic] de interés, que permita unificar aquellos que la organización considere asimilados (similares características o expectativas) y facilite la posterior priorización" (p. 3).

Estos autores afirman que dicha priorización permite "una reflexión en torno a qué grupos de interés debe considerar como prioritarios y por tanto establecer mecanismos de diálogo más intensivos […] y qué grupos de interés deben quedar en un plano secundario" (p. 3).

2.2.3. Metodología para Identificación de Grupos de Interés en La Línea de Investigación

Metodología Cualitativa – Descriptiva. Bajo este enfoque, se elige una estrategia cualitativa que pone "énfasis en procesos que no están rigurosamente examinados o medidos en términos de cantidad, monto, intensidad o frecuencia" (Schettini & Cortazo, 2015). Esto sin perjuicio

de que la información así obtenida sirva como sustento para buscar datos cualitativos y estudiarlos.

De acuerdo con lo anterior, se plantea un estudio analítico del entorno usando investigaciones previas y documentos oficiales, como fuentes -teniendo en cuenta los factores y dimensiones presentados en los modelos de la RSE- para llegar al desarrollo de los siguientes aspectos:

Consolidación de información base

1. Banco de información. Consolidación continua de un banco de información con realimentación o actualización, basado en el marco teórico propio de la gestión del riesgo en seguridad Digital y en los hallazgos de la investigación.

2. Determinación preliminar. Gracias a la implementación del punto anterior, se podrán establecer unos conjuntos o subconjuntos a quienes, en primera instancia, les resulta de interés lo generado a través de la investigación de esta línea.

Determinación de los grupos de interés

Una vez hallados los conjuntos que requieren de los resultados de la investigación, se procederá a profundizar en tales conjuntos y, teniendo el grado de incidencia de factores como: responsabilidad, influencia, dependencia, perspectivas diversas (oportunidades) se procederá a responder:

1. ¿Quiénes necesitan el producto de la investigación?
2. ¿Por qué lo necesitan y en qué medida?
3. ¿Cuál es el perfil de los destinatarios?

Esto incluye identificación de la agenda o interés de cada grupo, interés misional (si se trata de una institución o personal del Estado), interés comercial o corporativo entre otros.

4. ¿Qué beneficios y riesgos hay al divulgar la información contenida en los resultados? (Debe elaborarse una matriz)

5. ¿Quiénes se impactarán positiva o negativamente con el uso que, los posibles grupos de interés les den a los resultados de la investigación? (Debe elaborarse una matriz)

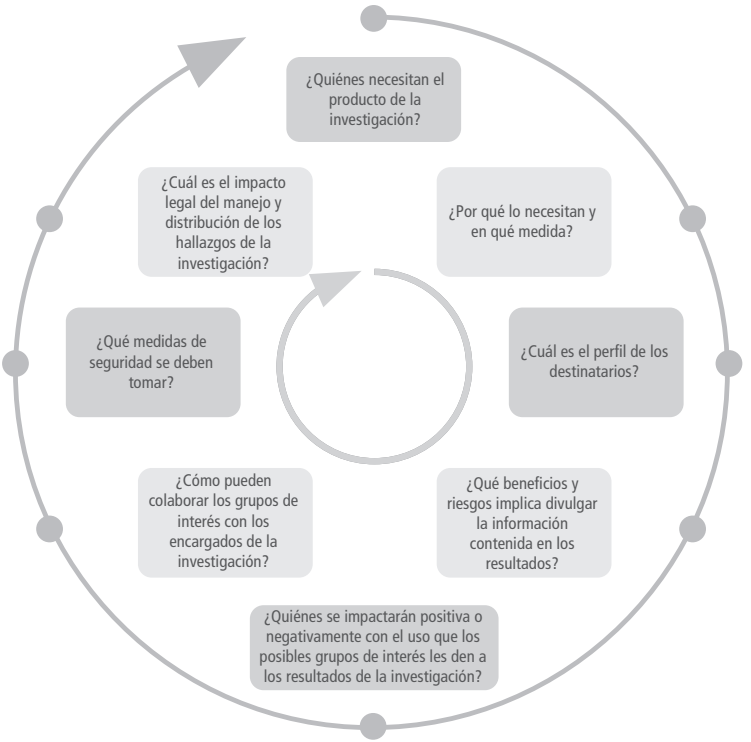
6. ¿Cómo pueden colaborar los grupos de interés con los encargados de la investigación?

7. ¿Qué medidas de seguridad se deben tomar?

8. ¿Cuál es el impacto legal del manejo y distribución de los hallazgos de la investigación?

Preparado en el marco del desarrollo de la metodología.

Figura 9. Determinación de los grupos de interés



Fuente: elaboración propia

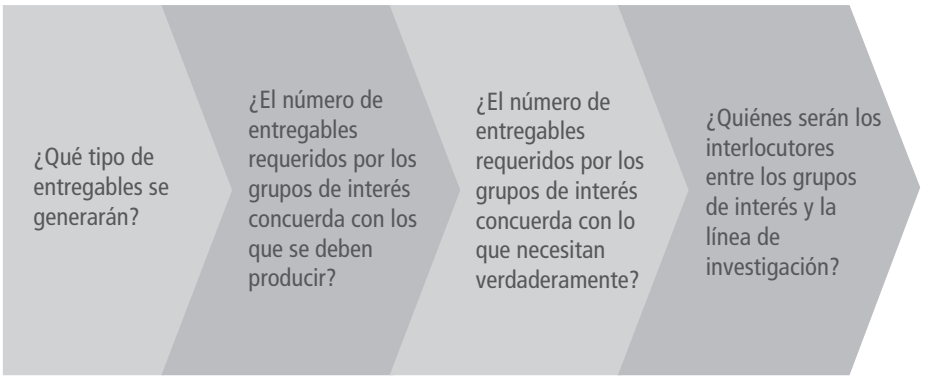
Productos de la investigación

Así, teniendo en cuenta el personal, los insumos establecidos se debe determinar:

1. ¿Qué tipo de entregables se generarán?
2. ¿El número de entregables requeridos por los grupos de interés concuerda con los que se deben producir?
3. ¿El número de entregables requeridos por los grupos de interés concuerda con lo que necesitan verdaderamente?
4. ¿Quiénes serán los interlocutores entre los grupos de interés y la línea de investigación?

Preparado en el marco del desarrollo de la metodología

Figura 10. Productos de la investigación



Fuente: Elaboración propia

En este orden se ha identificado que los grupos de interés corresponden a los sectores que hacen parte del ecosistema digital, a saber: I) el sector Gobierno; II) el sector Defensa; III) el sector Universitario y Académico; IV) el sector mixto y privado. En todos estos sectores debe establecerse un contexto inicial en cuanto a la gestión de riesgos de seguridad digital que fundamente las temáticas de investigación en la línea

correspondiente. Todo ello soportado sobre el concepto de Infraestructura Crítica Cibernética Nacional en los términos del documento *CONPES de seguridad Digital para Colombia:*

> entendida esta como aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado y cuya afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública (CONPES, 2016).