REPÚBLICA DE COLOMBIA

CONGRESO DE LA REPÚBLICA DE COLOMBIA
SENADO DE LA REPÚBLICA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

I S S N 0 1 2 3 - 9 0 6 6

AÑO XXXII - Nº 1076 Bogotá, D. C., martes, 15 de agosto de 2023 EDICIÓN DE 37 PÁGINAS

DIRECTORES: GREGORIO ELJACH PACHECO
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

JAIME LUIS LACOUTURE PEÑALOZA
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

SENADO DE LA REPÚBLICA

PONENCIAS

INFORME DE PONENCIA POSITIVA PARA PRIMER DEBATE PROYECTO DE LEY NÚMERO 10 DE 2023 SENADO

por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas.

INFORME DE PONENCIA PARA PRIMER DEBATE PROYECTO DE LEY NO. 010 DE 2023 SENADO "POR LA CUAL SE CREA LA AGENCIA NACIONAL DE SEGURIDAD DIGITAL Y SE FIJAN ALGUNAS COMPETENCIAS ESPECÍFICAS"

Bogotá, D.C., 15 de agosto de 2023

Señor
GERMÁN ALCIDES BLANCO ÁLVAREZ
Presidente
COMISIÓN PRIMERA
SENADO DE LA REPÚBLICA
Ciudad

Asunto: Ponencia para primer debate del Proyecto de Ley No. 010/2023 Senado "Por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas".

Respetado señor Presidente:

En cumplimiento del encargo recibido por parte de la honorable Mesa Directiva de la Comisión Primera del Senado de la República y de conformidad con lo establecido en el artículo 150 de la Ley 5ª de 1992, procedemos a rendir Informe de Ponencia positiva para primer debate del Proyecto de Ley 010/2023 Senado "Por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas".

El informe de ponencia se rinde en los siguientes términos:

1. TRÁMITE DE LA INICIATIVA

1.1. El Proyecto de Ley fue radicado el día 24 de julio de 2023 ante la Secretaría General del Senado de la República, suscrito por los senadores Ana María Castañeda, David Luna y la Representante Ingrid Sogamoso.

1.2. El Proyecto de Ley fue publicado en la Gaceta del Congreso No. 901 de 2023

1.3. La Secretaría de la Comisión Primera Constitucional del Senado de la República comunicó el 02 de agosto de 2023, que de acuerdo con el Acta MD-01 de la Mesa Directiva de la Comisión se designó como ponentes a los honorables senadores David Luna y Alfredo Deluque (coordinadores); así como a los honorables senadores Fabio Amín, Paloma Valencia, Clara López, Ariel Avila, Julián Gallo y Oscar Barreto.

1.4. Esta es la segunda ocasión en la que se presenta el Proyecto de Ley, habiéndose radicado en mayo de 2023, suscrito por los Senadores David Luna y Ana María Castañeda y la Representante Ingrid Sogamoso, el cual fue archivado por no haberse surtido primer debate durante la legislatura anterior de conformidad con el artículo 162 de la Constitución Política.

1.5. El Proyecto de Ley 010/2023 fue remitido a veinticuatro (24) organizaciones expertas en la materia, para que emitieran observaciones al texto radicado. Las organizaciones y entidades a la cuales se les envió para comentarios fueron:

ACEMI
ACIS
ACOLGEN
ALIADAS
AMCHAM
Alianza IN
ANDESCO
ASOTIC
BPRO
CCE
CCIT
CINTEL
Colombia Fintech
Defensoría del Pueblo
Ediligence
Escuela Superior de Guerra
FEDESOFT
Firma Digital
Fiscalía General de la Nación
Fundación Karisma
INNOVA
LegalTech Colombia
Superintendencia de Industria y Comercio
IMS Global

1.5 De las organizaciones mencionadas anteriormente se recibieron comentarios de:

- AmCham.
- CCE.
- CCIT.
- Defensoría del Pueblo.
- Fiscalía General de la Nación.
- Fundación Karisma.
- IMS Global.

2. OBJETO DEL PROYECTO DE LEY

El proyecto de Ley tiene por objeto la creación de la Agencia Nacional de Seguridad Digital, establecer sus funciones y dictar otras disposiciones; esto con el fin de crear una instancia que sea la máxima autoridad para la formulación y aplicación de la estrategia nacional y políticas públicas en materia de seguridad digital y ciberdefensa nacional en Colombia.

Esta propuesta responde a la necesidad que tiene el país de fortalecer su marco institucional en Seguridad Digital, para prevenir y combatir ciberataques de manera coordinada, con tiempos acordes a las necesidades de reacción. Así como garantizar el presupuesto y personal capacitado necesario para el funcionamiento de esta entidad.

3. JUSTIFICACIÓN DE LA INICIATIVA:

El Proyecto de Ley fue justificado por sus autores en los siguientes términos:

3.1 PROBLEMA QUE SE PRETENDE RESOLVER:

Colombia es el segundo país de América Latina con más ciberataques presentados (IBM,2022). Así mismo, a nivel mundial se encuentra en el puesto 69 (NCIS, 2022). Solo en el 2022 el país recibió 20 mil millones de intentos de ciberataques y grandes organizaciones fueron atacadas por este flagelo, tales como, la Fiscalía General de la Nación, el INVIMA, la E.P.S Colsanitas, Audifarma, Carvajal,Empresas Públicas de Medellín, CAFAM, entre otros.

A pesar de que en Colombia se ha establecido legislación para la investigación y reacción de ataques cibernéticos, se ha evidenciado la falta de coordinación entre las entidades hoy ya creadas: Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT); Comando Conjunto Cibernético y el Centro Cibernético Policial. A su vez, el poco presupuesto asignado y la falta de personal capacitado para cumplir con las necesidades de seguridad digital del país, es un aspecto que debe corregirse.

La iniciativa legislativa establece acciones para garantizar la coordinación entre el Comando Conjunto Cibernético y el Centro Cibernético Policial, así como con el Ministerio de Tecnologías de la Información y las Comunicaciones y sus entidades adscritas; el Ministerio de Defensa Nacional; la Fiscalía General de la Nación; y otros órganos del Estado, necesarios para generar una política preventiva en materia de Seguridad Digital.

3.2 CÓMO SE RESUELVE EL PROBLEMA:

El Proyecto de Ley establece la creación de la Agencia Nacional de Seguridad Digital, la cual será una nueva entidad que garantice la articulación entre el Estado, el sector privado y los ciudadanos. Esta entidad no significa más gasto de recursos pues se creará el Fondo Nacional para la Seguridad Digital y Ciberdefensa, el cual distribuirá los recursos que hoy están destinados a la ciberdefensa y buscará la inversión del sector privado.

Este Proyecto determina las funciones de la Agencia; así como su estructura y presupuesto, creando institucionalidad en la materia y permitiendo que Colombia pase de una política reactiva en materia de Seguridad Digital a una preventiva. Así mismo, el país sería pionero en la región en crear una Agencia de dicha naturaleza.

3.3 ANTECEDENTES DEL PROYECTO DE LEY

SOBRE LA INICIATIVA LEGISLATIVA:

El Proyecto de Ley que aquí se presenta tiene como principal objeto la creación de la Agencia Nacional de Seguridad Digital. De conformidad con el artículo 150 de la Constitución Política, le corresponde al Congreso hacer las leyes. En lo que respecta a la creación de entidades públicas, el numeral 7 del precitado artículo, señala que mediante esta facultad se podrá determinar la estructura de la administración nacional y crear y suprimir o fusionar ministerios, departamentos administrativos, superintendencias, establecimientos públicos y otras entidades del orden nacional.

A su vez, el artículo 154 constitucional establece que las leyes sobre las materias señaladas en el numeral 7 del artículo 150, es decir, las referentes a la creación de entidades, sólo podrán ser dictadas o reformadas por iniciativa del Gobierno Nacional.

En ese sentido, para el caso concreto, al tratarse de la creación de una Agencia Nacional, nos encontramos frente a un proyecto de ley que debe ser de iniciativa del gobierno nacional.

No obstante, como lo ha señalado la Corte Constitucional, la iniciativa privativa no solo se entiende satisfecha con la presentación del proyecto, sino también cuando *"Se acredite la aquiescencia o aval gubernamental posterior a este momento, siempre que se otorgue antes de la votación y aprobación del articulado en las plenarias. Aquella, además, puede ser dada por el ministro titular de la cartera que tenga relación con la materia, que no de manera necesaria por el presidente de la República"* (Corte Constitucional, sentencia C-047 de 2021).

ANTECEDENTES

Que el desarrollo y la masificación en el uso de las tecnologías de información y comunicaciones conlleva riesgos asociados que afectan los derechos de las personas, las infraestructuras críticas cibernéticas y los intereses nacionales de Colombia, a nivel nacional e internacional.

Estos riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave a la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados, o, incluso, por sujetos individuales.

Que el creciente uso de Tecnologías de la Información y las Comunicaciones suponen el surgimiento de nuevos riesgos y amenazas para la seguridad del país, sus habitantes y sus infraestructuras, los cuales deben ser abordados de manera integral.

Atendido el carácter transfronterizo del ciberespacio, una de las mejores formas de enfrentar los riesgos y amenazas que su uso intensivo genera es establecer relaciones de cooperación en ciberdefensa con otros actores estatales, organismos internacionales y participar de manera activa en foros y discusiones internacionales, que propenden a generar un ciberespacio seguro en el ámbito de la defensa.

Que el país está perdiendo la oportunidad de desarrollar capacidades propias que contribuyan a la autonomía tecnológica en materia de Seguridad Digital.

CONTEXTO ACTUAL:

Actualmente, Colombia es el segundo país de América Latina con más ciberataques presentados, solo superado por Brasil (IBM, 2022), y se encuentra en el puesto 69 del ranking global que mide el nivel de seguridad cibernética de los países (NCIS, 2022). Lo anterior, demuestra evidentes falencias en su política de ciberseguridad, como se detalla en la tabla presentada a continuación:

INDICADOR	%
Desarrollo de política de Ciberseguridad	29%
Análisis e información de amenazas de ciberataques.	40%
Educación y desarrollo profesional	67%
Contribución a la ciberseguridad global	33%
Protección de sus servicios digitales	0%
Protección de sus servicios esenciales	17%
Identificación digital y servicios de confianza	78%
Protección de datos personales	100%
Respuesta a ciberataques	50%
Manejo de crisis cibernéticas	20%
Operaciones militares en materia de ciberseguridad	67%

*Tabla de elaboración propia con información del National Cyber Security Index (2022)

Desde el 2022 el número de ataques cibernéticos en Colombia ha aumentado considerablemente en comparación con años anteriores. Según Fortinet (2023) el país recibió en el 2022, 20.000 millones de intentos de ciberataques, un crecimiento del 80% frente al 2021.

Dicho incremento va en relación con el panorama mundial, pues según el Informe de Riesgos Globales del Foro Económico Mundial (2023) los delitos cibernéticos incrementaron en un 600% después de la pandemia y es la octava amenaza mundial en términos de mayor impacto a la que se enfrenta hoy la humanidad.

Importantes infraestructuras críticas del Estado, tanto públicas como privadas, han sido víctimas de ciberataques y del robo masivo de información en el último año. Por ejemplo, Colsanitas (Grupo Keralty) perdió 0,8 terabytes de información entre los que se incluían estados financieros, balances, presupuestos e información personal de sus usuarios (Portafolio, 2022); el INVIMA fue víctima de tres ataques cibernéticos entre el 2022 y el 2023, de los que se estima fueron capturados 700GB de datos confidenciales de la entidad.

Por otra parte, la Fiscalía General de la Nación fue víctima de un ataque cibernético en el cual más de 10 TB de información sensible, incluyendo correos privados fueron secuestrados por parte de ciberdelincuentes (BluRadio, 2022). En mayo de 2023 la plataforma SECOP II, la cual es clave para los trámites de contratación pública en el país estuvo fuera de línea durante 34 horas según información revelada por el medio de comunicación Infobae (2023).

Modelo de Gobernanza en Seguridad Digital Actual:

En el año 2009, con el trabajo del entonces Ministerio de Comunicaciones y el Congreso de la República se sanciona la Ley 1341 o Ley de Tecnologías de la Información y las Comunicaciones (TIC). Esta Ley cumple el propósito de establecer un marco jurídico acorde con la realidad mundial y el posicionamiento de las Tecnologías de la Información y las Comunicaciones en el ciberespacio.

Por medio de esta Ley se transforma el Ministerio de Comunicaciones, pasando a ser el hoy Ministerio de Tecnologías de las Información y las Comunicaciones (MinTIC). Con su creación se *"constituye el reconocimiento por parte del Estado de que la promoción del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal son pilares para la consolidación de las sociedad de la información y del conocimiento e impactan en el mejoramiento de la inclusión social y de la competitividad del país" (CEPAL, 2011, pg. 8).*

Posteriormente, en el mismo año, ante la necesidad de modificar el Código Penal para reconocer delitos informáticos, el Congreso de la República expide la Ley 1273 de 2009, en la cual se establece la protección de la información y los datos y se "preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones". (Ley 1273, 2009). Ese mismo año, se crea la Unidad de Delitos Informáticos de la Fiscalía General de la Nación, encargada de investigar y perseguir los delitos informáticos en el país.

En el 2011 Colombia formalizó sus esfuerzos en establecer un modelo de gobernanza para reconocer la ciberseguridad y la ciberdefensa como elementos fundamentales para garantizar la defensa nacional, pues el ciberespacio se considera el quinto dominio de la seguridad de un Estado (Douzet, 2014).

Dada su importancia, el CONPES 3701 de 2011 estableció por primera vez los lineamientos de política para ciberseguridad y ciberdefensa del país, reconociendo la importancia de protegerlo de amenazas cibernéticas ante la importancia del ciberespacio para el desarrollo socioeconómico del país. Este CONPES tuvo como objetivo promover la cultura de la seguridad cibernética, concienciar a la población sobre los riesgos y buenas prácticas del uso de las Tecnologías de la Información y las Comunicaciones y establecer organismos de respuesta a los incidentes cibernéticos de la Nación.

