REPÚBLICA DE COLOMBIA

CONGRESO DE LA REPÚBLICA DE COLOMBIA
SENADO DE LA REPÚBLICA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

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

AÑO XXXII - Nº 711 | Bogotá, D. C., miércoles, 14 de junio de 2023 | EDICIÓN DE 17 PÁGINAS

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

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

RAMA LEGISLATIVA DEL PODER PÚBLICO

SENADO DE LA REPÚBLICA

PONENCIAS

INFORME DE PONENCIA PARA PRIMER DEBATE AL PROYECTO DE LEY NÚMERO 89 DE 2022 SENADO

por medio de la cual se establece el formato de sentencias de lectura fácil y se dictan otras disposiciones.

INFORME DE PONENCIA PARA PRIMER DEBATE.
PROYECTO DE LEY No. 89 DE 2022 SENADO "*POR MEDIO DE LA CUAL SE ESTABLECE EL FORMATO DE SENTENCIAS DE LECTURA FÁCIL Y SE DICTAN OTRAS DISPOSICIONES*".

Bogotá, D.C., 13 de junio de 2022.

Senador
FABIO RAÚL AMÍN SALEME
Presidente
Comisión Primera Constitucional Permanente
Senado de la República
Ciudad

En cumplimiento del encargo realizado por la Mesa Directiva de la Comisión Primera del Senado de la República, de manera atenta, me permito rendir Informe de Ponencia para Primer Debate del Proyecto de Ley No. 89 de 2022 Senado "*Por medio de la cual se establece el formato de sentencias de lectura fácil y se dictan otras disposiciones*", en los términos que se exponen a continuación.

I. TRÁMITE DE LA INICIATIVA.

El proyecto de ley 89 de 2022 Senado fue radicado en el Senado de la República el pasado 2 de agosto de 2022 por iniciativa de los congresistas Angélica Lozano, Jonathan Ferney Pulido, Duvalier Sánchez, Catherine Juvinao Clavijo, Santiago Osorio, Juan Sebastián Gómez, Carolina Giraldo, Jennifer Pedraza, Fabián Díaz Plata, Juan Diego Muñoz, Cristian Damilo Avendaño, Daniel Carvalho Mejía, Alejandro García Ríos, Jaime Raúl Salamanca, Iván Leonidas Nama, Inti Asprilla y David Luna. El texto original del proyecto de ley fue debidamente publicado en la Gaceta del Congreso N° 893 de 2022.

El 9 de agosto de 2022 el expediente del proyecto fue radicado en la Comisión Primera Constitucional Permanente del Senado de la República. El 12 de agosto de 2022 mediante Acta MD-03 fueron designados como ponentes para primer debate los Senadores Alexander López Maya (Coordinador), Alejandro Vega, Carlos Fernando Motoa, Oscar Barreto, Paloma Valencia, Julián Gallo, Rodolfo Hernández, Ariel Avila y Berner Zambrano.

II. OBJETO Y CONTENIDO DEL PROYECTO DE LEY.

La iniciativa legislativa tiene por objeto por objeto establecer el formato de sentencia de lectura fácil que tendrá aplicación en todas las jurisdicciones y especialidades del Estado colombiano, así como las actuaciones de las autoridades administrativas que ejerzan funciones jurisdiccionales y administrativas y en los procesos arbitrales.

La iniciativa consta de cinco (5) artículos incluido el relativo a la vigencia:

ARTÍCULO	CONTENIDO
1	Prevé el objeto del proyecto de ley.
2	Establece el derecho de todos los ciudadanos a comprender de manera accesible y sencilla los motivos y contenidos de las decisiones judiciales y administrativas e impone a los funcionarios competentes la obligación de elaborar de elaborar, además del formato tradicional, uno de lectura fácil que tendrá el mismo valor y efectos.
3	Dispone los parámetros del formato de lectura fácil y la obligación del Consejo Superior de la Judicatura de prestar apoyo técnico, administrativo y humanos para asegurar que todos los jueces y magistrados implementen este formato.
4	Establece que la Comisión Interinstitucional de la Rama Judicial y el Consejo Superior de la Judicatura en coordinación con el Ministerio de Justicia y del Derecho definirán el protocolo de elaboración de las sentencias de lectura fácil. Además dispone que la Escuela Judicial Rodrigo Lara Bonilla impartirá, a los jueces de todas las jurisdicciones, un módulo sobre el concepto y aplicación de las sentencias de lectura fácil.
5	Establece la vigencia y derogatorias.

