INFORME DE PONENCIA PARA SEGUNDO 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., 14 de noviembre de 2023

Señor
IVÁN LEONIDAS NAME VASQUEZ
Presidente
SENADO DE LA REPÚBLICA
Ciudad

Asunto: Ponencia para segundo 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 segundo 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. El Proyecto de Ley 010/2023 fue discutido y aprobado por la Comisión Primera Constitucional de Senado el día 31 de octubre de 2023, designando como ponente para segundo debate a los honorables senadores David Luna y Alfredo Deluque (coordinadores)

1.5. 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.

1.6. 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

De las organizaciones mencionadas anteriormente se recibieron comentarios de:

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

1.7. El día 15 de agosto de 2023 los senadores David Luna, Alfredo Deluque y Oscar Barreto radicaron ante la honorable Comisión Primera del Senado de la República informe de ponencia positiva para primer debate del proyecto. A su vez, los senadores Julián Gallo y Clara López presentaron ponencia de archivo el día 16 de agosto.

1.8. El 3 de octubre de 2023 se recibieron comentarios del Ministerio de Hacienda y Crédito Público, el cual se abstuvo de dar concepto favorable señalando que para la creación de la Agencia se requieren recursos que no están contemplados en Presupuesto, Marco Fiscal de Mediano Plazo y Marco de Gasto de Mediano Plazo Sectorial y que se requiere que los ponentes deben relacionar los costos fiscales de la iniciativa y la fuente de ingreso adicional generada para el financiamiento de dicho costo.

1.9. El 5 de octubre de 2023 el Ministerio de Defensa remitió observaciones al Proyecto de Ley, sugiriendo ajustes en las funciones de la Agencia y en las definiciones de los conceptos relevantes para que guarden correspondencia a la institucionalidad y normativa vigente.

1.10. En el marco de la discusión del proyecto, se invitó al Ministro de Tecnologías de la Información y las Comunicaciones a la Comisión Primera del Senado de la República para presentar sus observaciones al proyecto el día 17 de octubre de 2023, pero presentó excusa y no asistió. Al día siguiente se recibió concepto escrito del Ministro, en el cual si bien resaltó la importancia de crear una institucionalidad y gobernanza sólidas en materia de ciberseguridad, se abstuvo de dar concepto favorable sobre el proyecto mencionando que este proyecto de ley es de competencia de las Comisiones Sextas Constitucionales Permanentes y que, en todo caso, requiere iniciativa o aval del Gobierno.

1.11. Luego de discutir el proyecto en diversas sesiones de la Comisión Primera del Senado de la República, el día 31 de octubre de 2023 fue aprobado con proposiciones de los honorables senadores Paloma Valencia y Humberto De La Calle.

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).

Por su parte, el artículo 2 de la Ley 3 de 1992 señala que los asuntos relacionados con la estructura y organización de la administración nacional central serán de conocimiento de las Comisiones Primeras.

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	ADSCRIPCIÓN
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.	Federal Ministry of the Interior, Building and Community.

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.	Depende directamente de la Comisión.
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.	Secretaría General de la Defensa y la Seguridad Nacional.
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.	Australian Signals Directorate (ASD) *Es la entidad de inteligencia y 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.	Government Communications Headquarters - provides intelligence, protects information and informs relevant UK policy to keep society safe and successful in the internet age. *(es la entidad de inteligencia y protección de información).*
CISA- Cybersecurity and Infrastructure Security Agency	Estados Unidos	2018	Tiene la responsabilidad de proteger la infraestructura crítica del país, de promover la seguridad cibernética y coordinar la respuesta del país ante incidentes cibernéticos.	Es una Agencia adscrita al Departamento de Seguridad Nacional de los Estados Unidos
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.	Communications Security Establishment - Canada's national cryptologic agency, providing the Government of Canada with information technology security and foreign signals intelligence *(la entidad de inteligencia y seguridad de la tecnología de la información).*

INCIBE – Instituto Nacional de Ciberseguridad	España	2014	Entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.	Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial
Cyber Security Centre NCSC-EE	Estonia	2010	24/7 cyberspace monitoring, cyber incident response, protection of critical infrastructure, cyberspace analysis and prevention, surveillance, standardisation, cyber crisis management and exercises, and coordination of research and development.	Information System Authority (RIA)

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

En septiembre del 2023, varias entidades del Estado como la SIC; Supersalud, el Consejo Superior de la Judicatura, el Ministerio de Salud y otras entidades del Estado fueron víctimas de un ciberataque perpetrado mediante la modalidad Ransomware (”secuestro digital de información y aplicaciones”) hacía la empresa estadounidense IFX Network, la cual es proveedora de soluciones de telecomunicaciones y cuenta con presencia en 17 países de la región.