Las instancias que se conformaron a través de este CONPES fueron: ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), adscrito en su momento al Ministerio de Defensa Nacional; el Comando Conjunto Cibernético, equipo encargado de la defensa del país en el ciberespacio y el Centro Cibernético Policial, equipo encargado de la seguridad ciudadana en el espacio. El CONPES planteaba que dichas entidades serían las encargadas del diseño e implementación de políticas y estrategias de seguridad cibernética y del

establecimiento de mecanismos de protección de la información y de respuesta a incidentes cibernéticos.

Así mismo, bajo el Decreto 289 de 2011 se establece el Comité Nacional de Ciberseguridad como órgano de consulta y asesoría para la formulación de políticas en materia de ciberseguridad y en el 2012 se establece el Plan Nacional de Ciberseguridad desarrollando una serie de estrategias para proteger las infraestructuras críticas del país.

Mediante la Resolución 05839 de 2015, la Policía Nacional de Colombia establece las funciones del Centro Cibernético Policial como una dependencia de la Dirección de Investigación Criminal *"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"* (Resolución 05839, 2015, art. 15).

Posteriormente, en el 2016 el CONPES 3855 estructura la Política Nacional de Seguridad Digital a través de la protección de la información crítica del país y se plantea la necesidad de mejorar las capacidades de respuesta ante incidentes cibernéticos por medio de la coordinación de diferentes entidades del Estado y la asignación de recursos económicos a las instancias creadas en el CONPES 3701 de 2011. En el CONPES se señala que: "*Colombia no cuenta con una instancia de coordinación nacional en seguridad digital que optimice la gestión de los recursos destinados a esta materia*" (CONPES 3855, 2016, pág.32).

En el 2018, Colombia adopta mediante la Ley 1928 de ese año, el "Convenio sobre la ciberdelincuencia", firmado en Budapest en el año 2001. Este Convenio tiene como objetivo promover la cooperación internacional en la lucha contra la ciberdelincuencia en delitos como: acceso ilegal a sistemas informáticos, fraude informático, abuso de niños en línea, robo de identidad, entre otros.

En el 2020, el Departamento Nacional de Planeación establece el CONPES 3995: *"Política Nacional de Confianza y Seguridad Digital"*, el cual buscaba ejecutar los lineamientos planteados en el Convenio de Budapest y establecer medidas para mejorar la seguridad digital del país por medio de una actualización del marco de gobernanza en materia de seguridad digital.

El CONPES 3995 vuelve a hacer hincapié en la importancia de la coordinación entre las diferentes instancias del Estado, el sector privado y la academia para implementar de manera efectiva la política de confianza y seguridad digital; así como la necesidad de asignar recursos financieros para llevar a cabo las propuestas planteadas para la correcta aplicación de la "Política Nacional de Confianza y Seguridad Digital".

En el 2021, el Ministerio de Tecnologías de la Información y las Comunicaciones expide la Resolución 500 de 2021, en la cual se establecen los lineamientos para la implementación de la estrategia de seguridad digital y la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI). En esta resolución se manifestaba que todas las entidades públicas debían adoptar medidas técnicas, administrativas y de talento humano para garantizar la seguridad digital, esto con el fin de prevenir incidentes en la materia.

Posteriormente, en el 2022, el Gobierno Nacional expide el Decreto 338, el cual modifica el Título 21 de la parte 2, del libro 2 del Decreto 1078 de 2015 "Con el fin de establecer lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de estructuras críticas, cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta incidentes de seguridad digital" (Decreto 339, 2022).

De igual manera, el Ministerio de Tecnologías de la Información y las Comunicaciones expide la Resolución 00473, actualizada en la Resolución 3066 del mismo año, en donde se establece que el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia -ColCERT estará adscrito a dicho ministerio bajo la dirección del Viceministerio de Transformación Digital y tendrá como una de sus funciones "Actuar como punto único de contacto y coordinación para responder de manera rápida y eficiente a incidentes y vulnerabilidades de Seguridad Digital para la gestión de amenazas e incidentes de Seguridad Digital Nacional" (Resolución 03066, 2022, pg. 20).

De acuerdo con lo anterior, se evidencia que en materia de Política Nacional de Seguridad Digital, Colombia se ha caracterizado por ser un país donde se han creado marcos de normativos en materia de ciberseguridad. Sin embargo, la aplicación de los mismos se ha visto frenada ante la falta de coordinación de las instancias creadas, así como la falta de asignación presupuestal destinada al sector, lo que conlleva a no contar con el personal necesario para aplicar la normatividad.

En conclusión, es necesaria la creación de una Agencia Nacional de Seguridad Digital que cumpla el rol de ser la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de Seguridad Digital y Ciberdefensa Nacional, tal como ocurre en otros países.

Agencias Internacionales de Seguridad Digital:

Según cifras de TicTac (2022), cada minuto la economía mundial pierde US$11,4 millones por delitos asociados con el cibercrimen. Se estima que para el 2015 el costo global del cibercrimen ascienda a los US$10,5 billones. Así mismo, para el 2031 se calcula que habrá un ataque de ransomware cada dos segundos a negocios, usuarios o dispositivos

Surfshark (2022) publicó el estudio "Cybercrime statistics" en el cual da a conocer un panorama sobre la ciberdelincuencia a nivel global, en el cual se afirma que, en países como Estados Unidos, Irán, Israel, Emiratos Árabes y Qatar, el 50% de los correos electrónicos de cada 100 usuarios de internet han sido vulnerados por los ciberdelincuentes.

Ante el auge del cibercrimen, y con el fin de tener políticas preventivas, países alrededor del mundo han creado Agencias de Seguridad Digital, entendidas como estructuras organizativas especializadas que promuevan la coordinación, la colaboración, la respuesta eficiente y la educación en materia de Seguridad Digital, para así proteger las infraestructuras críticas y los datos personales de los ciudadanos. A continuación se presentan algunas Agencias de Seguridad Digital a nivel mundial:

NOMBRE	PAÍS	AÑO DE CREACIÓN	DESCRIPCIÓN
BSI - Bundesamt für Sicherheit in der Informationstechnik	Alemania	1991	Es responsable de la seguridad de la información y la ciberseguridad en el país. Tiene como objetivo proteger los sistemas de información y las infraestructuras críticas de Alemania, así como brindar asesoramiento y orientación a entidades públicas, privadas y ciudadanos en materia de seguridad cibernética.
ENISA - European Union Agency for Cybersecurity	Unión Europea	2004	Junto a la Red del Centro Nacional de Coordinación de la Unión Europea (NCCs) coordinan las políticas de innovación y política industrial en ciberseguridad de la Unión Europea. Busca fortalecer las capacidades en materia de tecnología para promover la economía y proteger a los ciudadanos de ataques cibernéticos.
ANSSI- Agence Nationale de la sécurité des systèmes d' information	Francia	2009	Creada por medio de la Ley de Programación Militar de Francia con el objetivo de proteger la información y la infraestructura crítica del país. Es la autoridad nacional en materia de seguridad cibernética y tiene la responsabilidad de cuidar los sistemas de información críticos del gobierno, empresas y organizaciones clave en Francia.

ACSC- Australian Cyber Security Agency	Australia	2014	Establecido como iniciativa del Gobierno para fortalecer y coordinar la ciberseguridad en el país. Se encarga de proporcionar orientación, inteligencia, asesoramiento y respuesta a incidentes de ciberseguridad.
NCSC- National Cyber Security Centre	Reino Unido	2016	Tiene la responsabilidad de proteger al Reino Unido contra amenazas cibernéticas proporcionando orientación y asesoramiento en Seguridad Digital y coordinar la respuesta a incidentes cibernéticos a nivel nacional.
CISA- Cybersecurity and Infraestructura Security Agency	Estados Unidos	2018	Es una Agencia adscrita al Departamento de Seguridad Nacional de los Estados Unidos y tiene la responsabilidad de proteger la infraestructura crítica del país, de promover la seguridad cibernética y coordinar la respuesta del país ante incidentes cibernéticos.

CCCS - Canadian Centre for Cyber Security	Canadá	2018	Tiene la responsabilidad de proteger y defender las redes de información y sistemas de Canadá ante amenazas cibernéticas. Proporciona asesoramiento y orientación en ciberseguridad tanto a entidades del estado, como al sector privado del país. Busca promover la colaboración y la cooperación en materia de ciberseguridad a nivel nacional e internacional.

* Tabla de elaboración propia con información de las diferentes Agencias mencionadas

COMENTARIOS DE LOS PONENTES

La necesidad de contar con una institucionalidad que adopte las políticas e imparta lineamientos en materia de seguridad digital, tanto a nivel público como privado y tanto en los aspectos operativos de cada entidad o persona jurídica de derecho privado como en lo industrial y en lo relativo a la intimidad de las personas naturales, es incuestionable. Esta institucionalidad, además, debe estar dotada desde el rango de ley de la máxima autoridad y tener dedicación exclusiva en la materia para que pueda tener la capacidad jurídica y técnica de dirigir y articular las acciones tendientes a garantizar la seguridad digital del país.

El Gobierno Nacional, con el apoyo de algunos Congresistas, presentó el 25 de julio de 2023 ante la Cámara de Representantes el Proyecto de Ley 023 de 2023 Cámara "Por la cual se crea la Agencia Nacional de Seguridad Digital y Asuntos Espaciales", que versa sobre la misma materia que el presente proyecto de ley. No obstante, el Proyecto de Ley 023 de 2023/ Cámara propone crear una Agencia que no solo tenga la misión de liderar y articular las políticas y lineamientos en Seguridad Digital sino también en Asuntos Espaciales.

Esta propuesta podría causar conflictos de interés entre ambas dependencias y dificultará la eficiencia y efectividad de sus operaciones, así mismo, distraerá recursos y esfuerzos que deberían distirbuirse de manera separada. Tanto la Seguridad Digital como la exploración espacial son campos altamente especializados que demandan expertos con conocimientos técnicos específicos, mezclar ambas agencias podría dificultar la contratación y retención de profesionales capacitados en cada área. La ciberseguridad y la investigación espacial tienen necesidades y prioridades distintas.

Cabe mencionar que Colombia sería el único país que le asignaría competencias sobre ambos asuntos a una misma autoridad. Como se indicó en el acápite de "Contexto Actual", los países líderes en Ciberseguridad tienen entidades dedicadas exclusivamente a la seguridad digital. Países como Estados Unidos, Canadá, Reino Unido, Australia y Brasil, por ejemplo, cuentan con entidades independientes para seguridad digital y asuntos espaciales. En Chile se está tramitando proyecto de Ley que crea una Agencia de Ciberseguridad, exclusivamente. Queda en evidencia, entonces, que las buenas prácticas sugieren tener una

autoridad específicamente dedicada a liderar y articular las políticas, estrategias, acciones y lineamientos en materia de Seguridad Digital.

Así mismo, el Proyecto de Ley 023 de 2023/Cámara contempla que la Agencia de Ciberseguridad esté adscrita al Departamento Administrativo de la Presidencia de la República, aspecto que consideramos dificultará la confianza de intercambio de información necesaria para prevenir posibles ciberataques en empresas privadas y entidades del sector público.

En este momento solo cuatro agencias están adscritas al Departamento Administrativo de la Presidencia y ninguna de ellas está enfocada en aspectos relacionados con tecnologías de la información o seguridad digital y aunque estos temas sean transversales a las demás carteras del Estado es el Ministerio de Tecnologías de la Información y las Comunicaciones el que posee la información sobre cómo ejecutar las políticas públicas en la materia, sería un retroceso cambiar de coordinador de la gestión en seguridad digital, sobre todo en materia de protección de datos.

Consideramos que la generación, coordinación y aplicación de la política de Seguridad Digital del país debe ser una política de Estado y no de Gobierno, por ello se debe velar por su independencia y su autonomía con el paso del tiempo.

REFERENCIAS

BluRadio. (2022, Noviembre 10). Más de 10 teras de información sensible de la Fiscalía estarían "secuestradas" por hackers. Blu Radio. Recuperado el 12 de mayo de 2023, de https://www.bluradio.com/judicial/mas-de-10-teras-de-informacion-sensible-de-la-fiscalia-estarian-secuestradas-por-hackers-rg10

CEPAL. (2011, Abril). *De las Telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09)*. Repositorio CEPAL. Retrieved May 17, 2023, from https://repositorio.cepal.org/bitstream/handle/11362/4818/1/S110124_es.pdf

CEPAL. (2021). Infraestructura resiliente: un imperativo para el desarrollo sostenible en América Latina y el Caribe. Repositorio CEPAL. Recuperado el 16 de mayo de 2023, de https://repositorio.cepal.org/bitstream/handle/11362/46646/1/S2000675_es.pdf

Dirección Nacional de Planeación. (2011, 14 de julio). CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa. Subdirección de Gestión y Desarrollo del Talento Humano. Recuperado el 15 de mayo de 2023, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Dirección Nacional de Planeación. (2016, 11 de abril). CONPES 3855 Política Nacional de Seguridad Digital en Colombia. Subdirección de Gestión y Desarrollo del Talento Humano. Recuperado el 15 de mayo de 2023, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. Hérodote, (152-153), 3-21. https://dialnet.unirioja.es/servlet/articulo?codigo=4743862

Google. (2022, Diciembre 7). Fog of War. Google. Recuperado el 16 de mayo de 2023, de https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

IBM. (2023). IBM Security X-Force Threat Intelligence Index 2023. https://www.ibm.com/reports/threat-intelligence

INFOBAE. (2023). Confirmaron ataque cibernético a la plataforma SECOP II. Infobae. Recuperado el 15 de mayo de 2023, de https://www.infobae.com/colombia/2023/05/03/confirmaron-ataque-cibernetico-a-la-plataforma-secop-ii/

La Republica. (2022, Septiembre 30). El costo global del cibercrimen en 2025 ascenderá a un total de US$10,5 billones. LaRepublica.co. Recuperado el 16 de mayo de 2023, de https://www.larepublica.co/empresas/el-costo-global-del-cibercrimen-en-2025-ascendera-a-un-total-de-us-10-5-billones-3458183

Lesmes, L. (2023, Abril 10). Ciberseguridad en Colombia: datos sobre ciberataques en el país - Novedades Tecnología - Tecnología. El Tiempo. Recuperado Mayo 12, 2023 de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-757651