III. CONCEPTOS FRENTE AL PROYECTO DE LEY.

Para efectos del análisis de la iniciativa objeto de estudio y para la elaboración del presente informe de ponencia solicité conceptos a: Ministerio de Justicia y del Derecho, Comisión Interinstitucional de la Rama Judicial, Consejo Superior de la Judicatura, Escuela Judicial Rodrigo Lara Bonilla, Consejo de Estado, Corte Suprema de Justicia y a la Corte Constitucional.

A continuación se hace referencia a los conceptos recibidos a la fecha de radicación del presente informe de ponencia:

1. MINISTERIO DE JUSTICIA Y DEL DERECHO.

Mediante comunicación identificada con radicado MJD-OFI22-0035782-VPJ-20000 del 20 de septiembre de 2022, la Viceministra de Promoción de la Justicia manifestó:

"(…) se considera necesario analizar cuatro aspectos problemáticos: (i) el plazo razonable como garantía del derecho al acceso a la justicia; (ii) el ámbito de aplicación, los sujetos obligados y la vigencia de norma; (iii) el principio de autonomía judicial; (iv) y el marco jurídico actual.

(…)

En el caso del proyecto normativo, el inciso segundo del artículo 2° señala: "los funcionarios competentes deberán elaborar, junto con el formato tradicional de sentencia o decisión, uno de lectura fácil utilizando lenguaje no técnico". Esto significa que los jueces y autoridades administrativas tendrían una nueva carga laboral, pues deben realizar la sentencia o auto que pone fin al proceso, y además, realizar el respectivo formato de lectura fácil. Esta nueva función puede conllevar a la ampliación de los términos para resolver un caso, y en consecuencia, la agudización del fenómeno de la congestión judicial.

En otras palabras, aunque el proyecto normativo tiene un fin loable (garantizar que los ciudadanos comprendan las decisiones de los jueces) al imponer una nueva carga a todos los jueces de la república podría generar un aumento de la congestión judicial. Por lo anterior, aunque se garantizaria el derecho de algunos ciudadanos a obtener una decisión en un lenguaje claro y cercano, los ciudadanos en general tendrían que esperar más tiempo para obtener una respuesta del sistema judicial, lo que podria generar una vulneración al principio de acceso a la administración de justicia, concretamente, la garantía de obtener una respuesta en un plazo razonable.

(…)

(…) todas las entidades de la Rama Ejecutiva del nivel central y descentralizado tanto del orden nacional como territorial, así como los órganos autónomos y de control tendrían que implementar el formato de lectura fácil. Además de la Rama judicial, e incluso la Rama legislativa cuando ejerza función administrativa. Esto en los casos y temas enlistados en el artículo 2° del proyecto.

(…)

En resumen, el proyecto tiene un amplio campo de aplicación y de sujetos obligados: la mayoría de los servidores de las tres ramas del poder público. Además, su vigencia, y por ende la obligación de expedir los formatos de lectura fácil, inicia desde el momento de la promulgación. En concepto de esta dirección, la vigencia inmediata y amplio campo de aplicación de la norma puede agudizar la congestión judicial en la rama judicial e incrementar el tiempo de respuesta en las actuaciones administrativas. Pues, se aumentaria la carga de trabajo de las autoridades, al tener que realizar formatos de lectura fácil, aun en ausencia de un protocolo para realizar dichos formatos.

(…)

Por otro lado, sería importante analizar si en lugar de formatos adicionales a las sentencias tradicionales es más conveniente realizar cursos de redacción o fortalecer los actuales cursos de lenguaje claro, con el fin de lograr a largo plazo que todas las sentencias y decisiones administrativas estén redactadas en un lenguaje claro.

(…)

De acuerdo con lo anterior, en concepto de esta Dirección la imposición de un formato obligatorio de sentencia de lectura fácil debe respetar la autonomía de los jueces. En ese sentido, aunque el proyecto normativo tenga un fin loable, al dejar un margen muy amplio de reglamentación del formato de sentencia en manos de entidades administrativas podría configurarse una posible vulneración a la autonomía judicial.

(…)

Desde el artículo 177 de la Ley 270 de 1996, se prevé que la Escuela Judicial, "Rodrigo Lara Bonilla" se constituirá en el centro de formación inicial y continuada de funcionarios y empleados al servicio de la Administración de Justicia. En el marco de esas funciones se encuentra que la Escuela Judicial Lara Bonilla ha venido adelantando procesos de capacitación y formación a los servidores y funcionarios de la Rama Judicial sobre lenguaje jurídico claro y redacción de sentencias a manera de ejemplo: "Curso Sobre Lenguaje Jurídico Claro y Redacción De Sentencias" organizado por la AECID. Año 2019.