Se estima que este ciberataque dejó fuera de servicio a 50 páginas web y aplicaciones de entidades del Estado, afectando gravemente incluso a la totalidad de los portales de la Rama Judicial del país, tanto así que el Consejo Superior de la Judicatura determinó que los términos judiciales fueron suspendidos hasta el próximo 20 de Septiembre. Por su

magnitud se considera uno de los ciberataques más contundentes a los que se han enfrentado las infraestructuras críticas del país.

Este ciberataque puso en riesgo los datos personales de los colombianos, teniendo en cuenta que las entidades con más afectación pertenecen al sector Salud y Justicia.

En una entrevista el Ministro de Salud, Guillermo Alfonso Jaramillo, informó que los ciberdelincuentes habían captado la información de los portales de la Superintendencia de Salud y el Ministerio de Salud. Sin embargo, la empresa IFX ha negado lo anterior y afirma que no se han evidenciado vulnerabilidades en la información, privacidad y seguridad de los datos alojados en la nube.

Según Fortinet, solo en la primera mitad del 2023 Colombia recibió cinco mil millones de intentos de ciberataques. La Agencia Nacional de Seguridad Digital es más que una necesidad, una obligación con los colombianos.

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. COMENTARIOS DE LOS PONENTES

Sobre el alcance del objeto de la Agencia y su ubicación en la estructura del Gobierno.

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 distribuirse 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. De acuerdo con la Corte Constitucional (Sentencia C-043 de 2023), las nuevas entidades del nivel central deben adscribirse a la cartera que tenga una relación temática relevante o estrecha con el asunto del que trate la nueva entidad, y será esa misma cartera (o esas) la(s) llamada(s) a otorgar el aval gubernamental que exige la ley. El DAPRE no es la entidad que tiene relación temática

con una Agencia de Seguridad Digital, existiendo el MinTIC que ya tiene esas funciones y capacidades.

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.

Sobre los recursos necesarios para poner en funcionamiento la Agencia.

Según concepto emitido por el Ministerio de Hacienda frente al Proyecto de Ley 023 de 2023 Cámara cuyo objeto es la creación de una Agencia de Seguridad Digital y Asuntos Espaciales, para poner en marcha dicha Agencia se requerirían **COP 92.783.000.000**, distribuidos así:

- Costos de planta: 37.451.696.756 (106 funcionarios).
    - 5 cargos de nivel directivo
    - 31 cargos de nivel asesor
    - 62 cargos de nivel profesional
    - 8 cargos de nivel técnico asistencial

- Costos por gastos generales: 25.590.000.000
    - Infraestructura de seguridad digital – 10.000.000.000
    - Compra de inmueble – 13.000.000.000
    - Computadores y puestos de trabajo – 1.590.000.000
    - Otros – 1.000.000.000

- Inversión: 23.741.000.000, dividido en las dos direcciones (seguridad digital y asuntos espaciales).

A diferencia del PL 023-23C, el presente proyecto de ley 010-23S propone una Agencia con competencia exclusiva para asuntos de seguridad digital. Teniendo en cuenta que hoy en día existen dependencias del Ministerio de Tecnologías de la Información y las Comunicaciones que ejercen funciones que eventualmente se reasignarían a la Agencia Nacional de Seguridad Digital, los recursos presupuestados para funcionamiento e inversión de estas dependencias se destinarían a la Agencia.