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Resolución 03066 [Por la cual se crean Grupos Internos de Trabajo del Ministerio de Tecnologías de la Información y las Comunicaciones, se asignan funciones y se derogan unas Resoluciones]. Recuperado el 12 de mayo de 2023, de https://mintic.gov.co/portal/715/articles-162594_recurso_4.pdf

NCSI. (2022). National Cyber Security Index. NCSI. Recuperado el 12 de mayo de 2023, de https://ncsi.ega.ee/ncsi-index/

Policía Nacional de Colombia. (2015). Resolución 05839. Recuperado de https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

Portafolio. (2022, Diciembre 21). EPS Sanitas: detalles del ciberataque que sufrió | Grupo Keralty | Empresas | Negocios. Portafolio. Recuperado el 12 de mayo de 2023, de https://www.portafolio.co/negocios/empresas/eps-sanitas-detalles-del-ciberataque-que-sufrio-grupo-keralty-575968

Surfshark. (2022). Cybercrime statistics. Surfshark. Recuperado el 16 de mayo de 2023, de https://surfshark.com/research/data-breach-impact/statistics

World Economic Forum. (n.d.). Global Cybersecurity Outlook 2023 | Weforum. Weforum. Recuperado el 16 de mayo de 2023, de https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

World Economic Forum. (2023). The Global Risks Report 2023. Recuperado de https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

World Economic Forum. (2023, Marzo 1). Esa es la razón por la que debemos reforzar la ciberseguridad en esta era de policrisis. El Foro Económico Mundial. Recuperado el 16 de mayo de 2023, de https://es.weforum.org/agenda/2023/03/ciberseguridad-en-la-era-de-la-policrisis/

4. CONFLICTOS DE INTERÉS:

Dando cumplimiento a lo establecido en el artículo 3 de la Ley 2003 del 19 de noviembre de 2019, por la cual se modifica parcialmente la Ley 5 de 1992, se hacen las siguientes consideraciones:

Se estima que de la discusión y aprobación del presente Proyecto de Ley no podría generarse un conflicto de interés en consideración al interés particular, actual y directo de los congresistas, de su cónyuge, compañero o compañera permanente, o parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil, por cuanto se tratan de disposiciones de carácter general.

Sobre este asunto ha señalado el Consejo de Estado (2019):

"No cualquier interés configura la causal de desinvestidura en comento, pues se sabe que sólo lo será aquél del que se pueda predicar que es directo, esto es, que per se el alegado beneficio, provecho o utilidad encuentre su fuente en el asunto que fue conocido por el legislador; particular, que el mismo sea específico o personal, bien para el congresista o quienes se encuentren relacionados con él; y actual o inmediato, que concurra para el momento en que ocurrió la participación o votación del congresista, lo que excluye sucesos contingentes, futuros o imprevisibles. También se tiene noticia que el interés puede ser de cualquier naturaleza, esto es, económico o moral, sin distinción alguna".

De igual forma, es pertinente señalar lo que la Ley 5 de 1992 dispone sobre la materia en el artículo 286, modificado por el artículo 1 de la Ley 2003 de 2019:

"Se entiende como conflicto de interés una situación donde la discusión o votación de un proyecto de ley o acto legislativo o artículo, pueda resultar en un beneficio particular, actual y directo a favor del congresista.

a) Beneficio particular: aquel que otorga un privilegio o genera ganancias o crea indemnizaciones económicas o elimina obligaciones a favor del congresista de las que no gozan el resto de los ciudadanos. Modifique normas que afecten investigaciones penales, disciplinarias, fiscales o administrativas a las que se encuentre formalmente vinculado.

b) Beneficio actual: aquel que efectivamente se configura en las circunstancias presentes y existentes al momento en el que el congresista participa de la decisión.

c) Beneficio directo: aquel que se produzca de forma específica respecto del congresista, de su cónyuge, compañero o compañera permanente, o parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil."

No obstante lo expuesto, se recuerda que si un congresista considera que se encuentra impedido, deberá manifestarlo oportunamente.

5. PLIEGO DE MODIFICACIONES:

TEXTO DEFINITIVO PRIMER DEBATE SENADO DE LA REPÚBLICA	PROPUESTA DE MODIFICACIONES	JUSTIFICACIÓN
ARTÍCULO 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad que coordinará, definirá y hará seguimiento a las políticas de seguridad digital implementadas por las entidades públicas y las personas naturales y jurídicas de derecho privado. Establecerá las obligaciones y deberes que tienen los órganos del Estado para determinar los requisitos mínimos para la	**ARTÍCULO 1. Objeto.** La presente ley tiene por objeto establecer la institucionalidad que coordinará, definirá y hará seguimiento a las políticas de seguridad digital **o ciberseguridad,** implementadas por las entidades públicas y las personas naturales y jurídicas de derecho privado. Establecerá las obligaciones y deberes que tienen los órganos del Estado para determinar los requisitos mínimos para la prevención, resolución y	Se adiciona la palabra "ciberseguridad" porque en el contexto del proyecto se habla de ciberseguridad. Se adicionan las obligaciones y deberes que tienen los órganos del Estado para determinar los incidentes de ciberseguridad

prevención, resolución y respuesta de incidentes de ciberseguridad.	respuesta de incidentes de ciberseguridad.	
ARTÍCULO 2. Principios. En el desarrollo, interpretación y aplicación de la presente Ley, además de los principios constitucionales, se aplicarán los que a continuación se prevén: **Principio de Coordinación**: Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto de la presente ley. **Principio de Confidencialidad**: Todas las personas y organizaciones que intervengan en materia de seguridad digital que tengan acceso a información que no tenga la naturaleza de información pública están obligadas a garantizar la reserva de esta, según corresponda y a través de mecanismos idóneos, inclusive después de finalizada su relación con alguna de las labores que comprende la gestión del riesgo. **Principio de Cooperación:** En el marco de las relaciones nacionales e internacionales en materia de seguridad digital, aunarán esfuerzos para el logro de los objetivos de seguridad digital del país. **Principio de Enfoque basado en riesgos**: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque basado en riesgos de forma tal que la definición y aplicación de controles y la toma de decisiones, siempre considere los riesgos como insumo principal. **Principio Perspectiva Interseccional:** La Agencia desarrollará sus funciones en consideración de las particularidades de los distintos grupos poblacionales y se regirá con un enfoque de inclusión interseccional en términos de sexo, identidad de género, raza, etnia, capacidad económica, clase social,	**ARTÍCULO 2. Principios.** En el desarrollo, interpretación y aplicación de la presente Ley, además de los principios constitucionales, se aplicarán los que a continuación se prevén: **Principio de Coordinación**: Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto de la presente ley. **Principio de Confidencialidad**: Todas las personas y organizaciones que intervengan en materia de seguridad digital que tengan acceso a información que no tenga la naturaleza de información pública están obligadas a garantizar la reserva de esta, según corresponda y a través de mecanismos idóneos, inclusive después de finalizada su relación con alguna de las labores que comprende la gestión del riesgo. **Principio de Cooperación:** En el marco de las relaciones nacionales e internacionales en materia de seguridad digital, aunarán esfuerzos para el logro de los objetivos de seguridad digital del país. **Principio de Enfoque basado en riesgos**: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque basado en riesgos de forma tal que la definición y aplicación de controles y la toma de decisiones, siempre considere los riesgos como insumo principal. **Principio Perspectiva Interseccional:** La Agencia desarrollará sus funciones en consideración de las particularidades de los distintos grupos poblacionales y se regirá con un enfoque de inclusión interseccional en términos de sexo, identidad de género, raza, etnia, capacidad económica, clase social, orientación política y edad; abordando los riesgos e impactos	Se agrega el principio de Protección de Datos y Privacidad como elementos clave de la ANSD.

orientación política y edad; abordando los riesgos e impactos diferenciados de las amenazas y riesgos para que la ciberseguridad responda a necesidades, prioridades y percepciones diferenciadas basadas en las particularidades de cada grupo poblacional. **Principio de Integridad**: El Estado desarrollará, a través de las entidades y organismos competentes las acciones necesarias para elevar la confiabilidad y la exactitud de los datos o información de forma que se evite su manipulación, su adulteración y cambios por personas, entidades o procesos no autorizados. **Principio de Neutralidad Tecnológica** El Estado garantizará la libre adopción de tecnologías que permitan fomentar la eficaz gestión de la seguridad de la información y la ciberseguridad, sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos. **Respeto a la privacidad**: La seguridad de la información y la ciberseguridad son base del aseguramiento de la privacidad y protección de datos personales, y su gestión deberá incluir medidas formales de protección de la privacidad. La gestión de la seguridad de la información y la ciberseguridad deberá igualmente, en todo momento, respetar la privacidad de las personas.	diferenciados de las amenazas y riesgos para que la ciberseguridad responda a necesidades, prioridades y percepciones diferenciadas basadas en las particularidades de cada grupo poblacional. **Principio de Integridad**: El Estado desarrollará, a través de las entidades y organismos competentes las acciones necesarias para elevar la confiabilidad y la exactitud de los datos o información de forma que se evite su manipulación, su adulteración y cambios por personas, entidades o procesos no autorizados. **Principio de Neutralidad Tecnológica** El Estado garantizará la libre adopción de tecnologías que permitan fomentar la eficaz gestión de la seguridad de la información y la ciberseguridad, sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos. **Respeto a la privacidad**: La seguridad de la información y la ciberseguridad son base del aseguramiento de la privacidad y protección de datos personales, y su gestión deberá incluir medidas formales de protección de la privacidad. La gestión de la seguridad de la información y la ciberseguridad deberá igualmente, en todo momento, respetar la privacidad de las personas. **Principio de Protección de Datos Personales: Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.** **Principio de Privacidad: Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el Régimen de Protección de Datos Personales.**	

ARTÍCULO 3. Definiciones. Para los efectos de la presente Ley, se adoptan las siguientes definiciones: a. **Agencia:** Es la Agencia Nacional de Seguridad Digital. b. **Amenazas:** Causa potencial de un incidente no deseado, el cual puede resultar en el daño a un sistema, individuo u organización. c. **Ciberataque:** Incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, filtrar, robar, hacer uso o acceder de manera ilícita a un activo de información o de tecnologías de la información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica. d. **Ciberdefensa**: Capacidad para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la seguridad *nacional*. e. **Ciberdiplomacia**: Uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio. f. **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 y para almacenar, modificar e intercambiar datos. g. **Ciberseguridad:** Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante	**ARTÍCULO 3. Definiciones.** Para los efectos de la presente Ley, se adoptan las siguientes definiciones: a. **Agencia:** Es la Agencia Nacional de Seguridad Digital. b. **Amenazas:** Causa potencial de un incidente no deseado, el cual puede resultar en el daño a un sistema, individuo u organización. c. **Ciberataque:** Incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, filtrar, robar, hacer uso o acceder de manera ilícita a un activo de información o de tecnologías de la información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica. d. **Ciberdefensa**: Capacidad para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la seguridad nacional. e. **Ciberdiplomacia**: Uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio. f. **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 y para almacenar, modificar e intercambiar datos. g. **Ciberseguridad:** ~~Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación,~~	Se modifica el concepto de Ciberseguridad con el fin de que tenga un enfoque hacía la confianza de la ciudadanía y el fortalecimiento de las economías digitales y no se entienda con un enfoque militarista, ya no usado en la concepción actual de ciberseguridad, apoyada por la OCDE. Se incluye la definición de delitos ciberneticos, delitos ciber habilitados a seguridad informática, sistema de información y Equipo de respuesta a incidentes con el fin de hacer claridad sobre dichos conceptos.

amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin. h. **Ecosistema Digital:** Conjunto de infraestructuras y prestaciones (plataformas, dispositivos de acceso) asociadas a la provisión de contenidos y servicios a través de Internet. Este es un sujeto de análisis fundamental para la definición de políticas públicas, en áreas tan diversas como la digitalización de procesos productivos y la protección de la privacidad de los usuarios. i. **Incidente:** Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital. j. **Infraestructuras críticas:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.	~~confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin.~~ **Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.** **h. Delitos cibernéticos: Aquellos que afectan la disponibilidad, integridad y confidencialidad de la información y los sistemas digitales. Estos solo pueden cometerse a través y en contra de un sistema informático.** **i. Delitos ciber habilitados: Aquellos que existían de forma previa a las TICs, pero que, con el desarrollo de éstas, ahora se desarrollan también mediante la modalidad cibernética.** j. **Ecosistema Digital:** Conjunto de infraestructuras y prestaciones (plataformas, dispositivos de acceso) asociadas a la provisión de contenidos y servicios a través de Internet. Este es un sujeto de análisis	

k. **Riesgo:** La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información. l. **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y 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. m. **Vulnerabilidad:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.	fundamental para la definición de políticas públicas, en áreas tan diversas como la digitalización de procesos productivos y la protección de la privacidad de los usuarios. k. **<u>Equipo de respuesta a incidentes de seguridad informática:</u>** <u>Grupo de especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, para actuar de acuerdo a procedimientos y políticas predefinidas, que colaboren en resolver la situación presentada.</u> l. **Incidente:** Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital. m. **Infraestructuras críticas:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. **n. Protección de Datos Personales:** Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales. o. **Privacidad:** Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el	

	Régimen de Protección de Datos Personales. p. **Riesgo:** La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información. q. **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y 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. r. **Sistema de Información.** Medio por el cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí. s. **Vulnerabilidad:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.	
ARTÍCULO 4. Creación y naturaleza jurídica de la Agencia. Créase la Agencia Nacional de Seguridad Digital, como una entidad descentralizada del orden nacional, de naturaleza especial que forma parte de la Rama Ejecutiva, con personería jurídica,	Sin modificaciones.	