Al mismo tiempo, en los procesos de capacitación se han incluido en los procesos de formación general: el Módulo de Interpretación Judicial y Estructura de la Sentencia.

(…)

Adicionalmente, el artículo 176 de la misma ley, obliga a que cada empleado deberá tomar cursos de capacitación y actualización en técnicas de administración y gestión judicial cuando menos cada tres años.

Por lo anterior, de llegar a ser aprobado el proyecto de ley, se podria considerar afectada la libertad de expresión de la juez contemplada en el aparte "Libertad de expresión y administración de justicia": "El derecho de los jueces a la libertad de expresión y a formular comentarios sobre asuntos de interés público sólo debe estar sometido a restricciones claramente delimitadas conforme sea necesario para proteger su independencia e imparcialidad". Consignada en la Declaración Conjunta del ***Relator*** *Especial de la ONU sobre la libertad de Opinión y Expresión, el Representante de la OSeE sobre la libertad de Prensa y el Relator Especial de la OEA sobre libertad de Expresión.*

(…)

Con fundamento en lo expuesto no se considera conveniente la aprobación del Proyecto de Ley 89 de 2022 (…)". (Subrayado fuera del texto).

2. CORTE CONSTITUCIONAL.

A través de comunicación ECC-2022-5923 - PET26523, manifestaron:

"(…) Es necesario precisar que, de conformidad con el numeral 4 del artículo 241 de la Constitución Política, la Corte Constitucional en desarrollo de sus atribuciones constitucionales tiene la función de control de constitucionalidad sobre las leyes tanto por su contenido material como por vicios de procedimiento en su formación.

Conforme a lo anterior, ante la posibilidad de que la Ley en mención llegue a eventual revisión de este Tribunal, la presidenta no puede pronunciarse por posibles impedimentos que puedan surgir (…)".

3. CONSEJO DE ESTADO.

Mediante oficio CE-PRESIDENCIA-PQRS-INT-2022-2418 del 2 de septiembre de 2022 el Presidente del Consejo de Estado manifestó:

"(…) Sobre su escrito allegado a este despacho el 25 de agosto de 2022, en el que solicita, como ponente designado para el primer debate, concepto, comentarios y observaciones frente al Proyecto de Ley 89 de 2022 «Por medio de la cual se establece el formato de sentencias de lectura fácil y se dictan otras disposiciones», con el propósito de obtener insumos para rendir el informe de ponencia y en la medida en que las disposiciones contenidas en el proyecto se relacionan con las competencias de esta Corporación, se informa que el pasado 29 de agosto se remitió, para su consideración, a la Comisión Normativa del Consejo de Estado por intermedio de su coordinador, magistrado José Roberto Sáchica Méndez (…)".

4. COMISIÓN NORMATIVA DEL CONSEJO DE ESTADO.

A través de comunicación No. 2022-093 el Coordinador de la Comisión Normativa del Consejo de Estado manifestó:

"(…) La Comisión Normativa del Consejo de Estado, por encargo de su Presidente, tuvo oportunidad de revisar el tema relacionado con su solicitud para que esta Corporación emitiera su concepto, comentarios y observaciones frente al Proyecto de Ley No. 89 de 2022 Senado «Por medio de la cual se establece el formato de sentencias de lectura fácil y se dictan otras disposiciones».

El Consejo de Estado agradece su invitación. No obstante esta circunstancia, se abstendrá de presentar concepto sobre el asunto, sin perjuicio de que ponga de presente las cargas impositivas y de trabajo que la eventual normativa acarrearía para la Rama Judicial; circunstancias que, sin duda, y al lado de otras varias importantes consideraciones, estamos seguros que serán analizadas en el curso del trámite legislativo correspondiente (…)". (Subrayado fuera del texto).

5. CONSEJO SUPERIOR DE LA JUDICATURA.

Mediante oficio PCSJO22-521 el Presidente del Consejo Superior de la Judicatura expuso:

"(…) ***1. El Proyecto de Ley genera una posible afectación a la independencia judicial.***

(…)

De aprobarse el texto propuesto, el Honorable Congreso de la República estaría interviniendo en la órbita de la autonomía e independencia judicial. Lo anterior, toda vez que se le resultaría imponiendo a los operadores judiciales una estructura, estilo, presentación em incluso, lenguaje, en la elaboración de sus providencias judiciales.