En ese sentido, los costos proyectados por MinHacienda se podrían reducir sustancialmente, previendo la creación de muchos menos cargos nuevos para la planta de personal y previendo que no sea necesario apropiar recursos adicionales para inversión y funcionamiento toda vez que reasignarían o redistribuirían recursos que ya están apropiados para dependencias e instancias que ya existen en la estructura del Gobierno Nacional. Incluso, teniendo en cuenta que el presente proyecto propone la adscripción de la Agencia a MinTIC, podría prescindirse de la adquisición de un inmueble para oficinas y adecuar un espacio del edificio del MinTIC para el funcionamiento de la Agencia.

Para financiar estos costos de puesta en funcionamiento de la Agencia, los ponentes proponemos la asignación de un 1% de los recursos del FONTIC a esta agencia. Para

2023 el FONTIC tenía un presupuesto de 2.092.626.646.034, por lo cual el 1% serían 20.926.286.460. Con estos recursos se financiarán los nuevos rubros de funcionamiento e inversión, distribuidos así:

- Costos de planta: $8.446.927.568 (29 nuevos funcionarios).
    - 1 cargo de nivel directivo
    - 3 cargos de nivel asesor
    - 20 cargos de nivel profesional
    - 5 cargos de nivel técnico asistencial
- Costos por gastos generales: 5.771.570.983
    - Infraestructura de seguridad digital – 5.187.422.142
    - Computadores y puestos de trabajo – 358.608.748
    - Otros – 225.540.093
- Inversión: $6.707.787.909.

De esta forma se atiende a lo dispuesto en el artículo 7 de la Ley 819 de 2003, que establece que todo proyecto de ley que ordene gasto deberá hacerse explícito y deberá ser compatible con el Marco Fiscal de Mediano Plazo.

5. 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.

6. PLIEGO DE MODIFICACIONES

TEXTO PARA SEGUNDO DEBATE PL 010-23S

Texto Aprobado Primer Debate	Texto Propuesto Segundo Debate	Observaciones
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	**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	Se modifican y se incluyen principios para proteger de manera especial a niños, niñas y adolescentes en entornos digitales

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	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. **En particular, la Agencia velará por la prevención de riesgos en los sujetos de especial protección, especialmente, las niñas, los niños y adolescentes como usuarios activos en el ecosistema digital.** 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	

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.	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, **y en particular, de niñas, niños y adolescentes.** 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. **Principio de participación: La Agencia, en el cumplimiento de sus funciones promoverá y atenderá las iniciativas de los Grupos de Interés, encaminadas a intervenir en los procesos de deliberación, formulación, ejecución, control y evaluación de la gestión pública, así como de proyectos**	

	normativos, lineamientos, estándares, herramientas y buenas prácticas de mejora regulatoria y guías que permitan la generación de valor público. **Principio del enfoque basado en el respeto a los derechos humanos: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque del respeto a los derechos humanos de tal forma que se reconozca a las personas naturales, en particular a las personas de especial protección constitucional, como los principales sujetos de la ciberseguridad.** **Protección Integral del Ciudadano. Se entiende por protección integral del ciudadano, el reconocimiento como sujeto de derechos, la garantía y cumplimiento de los mismos, la prevención de sus amenazas o vulneración y la seguridad de su restablecimiento inmediato en desarrollo de los derechos humanos, y de los derechos fundamentales amparados por la Constitución Política de Colombia.**	
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	**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	Se modifican las definiciones de algunos conceptos para que correspondan a las definiciones previstas actualmente en el ordenamiento jurídico colombiano (Decreto 338 de 2022). Este ajuste fue sugerido por el Ministerio de Defensa en concepto del 05 de octubre de 2023 remitido al Senado de la República.

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, infraestructuras e información del Estado y de los ciudadanos 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	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~~. **Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.** 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~~ **Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias** que es utilizad~~o~~ 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, infraestructuras e información del Estado y de los ciudadanos 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	

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	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.~~ **Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permite minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.** 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.~~ **Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.** 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	

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.	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.~~ **Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.** 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 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	**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 **del Gobierno Nacional** 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~~**Promover y determinar el alcance de los** 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, **sin perjuicio de las funciones asignadas al Ministerio de Relaciones Exteriores y** teniendo en cuenta	Teniendo en cuenta que entidades como el Ministerio de Defensa y la Policía Nacional tienen y mantendrán funciones relacionadas con ciberdefensa, y que existirán CSIRT sectoriales con funciones de respuesta ante incidentes, se corrige la función 1.1. en el sentido de aclarar que la Agencia coordinará y será punto de contacto de las respuestas oficiales ante incidentes pero no será la única entidad que los gestionará. Se modifica la función 1.4. para incluir al Ministerio de Relaciones Exteriores, considerando su rol de líder de negociación de instrumentos de cooperación internacional.