autonomía administrativa, financiera y patrimonio propio, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones. **Parágrafo.** La Agencia es la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de seguridad digital.		
ARTÍCULO 5. Misión. La Agencia es responsable de: a) liderar y fortalecer la gestión del ecosistema digital, coadyuvar en mantener un modelo de Ciberseguridad y la gestión de seguridad de la Información en las entidades del estado y de las personas naturales y jurídicas de derecho privado; b) articular la identificación de las infraestructuras críticas del país con las autoridades y entidades competentes; y c) coordinar y cooperar con la identificación de amenazas, vulnerabilidades, con el propósito de asegurar las plataformas del estado a través de la confidencialidad, integridad y disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento, asociados a los sistemas de información de la Entidades o en el ciberespacio para uso de la ciudadanía y del estado colombiano.	**ARTÍCULO 5. Misión.** La Agencia es responsable de: a) liderar y fortalecer la gestión del ecosistema digital, coadyuvar en mantener un modelo de Ciberseguridad y la gestión de seguridad de la Información en las entidades del estado y de las personas naturales y jurídicas de derecho privado; b) articular la identificación de las infraestructuras críticas del país con las autoridades y entidades competentes;~~—y~~ c) coordinar y cooperar con la identificación de amenazas, vulnerabilidades, con el propósito de asegurar las plataformas del estado a través de la confidencialidad, integridad y disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento, asociados a los sistemas de información de la Entidades o en el ciberespacio para uso de la ciudadanía y del estado colombiano; **y d) generar y coordinar programas de concientización para los colombianos acerca de la detección de amenazas cibernéticas y desarrollar líneas de acción para el fortalecimiento de la industria de Seguridad Digital en el país.**	Se agrega el numeral d) con el fin de establecer una misión pedagógica sobre aspectos clave en Seguridad Digital para los ciudadanos; así como fortalecer la industria de Seguridad Digital del país.
ARTÍCULO 6. Domicilio. La Agencia tendrá como domicilio principal la ciudad de Bogotá, D. C.	Sin modificaciones.	
ARTÍCULO 7. Objetivos. La Agencia será un organismo de carácter técnico especializado que tendrá como objeto la planificación, articulación y coordinación de las políticas de gestión de los riesgos de seguridad digital en el país,	Sin modificaciones.	

prevención de amenazas internas o externas contra el ecosistema digital del país, fortalecimiento de la confianza y seguridad de todas las partes interesadas en el ámbito digital. **PARÁGRAFO.** La Agencia no tendrá competencias de policía judicial, ni las que le corresponden a los organismos de inteligencia y contrainteligencia del Estado. En el ejercicio de sus funciones esta entidad garantizará el derecho de hábeas data, el derecho a la intimidad, a la privacidad, a la libertad de expresión en entornos digitales y al buen nombre de los ciudadanos. Cualquier información que obtenga, recopile, almacene, use, circule o suprima la Agencia deberá tratarse exclusivamente en el marco de sus competencias legales, y solo podrá ser usada, entregada o transferida a otros organismos con previa autorización judicial.		
ARTICULO 8. Régimen jurídico. Los actos unilaterales que realice la Agencia para el desarrollo de sus actividades son actos administrativos y estarán sujetos a las disposiciones del derecho público. Los contratos que deba celebrar la Agencia se regirán, por regla general, por las normas de contratación pública. Excepcionalmente, respecto de los contratos que se tengan que realizar para el desarrollo del objeto misional de la Agencia, dicha contratación se regirá por el derecho privado, aplicando los principios de la función administrativa y de la gestión fiscal y estarán sometidos al régimen de inhabilidades e incompatibilidades previsto para la contratación estatal. La Agencia, expedirá un manual de contratación en la cual se reglamente lo previsto en este inciso.	Sin modificaciones.	
ARTÍCULO 9. Funciones de la Agencia. La Agencia tendrá, entre otras, las siguientes funciones:	**ARTÍCULO 9. Funciones de la Agencia.** La Agencia tendrá, entre otras, las siguientes funciones:	1.6 Se agrega esta función con el propósito de trabajar en coordinación con el Ministerio de Relaciones Exteriores aquellos

1. Coordinación y colaboración: 1.1. Coordinar y gestionar, como punto de contacto único, la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que brinde información a los ciudadanos sobre los ciberataques que tengan impacto en el territorio nacional. 1.2. Coordinar con los actores del ecosistema de seguridad digital, el entendimiento y fortalecimiento de la gestión de los riesgos e incidentes de seguridad digital, ciberseguridad y protección de datos de la información que soportan la operación del estado. 1.3. Liderar la implementación de políticas tendientes al fortalecimiento del nivel de madurez de seguridad digital en las entidades del estado y coadyuvar en la implementación de mejores prácticas de seguridad en los sectores económicos y en la ciudadanía. 1.4. Adelantar acuerdos de cooperación internacional en temas relacionados con Seguridad Digital, Seguridad de la Información, Ciberseguridad, y Privacidad, tanto a nivel de protección de la información y las tecnologías de la información asociadas como las tecnologías operacionales propias de las infraestructuras y sectores críticos, teniendo en cuenta las políticas de	1. Coordinación y colaboración: 1.1. Coordinar y gestionar, como punto de contacto único, la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que brinde información a los ciudadanos sobre los ciberataques que tengan impacto en el territorio nacional. 1.2. Coordinar con los actores del ecosistema de seguridad digital, el entendimiento y fortalecimiento de la gestión de los riesgos e incidentes de seguridad digital, ciberseguridad y protección de datos de la información que soportan la operación del Estado. 1.3. Liderar la implementación de políticas tendientes al fortalecimiento del nivel de madurez de seguridad digital en las entidades del Estado y coadyuvar en la implementación de mejores prácticas de seguridad en los sectores económicos y en la ciudadanía. 1.4. Adelantar acuerdos de cooperación internacional en temas relacionados con Seguridad Digital, Seguridad de la Información, Ciberseguridad, y Privacidad, tanto a nivel de protección de la información y las tecnologías de la información asociadas como las tecnologías operacionales propias de las infraestructuras y sectores críticos, teniendo en cuenta las políticas de Gobierno y la normativa vigente, dentro del marco de los tratados	aspectos que tengan relación con ciberdiplomacia. 3.2 Se incluye en los programas de educación la investigación y el entrenamiento. Así como el hecho de promover el desarrollo nacional de una cultura de ciberseguridad. 3.4 La Agencia será la encargada de representar al Gobierno Nacional en eventos relacionados con su misión. Se agrega esta función al articulado 3.5 Colombia debe fortalecer su investigación y desarrollo tecnológico en temas de ciberseguridad. La Agencia, en conjunto con el Ministerio de Ciencia, Tecnología e Innovación será la responsable de la creación de la hoja de ruta que seguirá el país para desarrollar estas habilidades necesarias para el desarrollo profesional de los colombianos. 3.6 Es importante disminuir las falencias en el número de profesionales en las áreas de ciberseguridad y atender los requerimientos de la industria TIC. Esta función garantiza que los colombianos tengan facilidades a la hora de decidir un camino profesional en estas áreas del conocimiento. 4.1. se incluye en el numeral a dictar instrucciones circulares, órdenes de carácter general 4.4 Se agrega como función la creación del Observatorio de Seguridad Digital y Ciberdefensa, así como las entidades del Estado que son claves para su desarrollo. 5.6 Se establece la promoción y consolidación de los CSIRTS (Equipos de respuesta a incidentes de seguridad informática) claves para la protección de las infraestructuras críticas del país. 5.7. Se establece crear el registro nacional de incidentes de ciberseguridad en el cuál se ingresaran los datos técnicos y antecedentes de estos sucesos

Gobierno y la normativa vigente, dentro del marco de los tratados internacionales vinculantes para Colombia y del respeto de la facultad del Presidente de la República de dirigir las relaciones internacionales. 1.5. Organizar y coordinar una Comisión Intersectorial de Inteligencia Artificial que monitoree el desarrollo y uso de tecnologías que procesan datos que reciben y responden ante ellos, aprenden, razonan, planifican e incluso generan predicciones, y expida lineamientos, estándares e instrucciones tendientes a garantizar la seguridad de dichas tecnologías y a prevenir y mitigar los riesgos que de ellas se derivan. 2. Evaluación y mitigación de riesgos: 2.1. Asegurar el ecosistema digital y su gobernanza, de acuerdo con la dirección estratégica del gobierno nacional y establecer los lineamientos y/o políticas en materia de seguridad y gobernanza del ecosistema. 2.2. Contribuir a la protección y defensa del ciberespacio ante actos de penetración, infiltración, espionaje, sabotaje u otras actividades cuando atenten gravemente contra la administración pública y las infraestructuras críticas y proteger a las instituciones de	internacionales vinculantes para Colombia y del respeto de la facultad del Presidente de la República de dirigir las relaciones internacionales. 1.5. Organizar y coordinar una Comisión Intersectorial de Inteligencia Artificial que monitoree el desarrollo y uso de tecnologías que procesan datos que reciben y responden ante ellos, aprenden, razonan, planifican e incluso generan predicciones, y expida lineamientos, estándares e instrucciones tendientes a garantizar la seguridad de dichas tecnologías y a prevenir y mitigar los riesgos que de ellas se derivan. **1.6. <u>Coordinar y colaborar con agencias de seguridad digital y ciberdefensa de otros países, organismos internacionales y del sector privado con el fin de intercambiar información que pueda abordar los desafíos cibernéticos y coordinar con el Ministerio de Relaciones Exteriores, las acciones de ciberdiplomacia que se requieran para dicho fin.</u>** 2. Evaluación y mitigación de riesgos: 2.1. Asegurar el ecosistema digital y su gobernanza, de acuerdo con la dirección estratégica del gobierno nacional y establecer los lineamientos y/o políticas en materia de	

nivel nacional y territorial de la influencia de organizaciones criminales. 2.3. Contribuir a la protección de recursos tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público. 2.4. Brindar asesoría y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en seguridad digital y ciberdefensa. 2.5. Dictar protocolos, estándares e instrucciones generales que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información del país, para reducir los riesgos de seguridad digital de las entidades del estado, de los diferentes sectores económicos y de los ciudadanos. 2.6. Crear y coordinar un observatorio encargado de realizar análisis de amenazas cibernéticas, y colaborar con entidades públicas, sector privado y ciudadanos en el entendimiento de tácticas, técnicas y procedimientos de los delincuentes ante eventuales ciberataques, de recolectar información y de monitorear ataques tanto a nivel nacional e internacional. El observatorio trabajará en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, el	seguridad y gobernanza del ecosistema. 2.2. Contribuir a la protección y defensa del ciberespacio ante actos de penetración, infiltración, espionaje, sabotaje u otras actividades cuando atenten gravemente contra la administración pública y las infraestructuras críticas y proteger a las instituciones de nivel nacional y territorial de la influencia de organizaciones criminales. 2.3. Contribuir a la protección de recursos tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público. 2.4. Brindar asesoría y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en seguridad digital y ciberdefensa. 2.5. Dictar protocolos, estándares e instrucciones generales que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información del país, para reducir los riesgos de seguridad digital de las entidades del Estado, de los diferentes sectores económicos y de los ciudadanos. 2.6. Crear y coordinar un observatorio encargado de realizar análisis de amenazas cibernéticas, y colaborar con entidades públicas, sector privado y ciudadanos en el entendimiento de tácticas, técnicas y	

Ministerio de Defensa, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Relaciones Exteriores y el Ministerio de Educación. Los análisis y estudios elaborados por el Observatorio se presentarán al Consejo Directivo a través de informes por lo menos una vez al año. 3. Educación y prevención: 3.1. Fortalecer las capacidades y competencias en seguridad digital de los servidores públicos, trabajadores oficiales, contratistas, proveedores y demás grupos de interés que accedan a la información del estado colombiano. 3.2. Ofrecer en coordinación con el Ministerio de Educación Nacional programas de educación y concientización dirigidos a entidades públicas, sector privado y a los ciudadanos sobre ciberdefensa y gestión de amenazas, riesgos y ciberataques. 3.3. Trabajar de manera conjunta con instituciones educativas y de investigación en temas relacionados con seguridad digital y la ciberdefensa, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar los riesgos de ciberataques y de promover la innovación en soluciones de	procedimientos de los delincuentes ante eventuales ciberataques, de recolectar información y de monitorear ataques tanto a nivel nacional e internacional. El observatorio trabajará en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Relaciones Exteriores y el Ministerio de Educación. Los análisis y estudios elaborados por el Observatorio se presentarán al Consejo Directivo a través de informes por lo menos una vez al año. 3. Educación y prevención: 3.1. Fortalecer las capacidades y competencias en seguridad digital de los servidores públicos, trabajadores oficiales, contratistas, proveedores y demás grupos de interés que accedan a la información del Estado colombiano. 3.2. Ofrecer en coordinación con el Ministerio de Educación Nacional programas de educación y concientización dirigidos a entidades públicas, sector privado y a los ciudadanos sobre investigación entrenamiento de ciberdefensa y gestión de amenazas, riesgos y ciberataques.Promover el desarrollo nacional	

seguridad digital y ciberdefensa. 4. Planificación: 4.1. Diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa, el cual contendrá programas, lineamientos y estándares en materia de seguridad digital, de conformidad con recomendaciones y estándares internacionales. 4.2. La planificación y articulación de actividades orientadas a la identificación y caracterización de activos de información, activos relacionados y activos de infraestructuras críticas; 4.3. Planear, desarrollar, mantener y mejorar de forma continua los modelos de Ciberseguridad y gestión de seguridad de la Información para ambientes de tecnologías de la información y de sectores críticos y/o de control industrial operacional. 5. De ejecución: 5.1. Desarrollar actividades de Seguridad digital bajo sus principios rectores, en cumplimiento del marco legal y objetivo misional, con las autoridades y entidades competentes. 5.2. Promover el fortalecimiento y la consolidación de los equipos de respuesta a incidentes de seguridad informática de sectores que involucren	de una cultura de ciberseguridad. 3.3. Trabajar de manera conjunta con instituciones educativas y de investigación en temas relacionados con seguridad digital y la ciberdefensa, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar los riesgos de ciberataques y de promover la innovación en soluciones de seguridad digital y ciberdefensa. **3.4.** **Representar al Gobierno Nacional en conferencias especializadas y escenarios académicos internacionales y ante organismos multilaterales, en lo relacionado con la protección de la seguridad digital y ciberdefensa de la Nación** **3.5.** **Construir, en coordinación con el Ministerio de Ciencias, Tecnologías e Innovación, una hoja de ruta para fortalecer la investigación y desarrollo tecnológico en ciberseguridad y el asesoramiento en la creación de startups en la materia.** **3.6.** **Fomentar, en conjunto con el Ministerio de Educación Nacional, el estudio de carreras profesionales enfocadas en la ciberseguridad.** 4. Planificación: 4.1. Diseñar y publicar el Plan Nacional de Seguridad Digital y	