Vale destacar que, aun cuando se trata de un formato adicional, que no excluye la providencia de "formato tradicional", se trataría de un acto procesal con igual valor y efectos que, por lo tanto, no solo vincula a las partes del proceso, sino también al mismo funcionario judicial que la dicta. En esa medida, bien podrían las partes procesales, o cualquier tercero legitimado, valerse de los dos formatos, ya sea el "tradicional" o el formato de "lectura fácil", para promover recursos, iniciar procesos ejecutivos o incidentes, acciones de tutela o, incluso, denuncias penales. Además esto afecta los principios de economía, eficacia y eficiencia procesales, pues obliga a realizar un reproceso, es decir elaborar la sentencia judicial y también un formato especial diferente.

Se deriva de lo expuesto que, al otorgar el mismo valor y efectos a los dos formatos, el honorable Congreso de la República estaría impartiendo una directriz concreta a los operadores judiciales respecto de la forma en que ejercen la función pública de administrar justicia. Esto supone una interferencia externa que, según se explicó, está vedada por nuestro ordenamiento constitucional.

2. El Proyecto de Ley podría incrementar la congestión en los despachos judiciales.

Establecer el formato de lectura fácil como acto procesal adicional, en contravía de la apremiante necesidad de reducir la congestión judicial y las cargas de trabajo de los servidores judiciales, resulta contrario al propósito de reducir la congestión judicial. Esto supone, no solo una presión laboral para los servidores judiciales, sino también una potencial deterioración de la propia administración de justicia, pues los despachos tendrán que incorporar dentro de sus esquemas de distribución de trabajo y manejo del tiempo, la realización del formato de lectura fácil, en detrimento de la dedicación necesaria para la impartición de justicia, propiamente dicha.

Adicionalmente, es necesario tener en cuenta que la descripción de los perfiles de trabajo en los despachos y corporaciones del país no incorpora, típicamente, la idoneidad y experiencia profesional necesaria para llevar a cabo la labor que supone realizar el formato de lectura fácil. En ese sentido, puede presumirse que su adecuada elaboración supondría una carga de trabajo y tiempo particularmente importante; cualquiera que sea el valor y efecto de dicho formato. Sin embargo, tratándose de un acto procesal que habrá de estar dotado del mismo valor y efecto de la providencia judicial en su "formato tradicional", la carga sería aún mayor.

3. Existencia de alternativas para lograr el mismo objetivo

En cualquier caso, el Honorable Congreso de la República debe tener en cuenta que nuestro ordenamiento jurídico ya dispone de medidas para incentivar la elaboración de providencias judiciales de fácil comprensión y, ulteriormente, quepodrían suplir el propósito de la providencia judicial.

Al respecto, se tiene que el artículo 5 de la Ley Estatutaria 270 de 1996 establece:

"Las sentencias judiciales deberán referirse a todos los hechos y asuntos planteados en el proceso por los sujetos procesales.

La pulcritud del lenguaje; la claridad, la precisión y la concreción de los hechos materia de los debates y de las pruebas que los respaldan, que los Magistrados y Jueces hagan en las providencias judiciales, se tendrán en cuenta como factores esenciales en la evaluación del factor cualitativo de la calificación de sus servicios (…)."

Esta disposición estatutaria, conlleva a un incentivo que, sin interferir en la órbita de la autonomía e independencia judicial, promueve la elaboración de providencias judiciales de fácil comprensión.

Adicionalmente, y en línea con lo indicado anteriormente, de esta norma se deriva que el formato de lectura fácil, al tener el mismo valor y efecto de la providencia en su "formato tradicional", no podría alejarse de lo preceptuado en el artículo 55 de la Ley 270 de 1996 ,y por lo tanto, deberá incorporar referencia atodos los hechos y asuntos planteados por los sujetos procesales durante el proceso. Lo anterior, profundiza particularmente el riesgo advertido en el punto 2 del presente escrito.

De otro lado, no puede perderse de vista que, en todos aquellos casos en los que para acceder a la administración de justicia se requiera actuar a través de abogado, los y las profesionales del derecho tendrán el deber legal de rendir informes sobre las gestiones encomendadas, según deriva del inciso segundo del artículo 37 de la Ley 1123 de 2007. Este deber supone transmitir con claridad, entre otros, el contenido de las providencias judiciales.