Tecnologías Disruptivas que monitoree el desarrollo y uso de tecnologías relacionadas con la transformación digital disruptiva en sectores esenciales para el Estado y la ciudadanía como el transporte, la salud, los servicios públicos, los servicios financieros, la seguridad nacional, entre otros según la necesidad, 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	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 Tecnologías Disruptivas que monitoree el desarrollo y uso de tecnologías relacionadas con la transformación digital disruptiva en sectores esenciales para el Estado y la ciudadanía como el transporte, la salud, los servicios públicos, los servicios financieros, la seguridad nacional, entre otros según la necesidad, 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. 1.7. **Coordinar a los equipos de respuesta a incidentes de seguridad informática de Gobierno y sectoriales.** 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	

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, el Ministerio de Educación y la Superintendencia de Industria y Comercio. 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	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,	

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	el Ministerio de Relaciones Exteriores, el Ministerio de Educación y la Superintendencia de Industria y Comercio. 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	

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 persona jurídica o entidad que administre u opere infraestructuras críticas tendrá la obligación de informar a la Agencia, 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,	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	

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	Información y el Ministerio de Educación Nacional, la Fiscalía General de la Nación y la Dirección Nacional de Inteligencia. 4.5. Establecer que toda persona jurídica o entidad que administre u opere infraestructuras críticas tendrá la obligación de informar a la Agencia, 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	

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 las instrucciones que la Superintendencia de Industria y Comercio imparta en la materia.	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 las instrucciones que la Superintendencia de Industria y Comercio imparta en la materia.	
ARTÍCULO 13. Créese el rol del Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital como un funcionario de libre nombramiento, más no de libre remoción, por un periodo fijo de cuatro años, el cual tendrá como funciones: a. Ser el responsable de salvaguardar los derechos de los ciudadanos en relación con sus datos personales en materia de Seguridad Digital. b. Auditar las actividades de la Agencia Nacional de Seguridad Digital (ANSD) para garantizar el respeto a los derechos de los datos personales de los ciudadanos. c. Emitir recomendaciones y directrices para mejorar las prácticas de protección de datos en el desarrollo de funciones de la Agencia Nacional de Seguridad Digital. **PARÁGRAFO.** El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, será elegido de una terna de candidatos enviada por gremios del sector de tecnología y la protección de datos y designado por el Procurador General de la Nación.	**ARTÍCULO 13.** ~~Créese el rol del~~ La Agencia contará con un Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, **que será** ~~como~~ un funcionario de libre nombramiento, más no de libre remoción, **el cual se desempeñará** por un periodo fijo de cuatro años, ~~el cual~~ **y** tendrá como funciones: a. Ser el responsable de salvaguardar los derechos de los ciudadanos en relación con sus datos personales en materia de Seguridad Digital. b. Auditar **que** las actividades de la Agencia Nacional de Seguridad Digital (ANSD) ~~para~~ garanti**cen**~~zar~~ el respeto a **las normas de protección de datos personales, y reportar a la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio, o quien haga sus veces, los hallazgos que surjan.**~~los derechos de los datos personales de los ciudadanos~~. c. Emitir recomendaciones y directrices para mejorar las prácticas de protección de datos en el desarrollo de funciones de la Agencia Nacional de Seguridad Digital. **PARÁGRAFO 1.** El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, será elegido **por el Consejo Directivo** de una terna de candidatos enviada por	Se modifica este artículo nuevo aprobado en primer debate con el fin de armonizarlo con las funciones de la Superintendencia de Industria y Comercio en materia de protección de datos personales, de manera que se eviten duplicidades de funciones.