infraestructuras críticas. 5.3. Coadyuvar en el desarrollo, mantenimiento y mejora continua de los modelos de ciberseguridad y gestión de seguridad de la información para: i) entidades del estado a nivel de tecnologías de la información, y que sirva de base para las personas naturales y jurídicas de derecho privado; y ii) Infraestructura crítica y control industrial u operacional, sea su propiedad estatal, mixta, o privada. 5.4. Desarrollar actividades de protección del ecosistema digital en cooperación con los demás organismos nacionales e internacionales, así como con otras entidades del Estado y personas jurídicas de derecho privado que administren u operen infraestructuras críticas. 5.5. Ordenar el cese de operaciones en el ciberespacio ante un ataque que afecte la soberanía nacional y el ecosistema digital y su economía, en coordinación con el Ministerio de Defensa. 5.6. Las demás funciones relacionadas con las actividades de Seguridad Digital que le sean asignadas por el Presidente de la República de conformidad con la Constitución y la ley, siempre que se encuentren dentro del objeto señalado y cumplan con la condición de	Ciberdefensa, el cual contendrá programas,instrucciones, circulares, órdenes de carácter general y técnica; lineamientos y estándares en materia de seguridad digital, de conformidad con recomendaciones y estándares internacionales. 4.2. La planificación y articulación de actividades orientadas a la identificación y caracterización de activos de información, activos relacionados y activos de infraestructuras críticas; 4.3. Planear, desarrollar, mantener y mejorar de forma continua los modelos de Ciberseguridad y gestión de seguridad de la Información para ambientes de tecnologías de la información y de sectores críticos y/o de control industrial operacional. 4.4. **Constituir y coordinar el Observatorio de Seguridad Digital y Ciberdefensa, el cual tiene como fin reunir información sobre los ataques cibernéticos presentados a las infraestructuras críticas de la Nación, así como a empresas privadas y entidades del sector público. El Observatorio presentará sus informes mínimo una vez al año y trabajará en coordinación con el Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de**	

neutralidad de la presente ley. **PARÁGRAFO 1.** El Director General y los servidores públicos de la Agencia, desarrollarán y aplicarán los controles necesarios para garantizar que los procesos de planeación, recolección, procesamiento, análisis y difusión de la información se hagan de manera objetiva y en ningún caso se discriminará el ejercicio de sus funciones por razón de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político, o afectar los derechos y garantías de los partidos políticos de oposición. **PARÁGRAFO 2.** La Agencia desarrollará sus funciones en estricto cumplimiento del derecho de protección de los datos personales, de conformidad con la normativa vigente y en coordinación con la Superintendencia de Industria y Comercio.	**Tecnologías de la Información y el Ministerio de Educación Nacional, la Fiscalía General de la Nación y la Dirección Nacional de Inteligencia.** **4.5. Establecer que toda institución que posea infraestructura de la información calificada como crítica tendrá la obligación de informar a la agencia de Seguridad, los reportes de incidentes de ciberseguridad e informar respecto del plan de acción que adoptó.** 5. De ejecución: 5.1. Desarrollar actividades de Seguridad digital bajo sus principios rectores, en cumplimiento del marco legal y objetivo misional, con las autoridades y entidades competentes. 5.2. Promover el fortalecimiento y la consolidación de los equipos de respuesta a incidentes de seguridad informática de sectores que involucren infraestructuras críticas. 5.3. Coadyuvar en el desarrollo, mantenimiento y mejora continua de los modelos de ciberseguridad y gestión de seguridad de la información para: i) entidades del Estado a nivel de tecnologías de la información, y que sirva de base para las personas naturales y jurídicas de derecho privado; y ii) Infraestructura crítica y control industrial u	

		operacional, sea su propiedad estatal, mixta, o privada.	
		5.4. Desarrollar actividades de protección del ecosistema digital en cooperación con los demás organismos nacionales e internacionales, así como con otras entidades del Estado y personas jurídicas de derecho privado que administren u operen infraestructuras críticas.	
		5.5. Ordenar el cese de operaciones en el ciberespacio ante un ataque que afecte la soberanía nacional y el ecosistema digital y su economía, en coordinación con el Ministerio de Defensa.	
		5.6. **Promover la creación, el fortalecimiento y la consolidación de los CSIRTS (Equipos de respuesta a incidentes de seguridad informática) de sectores que involucren infraestructuras críticas, entre los que se cuentan, mínimamente de los sectores de salud; energía; transporte y servicios públicos; así como otros que considere pertinentes.**	
		5.7. **Crear el Registro Nacional de Incidentes de Ciberseguridad , el cual tendrá el carácter de reservado. En este registro se ingresaran los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con**	

	su análisis y estudio. sobre la base de este registro se podrán realizar las respectivas investigaciones por parte de la Agencia, asi como comunicar las alertas al Consejo técnico y elaborar recomendaciones para subsanar dichas brechas. 5.8. Las demás funciones relacionadas con las actividades de Seguridad Digital que le sean asignadas por el Presidente de la República de conformidad con la Constitución y la ley, siempre que se encuentren dentro del objeto señalado y cumplan con la condición de neutralidad de la presente ley. **PARÁGRAFO 1.** El Director General y los servidores públicos de la Agencia, desarrollarán y aplicarán los controles necesarios para garantizar que los procesos de planeación, recolección, procesamiento, análisis y difusión de la información se hagan de manera objetiva y en ningún caso se discriminará el ejercicio de sus funciones por razón de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político, o afectar los derechos y garantías de los partidos políticos de oposición. **PARÁGRAFO 2.** La Agencia desarrollará sus funciones en estricto cumplimiento del derecho de protección de los datos personales, de conformidad con la normativa vigente y en coordinación con la Superintendencia de Industria y Comercio.	
ARTÍCULO 10. Órganos de Dirección y Administración. La Dirección y administración de la Agencia, estarán a cargo de un	Sin modificaciones.	

Consejo Directivo y de un Director General, quien tendrá la representación legal de la misma. El Consejo Directivo, actuará como instancia máxima para orientar sus acciones y hacer seguimiento al cumplimiento de sus fines.		
ARTÍCULO 11. Funciones e Integración del Consejo Directivo. El Consejo Directivo será responsable de liderar la planificación, coordinación, articulación y gestión de los riesgos de seguridad digital y ciberseguridad en el país, incluyendo aquellos asociados a tecnologías operativas de infraestructura crítica y sistemas de control y actuación industrial, y será el soporte institucional y de coordinación para la definición, ejecución, seguimiento y el control de las estrategias, planes y acciones dirigidas a fortalecer la confianza y seguridad de todas las partes interesadas en el ámbito digital y de las infraestructuras críticas. El Consejo Directivo de la Agencia, estará integrado por cinco miembros, así: 1. Presidente de la Republica o a quien designe. 2. El Ministro de Defensa o su delegado. 3. El Director del Departamento Nacional de Planeación o su delegado. 4. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado. 5. El Superintendente de Industria y Comercio o su delegado. **PARAGRAFO 1:** El Consejo Directivo constituirá un Comité Público-Privado de Estrategia que será el encargado de la planeación de estrategias de largo plazo para fortalecer las capacidades en seguridad digital, potenciar el desarrollo de la industria de ciberseguridad en Colombia y promover la	Sin modificaciones	

educación de profesionales en el área. El Comité Público-Privado realizará recomendaciones al Consejo Directivo tendientes a atender las amenazas y los riesgos identificados en materia de seguridad digital y presentará informes de actualización sobre ataques perpetrados a nivel mundial y las formas de combatirlos mediante el uso de tecnologías de vanguardia y con los más altos estándares éticos. **PARÁGRAFO 2:** El Consejo Directivo, podrá crear grupos de trabajo ad hoc que aborden asuntos científicos y técnicos integrado por representantes de otras entidades públicas o privadas, representantes de los equipos de respuesta a incidentes de seguridad informática de Gobierno y sectoriales, representantes de organismos y gremios del sector privado nacional o internacional, y asesores y expertos de la industria, de la academia y de grupos empresariales o de consumidores, que podrá emitir recomendaciones específicas a nivel de sector y de tecnologías a implementar y participar con derecho a voz, pero sin voto en las reuniones del Consejo Directivo. **PARÁGRAFO 3:** El Consejo Directivo dictará su reglamento de funcionamiento. Las funciones del Consejo Directivo, y las reglas de creación y composición del Comité Público-Privado y de grupos de trabajo ad hoc se establecerán en el reglamento.		
ARTÍCULO 12. Director General y sus funciones. La administración de la Agencia, estará a cargo de un Director General, el cual tendrá la calidad de empleado público, elegido por el Presidente de la	Sin modificaciones.	

República, a partir de terna presentada por el Consejo Directivo, y será el representante legal de la entidad. Deberá cumplir con requisitos de estudios y experiencia mínimos que establecerá el Consejo Directivo. Son funciones del Director General las siguientes: 1. Dirigir, orientar, coordinar, vigilar y supervisar el desarrollo de las funciones a cargo de la Agencia. 2. Dirigir las actividades administrativas, financieras y presupuestales, y establecer las normas y procedimientos internos necesarios para el funcionamiento y prestación de los servicios de la Agencia. 3. Ejercer la representación de la Agencia y designar apoderados que representen a la Agencia en asuntos judiciales y extrajudiciales, para la defensa de los intereses de la misma. 4. Dirigir y promover la formulación de los planes, programas y proyectos relacionados con el cumplimiento de las funciones de la Agencia. 5. Presentar para aprobación del Consejo Directivo los estados financieros de la entidad. 6. Aprobar la estructuración técnica, legal y financiera de los proyectos a cargo de la Agencia. 7. Aprobar la estrategia de promoción de los proyectos de concesión u otras formas de Asociación Público-Privada. 8. Orientar y dirigir el seguimiento al desarrollo de los contratos de concesión a su cargo y, en caso de incumplimiento de cualquier obligación, adoptar de acuerdo con la		

ley las acciones necesarias. 9. Ordenar los gastos, expedir los actos y celebrar los convenios y contratos con personas naturales o jurídicas, así como con entidades públicas o privadas, nacionales o extranjeras, necesarios para el cumplimiento del objeto y funciones de la Agencia. 10. Someter a la aprobación del Consejo Directivo el Plan Estratégico Institucional y el Plan Operativo Institucional. 11. Promover la coordinación de la Agencia con las entidades u organismos públicos y privados. 12. Definir las políticas de comunicación de la Agencia y dar las instrucciones para que estas se cumplan de manera integral y coherente. 13. Proponer al Consejo Directivo la distribución, asignación y cobro de la contribución de valorización en los proyectos que lo requieran, de conformidad con la ley, y distribuir dicha contribución de acuerdo con las normas vigentes y los lineamientos del Consejo Directivo. 14. Convocar a sesiones ordinarias y extraordinarias del Consejo Directivo y de los Consejos Asesores. 15. Presentar al Consejo Directivo el anteproyecto de presupuesto, las modificaciones al presupuesto aprobado y los planes de inversión de la entidad, con arreglo a las disposiciones legales que regulan la materia. 16. Poner a consideración del Gobierno Nacional modificaciones a la		

estructura y planta de personal de la Agencia. 17. Distribuir los empleos de la planta de personal de acuerdo con la organización interna y las necesidades del servicio. 18. Distribuir entre las diferentes dependencias de la Agencia las funciones y competencias que la ley le otorgue a la entidad, cuando las mismas no estén asignadas expresamente a una de ellas. 19. Crear y organizar con carácter permanente o transitorio comités y grupos internos de trabajo. 20. Dirigir y desarrollar el sistema de control interno de la Agencia, de acuerdo con la normativa vigente. 21. Cumplir y hacer cumplir las decisiones del Consejo Directivo. 22. Ejercer la facultad nominadora, con excepción de los que corresponda a otra autoridad y dirigir la administración del talento humano de la Agencia. 23. Ejercer la función de control interno disciplinario en los términos de la ley. 24. Las demás funciones que le sean asignadas de conformidad con lo establecido en la ley.		
ARTÍCULO 13. Recursos y patrimonio. Los recursos y el patrimonio de la Agencia estarán constituidos por: 1. Los recursos del Presupuesto General de la Nación que se le asignen. 2. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento	**ARTÍCULO 13. Recursos y patrimonio**. Los recursos y el patrimonio de la Agencia estarán constituidos por: 1. Los recursos del Presupuesto General de la Nación que se le asignen. 2. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento	Se corrige error de tipografía.

del objetivo de la Agencia. 3. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia. 4. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia. 5. Los bienes muebles e inmuebles, así como acciones o títulos representativos de capital de sociedades o activos de la Nación, que le transfiera las entidades del sector y demás instituciones públicas 6. Las propiedades y demás activos que adquiera con recursos propios a cualquier título. 7. El valor de la contribución de valorización de los proyectos a su cargo. Los recaudos que se provengan de la ejecución de los proyectos de inversión a su cargo. 8. Los ingresos propios y los rendimientos producto de la administración de los mismos. 9. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título. 10. Los demás que reciba en desarrollo de su objeto.	del objetivo de la Agencia. 3. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia. 4. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia. 5. Los bienes muebles e inmuebles, así como acciones o títulos representativos de capital de sociedades o activos de la Nación, que le transfiera las entidades del sector y demás instituciones públicas 6. Las propiedades y demás activos que adquiera con recursos propios a cualquier título. 7. El valor de la contribución de valorización de los proyectos a su cargo. Los recaudos que ~~se~~ provengan de la ejecución de los proyectos de inversión a su cargo. 8. Los ingresos propios y los rendimientos producto de la administración de los mismos. 9. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título. 10. Los demás que reciba en desarrollo de su objeto.	