Finalmente, se resalta que el Plan de Formación de la Escuela Judicial "Rodrigo Lara Bonilla" de la vigencia 2022, aprobado por el Consejo Superior de la Judicatura mediante Acuerdo PCSJA22-11945 del 18 de abril de este año, incorpora el subprograma denominado "Formación en lenguaie judicial desde un enfoque práctico", que se justifica precisamente en considerar que "(...) el lenguaje que utiliza el servidor judicial debe ser comprensible para el ciudadano." (…)".

IV. ANÁLISIS DEL PROYECTO DE LEY.

1. El derecho al acceso a la administración de justicia y a la tutela judicial efectiva.

El artículo 229 de la Constitución dispone que "*Se garantiza el derecho de toda persona para acceder a la administración de justicia*". Así las cosas, este derecho se erige en nuestro Ordenamiento Jurídico como la garantía de que cualquier persona pueda acudir ante tribunales y jueces, en condiciones de igualdad para propugnar por la integridad del orden jurídico y por la debida protección o el restablecimiento de los derechos e intereses legítimos. Para la Corte Constitucional, el goce de esta garantía está supeditado a la estricta sujeción de los procedimientos previamente establecidos y con total observancia de las garantías sustanciales y procedimentales previstas en la ley[1].

Según la Corte Constitucional "*(…) el Estado debe garantizar su materialización y "(i) abstenerse de adoptar medidas discriminatorias o que obstaculicen el acceso a la justicia y su realización, (ii) impedir la interferencia o limitación del derecho y (iii) facilitar las condiciones para su goce efectivo (…)*"[2].

La garantía del derecho de acceso a la administración de justicia incluye el deber de dar una solución pronta y de fondo a los asuntos adelantados ante los funcionarios judiciales. Dichas decisiones deben ser adoptadas en un término razonable de tal forma que la respuesta judicial sea oportuna. En consecuencia, están prohibidas las dilaciones injustificadas en la administración de justicia[3].

[1] Sentencias T-283 de 2013 y T-052 de 2018.
[2] Sentencia C-426 de 2002.
[3] Sentencia T-441 de 2020.

En este orden de ideas se presentan en nuestro ordenamiento fenómenos como la mora judicial definido como "*un fenómeno multicausal, muchas veces estructural, que impide el disfrute efectivo del derecho de acceso a la administración de justicia (..) se presenta como resultado de acumulaciones procesales estructurales que superan la capacidad humana de los funcionarios a cuyo cargo se encuentra la solución de los procesos*"[4]. *La Corte Constitucional ha reconocido la realidad del país en materia de congestión del sistema judicial y el exceso de las cargas laborales*[5]. *Este tribunal es consciente que, en la mayoría de los casos, el represamiento de procesos "no permite a los funcionarios cumplir con los plazos legalmente establecidos*".[6]

La jurisprudencia constitucional ha fijado las circunstancias en las cuales se configura la mora judicial injustificada[7]. En primer lugar, cuando se presente un incumplimiento de los términos señalados en la ley para adelantar alguna actuación judicial. En segundo término, cuando no exista un motivo razonable que justifique dicha demora (i.e. congestión judicial o el volumen de trabajo). Por último, cuando la tardanza sea imputable a la omisión en el cumplimiento de las funciones por parte de una autoridad judicial[8].

La aprobación de una medida como la propuesta por la iniciativa objeto de estudio en las condiciones actuales de congestión judicial podría constituirse en un obstáculo en el acceso a la justicia y su realización generando posibles escenarios de mora judicial que vulneran este derecho.

2. La congestión judicial.

Aunque es loable querer simplificar el lenguaje empleado por el Estado para administrar justicia a través de las decisiones judiciales y administrativas, hacerlo operativo es más difícil de lo que parece. No solo porque la Rama Judicial no cuenta con el personal suficiente para prestar el apoyo técnico, administrativo y humano que requieren los jueces y magistrados del país sino porque ya es bastante difícil prestar el servicio bajo el modelo actual.

De hecho, en América Latina se ha reportado que en países como México hay jueces con hasta 900 procesos por resolver. Se trata de países donde la justicia tarda más de 600 días (2 años) en fallar sobre algo. Una situación aún más dramática ocurre en Colombia, donde la demora podría ascender hasta los 4 o 5 años. De ahí, fenómenos como la congestión judicial y la pérdida de confianza en el sistema judicial.