	~~gremios del sector de tecnología y la protección de datos y designado por~~ el Procurador General de la Nación. **PARÁGRAFO 2. El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital no reemplaza el rol de la Superintendencia de Industria y Comercio en materia de protección de datos personales y ejercerá sus funciones en coordinación con dicha entidad.**	
ARTÍCULO 14. 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	**ARTÍCULO 14. 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. <u>La asignación anual de un monto equivalente al 1% del presupuesto del Fondo Único de Tecnologías de la Información y las Comunicaciones – FONTIC.</u>** 3. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento del objetivo de la Agencia. 4. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia. 5. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia. 6. 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 7. Las propiedades y demás activos que adquiera con recursos propios a cualquier título. 8. El valor de la contribución de valorización de los proyectos a su cargo.	Se incluye la destinación de un 1% del FONTIC para la financiación de la Agencia y se ajusta numeración.

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.	Los recaudos que provengan de la ejecución de los proyectos de inversión a su cargo. 9. Los ingresos propios y los rendimientos producto de la administración de los mismos. 10. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título. 11. Los demás que reciba en desarrollo de su objeto.	
ARTÍCULO 16. 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 a Agencia, se les podrá imponer las siguientes	**ARTÍCULO 16.** 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)** ~~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 a Agencia, se les podrá imponer las siguientes	Se ajusta nuevamente el plazo para reportar incidentes de ciberseguridad de conformidad con las recomendaciones de expertos y sugerencias de los gremios que agrupan empresas que operan infraestructuras críticas.

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.	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.	
ARTÍCULO 17. 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. En todo caso, la planta de personal de la Agencia se integrará con cargos ya existentes en el Ministerio de Tecnologías de la Información y Comunicaciones y en el grupo de	**ARTÍCULO 17. 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. En todo caso, la planta de personal de la Agencia se integrará con cargos ya existentes en el Ministerio de Tecnologías de la Información y Comunicaciones, **el Ministerio de**	Se aclara y complementa la redacción del inciso segundo.

Transformación digital del Departamento Administrativo de Presidencia de la República. Y en ningún caso se podrá crear, ni aumentar, ningún gasto burocrático adicional al ya existente. **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.	**Defensa** y en el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República, **de manera que se conforme la Agencia con recursos humanos, económicos y físicos que ya estén presupuestados y que no sea necesario crear gasto**.~~Y en ningún caso se podrá crear, ni aumentar, ningún gasto burocrático~~ adicional al ya existente. **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.	

7. PROPOSICIÓN:

Con fundamento en las anteriores consideraciones, de manera respetuosa solicito al Senado de la República dar segundo 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~~
SENADOR DE LA REPÚBLICA

ALFREDO DELUQUE
SENADOR DE LA REPÚBLICA

OSCAR BARRETO

PALOMA VALENCIA LASERNA

SENADOR DE LA REPÚBLICA **SENADORA DE LA REPÚBLICA**

PROYECTO DE LEY No. 10 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. En particular, la Agencia velará por la prevención de riesgos en los sujetos de especial protección, especialmente, las niñas, los niños y adolescentes como usuarios activos en el ecosistema digital.

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, y en particular, de niñas, niños y adolescentes.

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.

Principio de participación: La Agencia, en el cumplimiento de sus funciones promoverá y atenderá las iniciativas de los Grupos de Interés, encaminadas a intervenir en los procesos de deliberación, formulación, ejecución, control y evaluación de la gestión pública, así como de proyectos normativos, lineamientos, estándares, herramientas y buenas prácticas de mejora regulatoria y guías que permitan la generación de valor público.

Principio del enfoque basado en el respeto a los derechos humanos: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque del respeto a los

derechos humanos de tal forma que se reconozca a las personas naturales, en particular a las personas de especial protección constitucional, como los principales sujetos de la ciberseguridad.

Protección Integral del Ciudadano: Se entiende por protección integral del ciudadano, el reconocimiento como sujeto de derechos, la garantía y cumplimiento de los mismos, la prevención de sus amenazas o vulneración y la seguridad de su restablecimiento inmediato en desarrollo de los derechos humanos, y de los derechos fundamentales amparados por la Constitución Política de Colombia.