ARTÍCULO 14. Las entidades del Estado y las personas jurídicas de derecho privado deberán implementar dentro de cada organización los protocolos, estándares e instrucciones generales relacionados con seguridad digital que definirá la Agencia de conformidad con las funciones establecidas en el artículo 6 de la presente ley, dentro los 6 meses siguientes a la expedición de la presente Ley **PARÁGRAFO.** La Agencia verificará la implementación de los protocolos, estándares e instrucciones generales que expida. En caso de incumplimiento, la Agencia podrá adelantar un proceso administrativo sancionatorio de conformidad con la normativa vigente.	Sin modificaciones	
ARTÍCULO 15. Las entidades del Estado y las personas jurídicas de derecho privado domiciliadas en Colombia que administran información cuya divulgación resultaría en la afectación de la soberanía nacional, la estabilidad económica, la seguridad nacional y el derecho al habeas data de los ciudadanos en el ciberespacio deberán informar a la Agencia acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras que supongan riesgos en su información, infraestructura crítica, datos sensibles y sistemas de información. Lo anterior deberá realizarse en un plazo máximo de setenta y dos (72) horas, con el fin de que la Agencia Nacional de Seguridad Digital pueda prestar soporte y ayuda en el momento del ciberataque e iniciar los protocolos necesarios dado el caso y se informe a la opinión pública cuando los hechos efectivamente supongan riesgos de pérdida de información, o impactos de seguridad a infraestructura crítica, datos sensibles, y/o sistemas de información. Asimismo, las entidades del Estado y las personas jurídicas de derecho privado deberán informar a la	**Artículo 15.** Las entidades del Estado y las personas jurídicas de derecho privado domiciliadas en Colombia que administran información cuya divulgación resultaría en la afectación de la soberanía nacional, la estabilidad económica, la seguridad nacional y el derecho al habeas data de los ciudadanos en el ciberespacio deberán informar a la Agencia acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras que supongan riesgos en su información, infraestructura crítica, datos sensibles y sistemas de información. Lo anterior deberá realizarse en un plazo máximo de ~~**setenta y dos (72) horas**~~ veinticuatro (24) horas una vez se conozca del hecho, el cual podrá prorrogarse por una sola vez por el mismo tiempo, con el fin de que la Agencia Nacional de Seguridad Digital pueda prestar soporte y ayuda en el momento del ciberataque e iniciar los protocolos necesarios dado el caso y se informe a la opinión pública cuando los hechos efectivamente supongan riesgos de pérdida de información, o impactos de seguridad a infraestructura crítica, datos	Se modifica el tiempo de 72 horas a 48 horas para informar del ciberataque y delitos cibernéticos a la Agencia Nacional de Seguridad Digital.

Agencia los eventos de materialización de dichas amenazas perpetrados contra sus infraestructuras, en los términos que defina la reglamentación que para el efecto expida la Agencia. En caso de que las personas jurídicas de derecho privado que administren u operen infraestructuras críticas, no informen de los riesgos o eventos en el tiempo establecido por la Agencia, se les podrá imponer las siguientes sanciones, a través del desarrollo del proceso administrativo sancionatorio: 1. Multa de hasta doscientos (200) salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial para la imposición de la multa. 2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años, dependiendo del impacto del incidente. 3. Inclusión en la lista que la Agencia conformará de personas jurídicas de derecho privado que no cumplen con buenas prácticas de seguridad digital. 4. Prohibición de recibir cualquier tipo de apoyo, incentivo o subsidio del Gobierno, en un plazo hasta de cinco (05) años, dependiendo del impacto del incidente. Para los representantes de las entidades del estado que no realicen los reportes de riesgos, amenazas y eventos de materialización aplicarán las sanciones de acuerdo con lo dispuesto en la Ley 2094 de 2021 y la Ley 610 de 2000 y las normas que las adicionen, modifiquen o	sensibles, y/o sistemas de información. Asimismo, las entidades del Estado y las personas jurídicas de derecho privado deberán informar a la Agencia los eventos de materialización de dichas amenazas perpetrados contra sus infraestructuras, en los términos que defina la reglamentación que para el efecto expida la Agencia. En caso de que las personas jurídicas de derecho privado que administren u operen infraestructuras críticas, no informen de los riesgos o eventos en el tiempo establecido por la Agencia, se les podrá imponer las siguientes sanciones, a través del desarrollo del proceso administrativo sancionatorio; 1. Multa de hasta doscientos (200) salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial para la imposición de la multa. 2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años, dependiendo del impacto del incidente. 3. Inclusión en la lista que la Agencia conformará de personas jurídicas de derecho privado que no cumplen con buenas prácticas de seguridad digital. 4. Prohibición de recibir cualquier tipo de apoyo, incentivo o subsidio del Gobierno, en un plazo hasta de cinco (05) años, dependiendo del	

sustituyan, por omisión en el cumplimiento de los deberes propios del cargo o función.	impacto del incidente. Para los representantes de las entidades del Estado que no realicen los reportes de riesgos, amenazas y eventos de materialización aplicarán las sanciones de acuerdo con lo dispuesto en la Ley 2094 de 2021 y la Ley 610 de 2000 y las normas que las adicionen, modifiquen o sustituyan, por omisión en el cumplimiento de los deberes propios del cargo o función.	
ARTÍCULO 16. Adopción de la estructura y de la planta de personal de la Agencia. El Gobierno Nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones y en coordinación con el grupo de Transformación Digital del Departamento Administrativo de Presidencia de la República, procederá a adoptar la estructura y la planta de personal de la Agencia, dentro de los seis meses siguientes a partir de la promulgación de la presente ley. **PARÁGRAFO** Hasta tanto se adopte la estructura y la planta de personal de la Agencia, el Ministerio de Tecnologías de la Información y Comunicaciones, en coordinación con el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República cumplirán las funciones señaladas para dicho organismo en la presente ley.	Sin modificaciones.	
ARTÍCULO 17. Aplicación, Vigencia. La presente Ley rige a partir de la fecha de su sanción y promulgación.	Sin modificaciones	

6. PROPOSICIÓN:

Con fundamento en las anteriores consideraciones, de manera respetuosa solicito a la Comisión Primera del Senado de la República, dar primer debate y aprobar el proyecto de Ley No.010/2023 Senado "**Por medio del cual se crea la Agencia Nacional de Seguridad Digital y se crean otras disposiciones**", conforme al texto que se anexa.

Cordialmente,

DAVID LUNA SÁNCHEZ
Senador de la República

ALFREDO DELUQUE ZULETA
Senador de la República

OSCAR BARRETO QUIROGA
Senador de la República

Texto propuesto para Primer Debate ante la Comisión Primera del Senado de la República:

PROYECTO DE LEY No. 010 DE 2023

"Por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas"

El Congreso de Colombia,

DECRETA:

CAPÍTULO I. Creación, naturaleza jurídica, objeto, domicilio y funciones

ARTÍCULO 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad que coordinará, definirá y hará seguimiento a las políticas de seguridad digital o ciberseguridad, implementadas por las entidades públicas y las personas naturales y jurídicas de derecho privado. Establecerá las obligaciones y deberes que tienen los órganos del Estado para determinar los requisitos mínimos para la prevención, resolución y respuesta de incidentes de ciberseguridad.

ARTÍCULO 2. Principios. En el desarrollo, interpretación y aplicación de la presente Ley, además de los principios constitucionales, se aplicarán los que a continuación se prevén:

Principio de Coordinación: Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto de la presente ley.

Principio de Confidencialidad: Todas las personas y organizaciones que intervengan en materia de seguridad digital que tengan acceso a información que no tenga la naturaleza de información pública están obligadas a garantizar la reserva de esta, según corresponda y a través de mecanismos idóneos, inclusive después de finalizada su relación con alguna de las labores que comprende la gestión del riesgo.

Principio de Cooperación: En el marco de las relaciones nacionales e internacionales en materia de seguridad digital, aunarán esfuerzos para el logro de los objetivos de seguridad digital del país.

Principio de Enfoque basado en riesgos: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque basado en riesgos de forma tal que la definición y aplicación de controles y la toma de decisiones, siempre considere los riesgos como insumo principal.

Principio Perspectiva Interseccional: La Agencia desarrollará sus funciones en consideración de las particularidades de los distintos grupos poblacionales y se regirá con un enfoque de inclusión interseccional en términos de sexo, identidad de género, raza, etnia, capacidad económica, clase social, orientación política y edad; abordando los riesgos e impactos diferenciados de las amenazas y riesgos para que la ciberseguridad responda a necesidades, prioridades y percepciones diferenciadas basadas en las particularidades de cada grupo poblacional.

Principio de Integridad: El Estado desarrollará, a través de las entidades y organismos competentes las acciones necesarias para elevar la confiabilidad y la exactitud de los datos o información de forma que se evite su manipulación, su adulteración y cambios por personas, entidades o procesos no autorizados.

Principio de Neutralidad Tecnológica: El Estado garantizará la libre adopción de tecnologías que permitan fomentar la eficaz gestión de la seguridad de la información y la ciberseguridad, sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos.

Respeto a la privacidad: La seguridad de la información y la ciberseguridad son base del aseguramiento de la privacidad y protección de datos personales, y su gestión deberá incluir medidas formales de protección de la privacidad. La gestión de la seguridad de la información y la ciberseguridad deberá igualmente, en todo momento, respetar la privacidad de las personas.

Principio de Protección de Datos Personales: Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.

Principio de Privacidad: Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el Régimen de Protección de Datos Personales.

ARTÍCULO 3. Definiciones. Para los efectos de la presente Ley, se adoptan las siguientes definiciones:

a. **Agencia:** Es la Agencia Nacional de Seguridad Digital.
b. **Amenazas:** Causa potencial de un incidente no deseado, el cual puede resultar en el daño a un sistema, individuo u organización.
c. **Ciberataque:** Incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, filtrar, robar, hacer uso o acceder de manera ilícita a un activo de información o de tecnologías de la información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica.
d. **Ciberdefensa**: Capacidad para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la seguridad nacional.
e. **Ciberdiplomacia**: Uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio.
f. **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 y para almacenar, modificar e intercambiar datos.
g. **Ciberseguridad:** Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.
h. **Delitos cibernéticos**: Aquellos que afectan la disponibilidad, integridad y confidencialidad de la información y los sistemas digitales. Estos solo pueden cometerse a través y en contra de un sistema informático.
i. **Delitos ciber habilitados**: Aquellos que existían de forma previa a las TICs, pero que, con el desarrollo de éstas, ahora se desarrollan también mediante la modalidad cibernética.
j. **Ecosistema Digital:** Conjunto de infraestructuras y prestaciones (plataformas, dispositivos de acceso) asociadas a la provisión de contenidos y servicios a través de Internet. Este es un sujeto de análisis fundamental para la definición de políticas públicas, en áreas tan diversas como la digitalización de procesos productivos y la protección de la privacidad de los usuarios.
k. **Equipo de respuesta a incidentes de seguridad informática:** Grupo de especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, para actuar de acuerdo a procedimientos y políticas predefinidas, que colaboren en resolver la situación presentada.
l. **Incidente:** Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.
m. **Infraestructuras críticas:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
n. **Protección de Datos Personales:** Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.
o. **Privacidad:** Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el Régimen de Protección de Datos Personales.
p. **Riesgo:** La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.
q. **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y 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.

r. **Sistema de Información:** Medio por el cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.

s. **Vulnerabilidad:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.

ARTÍCULO 4. Creación y naturaleza jurídica de la Agencia. Créase la Agencia Nacional de Seguridad Digital, como una entidad descentralizada del orden nacional, de naturaleza especial que forma parte de la Rama Ejecutiva, con personería jurídica, autonomía administrativa, financiera y patrimonio propio, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

Parágrafo. La Agencia es la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de seguridad digital.

ARTÍCULO 5. Misión. La Agencia es responsable de: a) liderar y fortalecer la gestión del ecosistema digital, coadyuvar en mantener un modelo de Ciberseguridad y la gestión de seguridad de la Información en las entidades del estado y de las personas naturales y jurídicas de derecho privado; b) articular la identificación de las infraestructuras críticas del país con las autoridades y entidades competentes; c) coordinar y cooperar con la identificación de amenazas, vulnerabilidades, con el propósito de asegurar las plataformas del estado a través de la confidencialidad, integridad y disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento, asociados a los sistemas de información de la Entidades o en el ciberespacio para uso de la ciudadanía y del estado colombiano; y d) generar y coordinar programas de concientización para los colombianos acerca de la detección de amenazas cibernéticas y desarrollar líneas de acción para el fortalecimiento de la industria de Seguridad Digital en el país.

ARTÍCULO 6. Domicilio. La Agencia tendrá como domicilio principal la ciudad de Bogotá, D. C.

ARTÍCULO 7. Objetivos. La Agencia será un organismo de carácter técnico especializado que tendrá como objeto la planificación, articulación y coordinación de las políticas de gestión de los riesgos de seguridad digital en el país, prevención de amenazas internas o externas contra el ecosistema digital del país, fortalecimiento de la confianza y seguridad de todas las partes interesadas en el ámbito digital.

PARÁGRAFO. La Agencia no tendrá competencias de policía judicial, ni las que le corresponden a los organismos de inteligencia y contrainteligencia del Estado. En el ejercicio de sus funciones esta entidad garantizará el derecho de hábeas data, el derecho a la intimidad, a la privacidad, a la libertad de expresión en entornos digitales y al buen nombre de los ciudadanos. Cualquier información que obtenga, recopile, almacene, use, circule o suprima la Agencia deberá tratarse exclusivamente en el marco de sus competencias legales, y sólo podrá ser usada, entregada o transferida a otros organismos con previa autorización judicial.

ARTÍCULO 8. Régimen jurídico. Los actos unilaterales que realice la Agencia para el desarrollo de sus actividades son actos administrativos y estarán sujetos a las disposiciones del derecho público.

Los contratos que deba celebrar la Agencia se regirán, por regla general, por las normas de contratación pública. Excepcionalmente, respecto de los contratos que se tengan que realizar para el desarrollo del objeto misional de la Agencia, dicha contratación se regirá por el derecho privado, aplicando los principios de la función administrativa y de la gestión fiscal y estarán sometidos al régimen de inhabilidades e incompatibilidades previsto para la contratación estatal. La Agencia, expedirá un manual de contratación en la cual se reglamente lo previsto en este inciso.

ARTÍCULO 9. Funciones de la Agencia. La Agencia tendrá, entre otras, las siguientes funciones:

1. Coordinación y colaboración:

1.1. Coordinar y gestionar, como punto de contacto único, la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que brinde información a los ciudadanos sobre los ciberataques que tengan impacto en el territorio nacional.

1.2. Coordinar con los actores del ecosistema de seguridad digital, el entendimiento y fortalecimiento de la gestión de los riesgos e incidentes de seguridad digital, ciberseguridad y protección de datos de la información que soportan la operación del Estado.

1.3. Liderar la implementación de políticas tendientes al fortalecimiento del nivel de madurez de seguridad digital en las entidades del Estado y coadyuvar en la implementación de mejores prácticas de seguridad en los sectores económicos y en la ciudadanía.

1.4. Adelantar acuerdos de cooperación internacional en temas relacionados con Seguridad Digital, Seguridad de la Información, Ciberseguridad, y Privacidad, tanto a nivel de protección de la información y las tecnologías de la información asociadas como las tecnologías operacionales propias de las infraestructuras y sectores críticos, teniendo en cuenta las políticas de Gobierno y la normativa vigente, dentro del marco de los tratados internacionales vinculantes para Colombia y del respeto de la facultad del Presidente de la República de dirigir las relaciones internacionales.

1.5. Organizar y coordinar una Comisión Intersectorial de Inteligencia Artificial que monitoree el desarrollo y uso de tecnologías que procesan datos que reciben y responden ante ellos, aprenden, razonan, planifican e incluso generan predicciones, y expida lineamientos, estándares e instrucciones tendientes a garantizar la seguridad de dichas tecnologías y a prevenir y mitigar los riesgos que de ellas se derivan.

1.6. Coordinar y colaborar con agencias de seguridad digital y ciberdefensa de otros países, organismos internacionales y del sector privado con el fin de intercambiar información que pueda abordar los desafíos cibernéticos y coordinar con el Ministerio de Relaciones Exteriores, las acciones de ciberdiplomacia que se requieran para dicho fin.

2. Evaluación y mitigación de riesgos:

2.1. Asegurar el ecosistema digital y su gobernanza, de acuerdo con la dirección estratégica del gobierno nacional y establecer los lineamientos y/o políticas en materia de seguridad y gobernanza del ecosistema.

2.2. Contribuir a la protección y defensa del ciberespacio ante actos de penetración, infiltración, espionaje, sabotaje u otras actividades cuando atenten gravemente contra la administración pública y las infraestructuras críticas y proteger a las instituciones de nivel nacional y territorial de la influencia de organizaciones criminales.

2.3. Contribuir a la protección de recursos tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público.

2.4. Brindar asesoría y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en seguridad digital y ciberdefensa.

2.5. Dictar protocolos, estándares e instrucciones generales que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información del país, para reducir los riesgos de seguridad digital de las entidades del Estado, de los diferentes sectores económicos y de los ciudadanos.

2.6. Crear y coordinar un observatorio encargado de realizar análisis de amenazas cibernéticas, y colaborar con entidades públicas, sector privado y ciudadanos en el entendimiento de tácticas, técnicas y procedimientos de los delincuentes ante eventuales ciberataques, de recolectar información y de monitorear ataques tanto a nivel nacional e internacional. El observatorio trabajará en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Relaciones Exteriores y el Ministerio de Educación. Los análisis y estudios elaborados por el Observatorio se presentarán al Consejo Directivo a través de informes por lo menos una vez al año.

3. Educación y prevención:

3.1. Fortalecer las capacidades y competencias en seguridad digital de los servidores públicos, trabajadores oficiales, contratistas, proveedores y demás grupos de interés que accedan a la información del Estado colombiano.

3.2. Ofrecer en coordinación con el Ministerio de Educación Nacional programas de educación y concientización dirigidos a entidades públicas, sector privado y a los ciudadanos sobre investigación entrenamiento de ciberdefensa y gestión de amenazas, riesgos y ciberataques.Promover el desarrollo nacional de una cultura de ciberseguridad.

3.3. Trabajar de manera conjunta con instituciones educativas y de investigación en temas relacionados con seguridad digital y la ciberdefensa, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar los riesgos de ciberataques y de promover la innovación en soluciones de seguridad digital y ciberdefensa.

3.4. Representar al Gobierno Nacional en conferencias especializadas y escenarios académicos internacionales y ante organismos multilaterales, en lo relacionado con la protección de la seguridad digital y ciberdefensa de la Nación

3.5. Construir, en coordinación con el Ministerio de Ciencias, Tecnologías e Innovación, una hoja de ruta para fortalecer la investigación y desarrollo tecnológico en ciberseguridad y el asesoramiento en la creación de startups en la materia.

3.6. Fomentar, en conjunto con el Ministerio de Educación Nacional, el estudio de carreras profesionales enfocadas en la ciberseguridad.

4. Planificación:

4.1. Diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa, el cual contendrá programas,instrucciones, circulares, órdenes de carácter general y técnica; lineamientos y estándares en materia de seguridad digital, de conformidad con recomendaciones y estándares internacionales.

4.2. La planificación y articulación de actividades orientadas a la identificación y caracterización de activos de información, activos relacionados y activos de infraestructuras críticas;

4.3. Planear, desarrollar, mantener y mejorar de forma continua los modelos de Ciberseguridad y gestión de seguridad de la Información para ambientes de tecnologías de la información y de sectores críticos y/o de control industrial operacional.

4.4. Constituir y coordinar el Observatorio de Seguridad Digital y Ciberdefensa, el cual tiene como fin reunir información sobre los ataques cibernéticos presentados a las infraestructuras críticas de la Nación, así como a empresas privadas y entidades del sector público. El Observatorio presentará sus informes mínimo una vez al año y trabajará en coordinación con el Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Tecnologías de la Información y el Ministerio de Educación Nacional, la Fiscalía General de la Nación y la Dirección Nacional de Inteligencia.

4.5. Establecer que toda institución que posea infraestructura de la información calificada como crítica tendrá la obligación de informar a la agencia de Seguridad, los reportes de incidentes de ciberseguridad e informar respecto del plan de acción que adoptó.

5. De ejecución:

5.1. Desarrollar actividades de Seguridad digital bajo sus principios rectores, en cumplimiento del marco legal y objetivo misional, con las autoridades y entidades competentes.

5.2. Promover el fortalecimiento y la consolidación de los equipos de respuesta a incidentes de seguridad informática de sectores que involucren infraestructuras críticas.

5.3. Coadyuvar en el desarrollo, mantenimiento y mejora continua de los modelos de ciberseguridad y gestión de seguridad de la información para: i) entidades del Estado a nivel de tecnologías de la información, y que sirva de base para las personas naturales y jurídicas de derecho privado; y ii) Infraestructura crítica y control industrial u operacional, sea su propiedad estatal, mixta, o privada.

5.4. Desarrollar actividades de protección del ecosistema digital en cooperación con los demás organismos nacionales e internacionales, así como con otras entidades del Estado y personas jurídicas de derecho privado que administren u operen infraestructuras críticas.

5.5. Ordenar el cese de operaciones en el ciberespacio ante un ataque que afecte la soberanía nacional y el ecosistema digital y su economía, en coordinación con el Ministerio de Defensa.

5.6. Promover la creación, el fortalecimiento y la consolidación de los CSIRTS (Equipos de respuesta a incidentes de seguridad informática) de sectores que involucren infraestructuras críticas, entre los que se cuentan, mínimamente de los sectores de salud; energía; transporte y servicios públicos; así como otros que considere pertinentes.

5.7. Crear el Registro Nacional de Incidentes de Ciberseguridad , el cual tendrá el carácter de reservado. En este registro se ingresaran los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. sobre la base de este registro se podrán realizar las respectivas investigaciones por parte de la Agencia, asi como comunicar las alertas al Consejo técnico y elaborar recomendaciones para subsanar dichas brechas.

5.8. Las demás funciones relacionadas con las actividades de Seguridad Digital que le sean asignadas por el Presidente de la República de conformidad con la Constitución y la ley, siempre que se encuentren dentro del objeto señalado y cumplan con la condición de neutralidad de la presente ley.

PARÁGRAFO 1. El Director General y los servidores públicos de la Agencia, desarrollarán y aplicarán los controles necesarios para garantizar que los procesos de planeación, recolección, procesamiento, análisis y difusión de la información se hagan de manera objetiva y en ningún caso se discriminará el ejercicio de sus funciones por razón de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político, o afectar los derechos y garantías de los partidos políticos de oposición.

PARÁGRAFO 2. La Agencia desarrollará sus funciones en estricto cumplimiento del derecho de protección de los datos personales, de conformidad con la normativa vigente y en coordinación con la Superintendencia de Industria y Comercio.

CAPÍTULO II. Dirección y Administración.

ARTÍCULO 10. Órganos de Dirección y Administración. La Dirección y administración de la Agencia, estarán a cargo de un Consejo Directivo y de un Director General, quien tendrá la representación legal de la misma. El Consejo Directivo, actuará como instancia máxima para orientar sus acciones y hacer seguimiento al cumplimiento de sus fines.

ARTÍCULO 11. Funciones e Integración del Consejo Directivo. El Consejo Directivo será responsable de liderar la planificación, coordinación, articulación y gestión de los riesgos de seguridad digital y ciberseguridad en el país, incluyendo aquellos asociados a tecnologías operativas de infraestructura crítica y sistemas de control y actuación industrial, y será el soporte institucional y de coordinación para la definición, ejecución, seguimiento y el control de las estrategias, planes y acciones dirigidas a fortalecer la confianza y seguridad de todas las partes interesadas en el ámbito digital y de las infraestructuras críticas.

El Consejo Directivo de la Agencia, estará integrado por cinco miembros, así:

1. Presidente de la República o a quien designe.
2. El Ministro de Defensa o su delegado.
3. El Director del Departamento Nacional de Planeación o su delegado.
4. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado.
5. El Superintendente de Industria y Comercio o su delegado.

PARÁGRAFO 1: El Consejo Directivo constituirá un Comité Público-Privado de Estrategia que será el encargado de la planeación de estrategias de largo plazo para fortalecer las capacidades en seguridad digital, potenciar el desarrollo de la industria de ciberseguridad en Colombia y promover la educación de profesionales en el área. El Comité Público-Privado realizará recomendaciones al Consejo Directivo tendientes a atender las amenazas y los riesgos identificados en materia de seguridad digital y presentará informes de actualización sobre ataques perpetrados a nivel mundial y las formas de combatirlos mediante el uso de tecnologías de vanguardia y con los más altos estándares éticos.

PARÁGRAFO 2: El Consejo Directivo, podrá crear grupos de trabajo ad hoc que aborden asuntos científicos y técnicos integrado por representantes de otras entidades públicas o privadas, representantes de los equipos de respuesta a incidentes de seguridad informática de Gobierno y sectoriales, representantes de organismos y gremios del sector privado nacional o internacional, y asesores y expertos de la industria, de la academia y de grupos empresariales o de consumidores, que podrá emitir recomendaciones específicas a nivel de sector y de tecnologías a implementar y participar con derecho a voz, pero sin voto en las reuniones del Consejo Directivo.

PARÁGRAFO 3: El Consejo Directivo dictará su reglamento de funcionamiento. Las funciones del Consejo Directivo, y las reglas de creación y composición del Comité Público-Privado y de grupos de trabajo ad hoc se establecerán en el reglamento.

ARTÍCULO 12. Director General y sus funciones. La administración de la Agencia, estará a cargo de un Director General, el cual tendrá la calidad de empleado público, elegido por el Presidente de la República, a partir de terna presentada por el Consejo Directivo, y será el representante legal de la entidad. Deberá cumplir con requisitos de estudios y experiencia mínimos que establecerá el Consejo Directivo.

Son funciones del Director General las siguientes:

1. Dirigir, orientar, coordinar, vigilar y supervisar el desarrollo de las funciones a cargo de la Agencia.
2. Dirigir las actividades administrativas, financieras y presupuestales, y establecer las normas y procedimientos internos necesarios para el funcionamiento y prestación de los servicios de la Agencia.
3. Ejercer la representación de la Agencia y designar apoderados que representen a la Agencia en asuntos judiciales y extrajudiciales, para la defensa de los intereses de la misma.
4. Dirigir y promover la formulación de los planes, programas y proyectos relacionados con el cumplimiento de las funciones de la Agencia.
5. Presentar para aprobación del Consejo Directivo los estados financieros de la entidad.
6. Aprobar la estructuración técnica, legal y financiera de los proyectos a cargo de la Agencia.
7. Aprobar la estrategia de promoción de los proyectos de concesión u otras formas de Asociación Público-Privada.
8. Orientar y dirigir el seguimiento al desarrollo de los contratos de concesión a su cargo y, en caso de incumplimiento de cualquier obligación, adoptar de acuerdo con la ley las acciones necesarias.
9. Ordenar los gastos, expedir los actos y celebrar los convenios y contratos con personas naturales o jurídicas, así como con entidades públicas o privadas, nacionales o extranjeras, necesarios para el cumplimiento del objeto y funciones de la Agencia.
10. Someter a la aprobación del Consejo Directivo el Plan Estratégico Institucional y el Plan Operativo Institucional.
11. Promover la coordinación de la Agencia con las entidades u organismos públicos y privados.
12. Definir las políticas de comunicación de la Agencia y dar las instrucciones para que estas se cumplan de manera integral y coherente.
13. Proponer al Consejo Directivo la distribución, asignación y cobro de la contribución de valorización en los proyectos que lo requieran, de conformidad con la ley, y distribuir dicha contribución de acuerdo con las normas vigentes y los lineamientos del Consejo Directivo.
14. Convocar a sesiones ordinarias y extraordinarias del Consejo Directivo y de los Consejos Asesores.
15. Presentar al Consejo Directivo el anteproyecto de presupuesto, las modificaciones al presupuesto aprobado y los planes de inversión de la entidad, con arreglo a las disposiciones legales que regulan la materia.
16. Poner a consideración del Gobierno Nacional modificaciones a la estructura y planta de personal de la Agencia.
17. Distribuir los empleos de la planta de personal de acuerdo con la organización interna y las necesidades del servicio.
18. Distribuir entre las diferentes dependencias de la Agencia las funciones y competencias que la ley le otorgue a la entidad, cuando las mismas no estén asignadas expresamente a una de ellas.
19. Crear y organizar con carácter permanente o transitorio comités y grupos internos de trabajo.
20. Dirigir y desarrollar el sistema de control interno de la Agencia, de acuerdo con la normativa vigente.
21. Cumplir y hacer cumplir las decisiones del Consejo Directivo.
22. Ejercer la facultad nominadora, con excepción de los que corresponda a otra autoridad y dirigir la administración del talento humano de la Agencia.
23. Ejercer la función de control interno disciplinario en los términos de la ley.
24. Las demás funciones que le sean asignadas de conformidad con lo establecido en la ley.