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 del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.

e. **Ciberdiplomacia:** Uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio.

f. **Ciberespacio**: Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias que es utilizada 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, infraestructuras e información del Estado y de los ciudadanos 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**: Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permite minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

l. **Incidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

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:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

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, como punto de contacto único, la respuesta oficial del Gobierno Nacional 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. Promover y determinar el alcance de los 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,

sin perjuicio de las funciones asignadas al Ministerio de Relaciones Exteriores y 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 Tecnologías Disruptivas que monitoree el desarrollo y uso de tecnologías relacionadas con la transformación digital disruptiva en sectores esenciales para el Estado y la ciudadanía como el transporte, la salud, los servicios públicos, los servicios financieros, la seguridad nacional, entre otros según la necesidad, 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.

1.7. Coordinar a los equipos de respuesta a incidentes de seguridad informática de Gobierno y sectoriales.

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, el Ministerio de Educación y la Superintendencia de Industria y Comercio. 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 persona jurídica o entidad que administre u opere infraestructuras críticas tendrá la obligación de informar a la Agencia, 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 las instrucciones que la Superintendencia de Industria y Comercio imparta en la materia.

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.

PARAGRAFO 4. Los funcionarios miembros del Consejo Directivo serán responsables disciplinariamente por las faltas que cometan en ejercicio de las funciones asignadas en la presente ley. En especial, la referente a la protección y manejo de los datos personales de las personas. En caso de incurrir en faltas en la materia, serán sancionados según el Código Único Disciplinario o la Ley que la derogue o modifique.

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.

ARTÍCULO 13. La Agencia contará con un Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, que será un funcionario de libre nombramiento, más no de libre remoción, el cual se desempeñará por un periodo fijo de cuatro años, y tendrá como funciones:

a. Ser el responsable de salvaguardar los derechos de los ciudadanos en relación con sus datos personales en materia de Seguridad Digital.

b. Auditar que las actividades de la Agencia Nacional de Seguridad Digital (ANSD) garanticen el respeto a las normas de protección de datos personales, y reportar a la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio, o quien haga sus veces, los hallazgos que surjan.

c. Emitir recomendaciones y directrices para mejorar las prácticas de protección de datos en el desarrollo de funciones de la Agencia Nacional de Seguridad Digital.

PARÁGRAFO 1. El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, será elegido por el Consejo Directivo de una terna de candidatos enviada por el Procurador General de la Nación.

PARÁGRAFO 2. El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital no reemplaza el rol de la Superintendencia de Industria y Comercio en materia de protección de datos personales y ejercerá sus funciones en coordinación con dicha entidad.

CAPITULO III. Recursos y Patrimonio.

ARTÍCULO 14. 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. La asignación anual de un monto equivalente al 1% del presupuesto del Fondo Único de Tecnologías de la Información y las Comunicaciones – FONTIC.

3. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento del objetivo de la Agencia.

4. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia.

5. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia.

6. 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

7. Las propiedades y demás activos que adquiera con recursos propios a cualquier título.

8. 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.

9. Los ingresos propios y los rendimientos producto de la administración de los mismos.

10. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título.

11. Los demás que reciba en desarrollo de su objeto.

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

ARTÍCULO 15. 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 16. 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 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 a 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 V. Disposiciones Finales.

ARTÍCULO 17. 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.

En todo caso, la planta de personal de la Agencia se integrará con cargos ya existentes en el Ministerio de Tecnologías de la Información y Comunicaciones, el Ministerio de Defensa y en el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República, de manera que se conforme la Agencia con recursos humanos, económicos y físicos que ya estén presupuestados y que no sea necesario crear gasto adicional al ya existente.

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 18. APLICACIÓN, VIGENCIA. La presente Ley rige a partir de la fecha de su sanción y promulgación.

Cordialmente,

DAVID LUNA
SENADOR DE LA REPÚBLICA

ALFREDO DELUQUE
SENADOR DE LA REPÚBLICA

OSCAR BARRETO
SENADOR DE LA REPÚBLICA

PALOMA VALENCIA LASERNA
SENADORA DE LA REPÚBLICA