CAPITULO III. Recursos y Patrimonio.

ARTÍCULO 13. Recursos y patrimonio. Los recursos y el patrimonio de la Agencia estarán constituidos por:

1. Los recursos del Presupuesto General de la Nación que se le asignen.
2. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento del objetivo de la Agencia.
3. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia.
4. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia.
5. Los bienes muebles e inmuebles, así como acciones o títulos representativos de capital de sociedades o activos de la Nación, que le transfiera las entidades del sector y demás instituciones públicas
6. Las propiedades y demás activos que adquiera con recursos propios a cualquier título.
7. El valor de la contribución de valorización de los proyectos a su cargo. Los recaudos que provengan de la ejecución de los proyectos de inversión a su cargo.
8. Los ingresos propios y los rendimientos producto de la administración de los mismos.
9. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título.

Los demás que reciba en desarrollo de su objeto.

CAPÍTULO IV. Implementación de Protocolos, Estándares e Instrucciones Generales y Sanciones.

ARTÍCULO 14. Las entidades del Estado y las personas jurídicas de derecho privado deberán implementar dentro de cada organización los protocolos, estándares e instrucciones generales relacionados con seguridad digital que definirá la Agencia de conformidad con las funciones establecidas en el artículo 6 de la presente ley, dentro los 6 meses siguientes a la expedición de la presente Ley

PARÁGRAFO. La Agencia verificará la implementación de los protocolos, estándares e instrucciones generales que expida. En caso de incumplimiento, la Agencia podrá adelantar un proceso administrativo sancionatorio de conformidad con la normativa vigente.

ARTÍCULO 15. Las entidades del Estado y las personas jurídicas de derecho privado domiciliadas en Colombia que administran información cuya divulgación resultaría en la afectación de la soberanía nacional, la estabilidad económica, la seguridad nacional y el

derecho al habeas data de los ciudadanos en el ciberespacio deberán informar a la Agencia acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras que supongan riesgos en su información, infraestructura crítica, datos sensibles y sistemas de información. Lo anterior deberá realizarse en un plazo máximo de veinticuatro (24) horas una vez se conozca del hecho, el cual podrá prorrogarse por una sola vez por el mismo tiempo, con el fin de que la Agencia Nacional de Seguridad Digital pueda prestar soporte y ayuda en el momento del ciberataque e iniciar los protocolos necesarios dado el caso y se informe a la opinión pública cuando los hechos efectivamente supongan riesgos de pérdida de información, o impactos de seguridad a infraestructura crítica, datos sensibles, y/o sistemas de información.

Asimismo, las entidades del Estado y las personas jurídicas de derecho privado deberán informar a la Agencia los eventos de materialización de dichas amenazas perpetrados contra sus infraestructuras, en los términos que defina la reglamentación que para el efecto expida la Agencia.

En caso de que las personas jurídicas de derecho privado que administren u operen infraestructuras críticas, no informen de los riesgos o eventos en el tiempo establecido por la Agencia, se les podrá imponer las siguientes sanciones, a través del desarrollo del proceso administrativo sancionatorio:

1. Multa de hasta doscientos (200) salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial para la imposición de la multa.

2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años, dependiendo del impacto del incidente.

3. Inclusión en la lista que la Agencia conformará de personas jurídicas de derecho privado que no cumplen con buenas prácticas de seguridad digital.

4. Prohibición de recibir cualquier tipo de apoyo, incentivo o subsidio del Gobierno, en un plazo hasta de cinco (05) años, dependiendo del impacto del incidente.

Para los representantes de las entidades del Estado que no realicen los reportes de riesgos, amenazas y eventos de materialización aplicarán las sanciones de acuerdo con lo dispuesto en la Ley 2094 de 2021 y la Ley 610 de 2000 y las normas que las adicionen, modifiquen o sustituyan, por omisión en el cumplimiento de los deberes propios del cargo o función.

CAPÍTULO VI. Disposiciones Finales.

ARTÍCULO 16. Adopción de la estructura y de la planta de personal de la Agencia. El Gobierno Nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones y en coordinación con el grupo de Transformación Digital del Departamento Administrativo de Presidencia de la República, procederá a adoptar la estructura y la planta de personal de la Agencia, dentro de los seis meses siguientes a partir de la promulgación de la presente ley.

PARÁGRAFO Hasta tanto se adopte la estructura y la planta de personal de la Agencia, el Ministerio de Tecnologías de la Información y Comunicaciones, en coordinación con el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República cumplirán las funciones señaladas para dicho organismo en la presente ley.

ARTÍCULO 17. Aplicación, Vigencia. La presente Ley rige a partir de la fecha de su sanción y promulgación.

Cordialmente,

DAVID LUNA SÁNCHEZ
Senador de la República

ALFREDO DELUQUE ZULETA
Senador de la República

OSCAR BARRETO QUIROGA
Senador de la República

CONCEPTOS JURÍDICOS

CONCEPTO JURÍDICO MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO A LA PONENCIA PROPUESTA PARA SEGUNDO DEBATE AL PROYECTO DE LEY NO. 142 DE 2022 SENADO

por la cual se dictan normas para garantizar los derechos a la vida, a la integridad personal y a la salud de los individuos mediante una movilidad segura, sostenible e incluyente para todos los actores viales y se dictan otras disposiciones.

3. Despacho del Viceministro Técnico

Honorable Congresista
IVÁN LEÓNIDAS NAME VÁSQUEZ
Senado de la República
CONGRESO DE LA REPÚBLICA
Carrera 7 No. 8-68
Ciudad.

Radicado: 2-2023-042536
Bogotá D.C., 11 de agosto de 2023 18:45

Radicado entrada
No. Expediente 35824/2023/OFI

Asunto: Comentarios a la ponencia propuesta para segundo debate al Proyecto de Ley No. 142 de 2022 Senado *"Por la cual se dictan normas para garantizar los derechos a la vida, a la integridad personal y a la salud de los individuos mediante una movilidad segura, sostenible e incluyente para todos los actores viales y se dictan otras disposiciones*." Radicado: 1-2023-042984

Respetado Presidente:

En atención a la solicitud de concepto de impacto fiscal de la Honorable Senadora Ana Carolina Espitia Jerez, y en cumplimiento de lo dispuesto en el artículo 7 de la Ley 819 de 2003[1], el Ministerio de Hacienda y Crédito Público presenta los comentarios y consideraciones a la ponencia propuesta para segundo debate al Proyecto de Ley del asunto en los siguientes términos:

El proyecto de Ley, de iniciativa parlamentaria, de acuerdo con lo contemplado en su artículo 1, tiene por objeto *"garantizar el derecho a la vida, a la integridad personal y a la salud de los individuos en el sistema de tránsito y transporte terrestre mediante una movilidad segura, sostenible e incluyente para todos los actores viales, regulando los principales factores de riesgo que atentan contra la seguridad de las personas en el territorio nacional; dentro de los perímetros urbanos y en zonas rurales y, reforzando los instrumentos normativos para disuadir a los conductores que realicen maniobras altamente peligrosas que ponen en riesgo la vida de las personas en las vías."*[2].

Respecto de las propuestas contenidas en la iniciativa, se encuentra que varias responden a aspectos reglamentarios que ya son competencia de entidades del sector respectivo, lo cual en principio no tendría repercusiones presupuestales adicionales, siempre y cuando en tales aspectos su ejecución esté contenida en los recursos actuales y proyectados en el marco de gasto de mediano plazo del sector. A este respecto, es pertinente resaltar que el diseño e implementación de políticas públicas, así como su inspección y vigilancia, recae en los diferentes Ministerios, según el artículo 58 de la Ley 489 de 1998[3], que señala son quienes tienen por objetivos primordiales *"la formulación y adopción de las políticas, planes generales, programas y proyectos del Sector Administrativo que dirigen"*, los cuales se cumplen a través de las entidades descentralizadas del orden nacional adscritas o vinculadas al sector.

Cabe mencionar que la asignación de recursos en Colombia se encuentra sometida al principio de legalidad que involucra la incorporación de ingresos y los gastos en el presupuesto. Para incluir estos recursos en la ley anual de presupuesto debe establecerse el monto de ingresos y, de otro lado, las erogaciones como una autorización máxima de gasto a los órganos que lo conforman. En ese contexto, las entidades nacionales deben ajustarse a las disponibilidades presupuestales y priorización de la política pública, acorde con el Plan Nacional de Desarrollo y en virtud de su autonomía presupuestal, tal como lo han dispuesto los artículos 39 y 47 del Estatuto Orgánico de Presupuesto (EOP)[4]. Así las cosas, de conformidad con el EOP, cada entidad pública correspondiente a una sección presupuestal deberá incluir en los respectivos anteproyectos de presupuesto los programas y proyectos que, de acuerdo con las competencias del sector presupuestal, se propongan realizar durante la respectiva vigencia fiscal, acorde con las normas de austeridad en dichos gastos[5].

De otra parte, el artículo 7 del Proyecto de Ley establece que el Gobierno nacional diseñará un programa para garantizar la gratuidad de los desplazamientos de los niños, niñas y adolescentes en condición de vulnerabilidad en zonas rurales desde y hacia sus establecimientos educativos. Frente al particular, es preciso anotar que actualmente el servicio de transporte escolar está a cargo de las secretarías de educación territoriales, bajo las disposiciones en la materia del Ministerio de Transporte, para lo cual cuentan con fuentes de financiación como aportes del Sistema General de Participaciones, del Sistema General de Regalías, o recursos propios de las entidades territoriales.

Por otro lado, los artículos 11, 12 y 17 del proyecto plantean la gratuidad en la expedición de las licencias de conducción por primera vez, así como la construcción de infraestructura vial para motos y bicicletas, y un registro de lesiones corporales en vías nacionales concesionadas y no concesionadas, lo cual tendría efectos fiscales que en la iniciativa no se encuentran evaluados ni plantea fuentes adicionales de financiación.

Adicionalmente, el artículo 23 de la iniciativa pretende incluir una partida arancelaria, adicionando un código numérico al artículo 468-1 del Estatuto Tributario[6], el cual tiene como efecto someter a todos los bienes que integran dicha subpartida a un tratamiento preferencial en el IVA. Los bienes que integran la partida 87.15.00.00.10 estarían sometidos al IVA a una tarifa del 5%. Al respecto, se indica que introducir tratamientos diferenciados en el IVA tendría un impacto negativo en el recaudo fiscal ya que estos bienes están actualmente gravados a la tarifa del 19%.

En línea con lo anterior, es preciso resaltar que el año pasado fue sancionada la Ley 2277 de 2022 "*Por medio de la cual se adopta una reforma tributaria para la igualdad y la justicia social y se dictan otras disposiciones*", de iniciativa de este Ministerio, cuyo articulado busca, entre otras cosas, "*lograr la consecución suficiente de recursos para financiar el fortalecimiento del sistema de protección social*"[7] , lo cual se alcanza "*a través de ajustes al sistema tributario, que permiten avanzar en materia de progresividad, equidad, justicia, simplicidad y eficiencia*"[8].

Igualmente, cabe advertir que todo beneficio tributario que se incluya en un proyecto de Ley debe contar con el aval del Gobierno nacional, representado en este Ministerio en asuntos tributarios[9], de acuerdo con lo establecido en el artículo 154 de la Carta Política y la interpretación de este artículo por la Corte Constitucional[10], so pena de incurrir en un vicio de inconstitucionalidad, de manera que estas propuestas de ley podrían incurrir en un vicio de inconstitucionalidad al no contar con el aval de este Ministerio, por las razones expuestas.

[1] Por la cual se dictan normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal y se dictan otras disposiciones
[2] Gaceta 406 de 2023, Pág. 10.
[3] Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.

[4] Decreto 111 "Por el cual se compilan la Ley 38 de 1989, la Ley 179 de 1994 y la Ley 225 de 1995 que conforman el estatuto orgánico del presupuesto".
[5] Artículo 14, Ley 2155 de 2021 "Por medio de la cual se expide la Ley de Inversión Social y se dictan otras disposiciones" y Decreto 397 de 2022 "Por el cual se establece el Plan de Austeridad del Gasto 2022 para los órganos que hacen parte del Presupuesto General de la Nación"
[6] Decreto 624 de 1989. Por el cual se expide el Estatuto Tributario de los Impuestos Administrados por la Dirección General de Impuestos Nacionales.
[7] Gaceta del Congreso 917 de 2022
[8] Gaceta del Congreso 917 de 2022
[9] Decreto 4712 de 2008 "Por el cual se modifica la estructura del Ministerio de Hacienda y Crédito Público."
[10] Ver, entre otras, la sentencia C-821 de 2011

Finalmente, es necesario resaltar la necesidad de dar cumplimiento a lo establecido en el artículo 7 de la Ley 819 de 2003, el cual establece que toda iniciativa debe hacer explícita su compatibilidad con el Marco Fiscal de Mediano Plazo, y debe incluir expresamente en la exposición de motivos y en las ponencias de trámite respectivas, los costos fiscales de la iniciativa y la fuente de ingreso adicional generada para el respectivo financiamiento.

Por lo expuesto, esta Cartera Ministerial se abstiene de emitir concepto favorable al proyecto de ley del asunto y manifiesta la disposición de colaborar con la actividad legislativa dentro de los parámetros constitucionales y legales de disciplina fiscal vigentes.

Cordialmente,

MARÍA FERNANDA VALDÉS VALENCIA
Viceministra Técnica
DGPPN/DIAN/OAJ

Con Copia: Dr. Gregorio Eljach Pacheco, Secretario del Senado de la República.

CONTENIDO

IMPRENTA NACIONAL DE COLOMBIA - 2023