En esta misma línea:

- El índice Rule of Law (2022) de World Justice Project estima que el nivel de confianza en los sistemas judiciales latinoamericanos cayó un 61% en 2021.
- Por su parte, el Consejo Superior de la Judicatura estimó en el Índice de la Congestión de la Justicia en Colombia ascendió al 57.5% en 2021.
- En el Índice Global de Impunidad de la Universidad De Puebla (2022), Colombia figure entre los países con más impunidad a nivel global, ocupando la posición 49 de 69 países ranqueados.

Al respecto, el Ministerio de Justicia advirtió en 2021 que Colombia sólo tenía 11 jueces por cada 100.000 habitantes. En contraste, la Comisión Europea para la Eficiencia de la Justicia (2020) estimó en 18 el promedio de jueces de 47 países europeos. Por ende, esta iniciativa en lugar de contribuir a la descongestión terminará por extender los tiempos de respuesta de la justicia.

Por lo tanto, no se estima conveniente que se aumente la carga laboral de la Rama Judicial e incluso de los funcionarios que emiten decisiones administrativas. Cabe mencionar, que en un escenario de déficit de personal como el actual, el Estado debería dirigir sus esfuerzos a robustecer los recursos humanos y técnicos del poder judicial, esto es, aumentar el presupuesto de la rama, más personal de planta y la digitalización del servicio. Podría apelarse además a un trabajo conjunto con el sector educativo (las facultades de derecho) para articular esfuerzos y capacitar a estudiantes y miembros de la rama judicial en la simplificación del lenguaje empleado en las decisiones judiciales en el mediano y largo plazo.

V. CONFLICTO DE INTERÉS.

Dando alcance a lo establecido en el artículo 3 de la Ley 2003 de 2019 "*Por la cual se modifica parcialmente la Ley 5 de 1992*", se hacen las siguientes consideraciones a fin de describir las circunstancias o eventos que podrían generar conflicto de interés en la discusión y votación de la presente iniciativa legislativa, de conformidad con el artículo 286 de la Ley 5 de 1992, modificado por el artículo 1 de la Ley 2003 de 2019, a cuyo tenor reza:

> *"(…) Artículo 286. Régimen de conflicto de interés de los congresistas. Todos los congresistas deberán declarar los conflictos De intereses que pudieran surgir en ejercicio de sus funciones.*
>
> *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.*

[4] Sentencia T-052 de 2018.
[5] Sentencia SU-394 de 2016.
6 Ibídem.
[7] Sentencias T-292 de 1999, T-220 de 2007, T-230 de 2013 y T-052 de 2018.
[8] Sentencia T-099-2021.

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 (…)".

Sobre este asunto la Sala Plena Contenciosa Administrativa del Honorable Consejo de Estado en su Sentencia 02830 del 16 de julio de 2019, M.P. Carlos Enrique Moreno Rubio, señaló que:

"(…) 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 (…)".

Así las cosas, siguiendo lo dispuesto por el artículo 3 de la Ley 2003 de 2019, que modifica el artículo 291 de la Ley 5 de 1992, que dispone el incluir "*un acápite que describa las circunstancias o eventos que podrían generar un conflicto de interés para la discusión y votación del proyecto, de acuerdo al artículo 286*", se señala que este proyecto de ley no genera conflicto de interés pues busca beneficios generales.

En todo caso, esto no exime a que el congresista que así lo considere, manifieste otras razones por las cuales pueda tener conflictos de intereses.

Finalmente, se recuerda que se deberá tener en cuenta lo establecido en la Sentencia C-302 de 2021 de la Corte Constitucional que declaró inconstitucional el literal e) del artículo 1 de la Ley 2003 de 2019, que establecía que los congresistas no incurren en conflicto de interés cuando participan, discuten o votan artículos que beneficien a los sectores económicos de los financiadores de su campaña electoral . En ese sentido, las posibles causales de conflicto señaladas previamente con relación al congresista, cónyuge, compañero o compañera permanente, o parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil, también serán aplicables con respecto a los financiadores de campaña.

VI. PROPOSICIÓN.

Con fundamento en las anteriores consideraciones, de manera respetuosa solicito a la Comisión Primera del Senado de la República **ARCHIVAR** el Proyecto de Ley No. 89 de 2022 Senado "*Por medio de la cual se establece el formato de sentencias de lectura fácil y se dictan otras disposiciones*".

Atentamente,

CARLOS FERNANDO MOTOA SOLARTE
Ponente

INFORME DE PONENCIA PARA PRIMER DEBATE PROYECTO DE LEY NÚMERO 331 DE 2023 SENADO

por medio del cual se crea la Agencia Nacional de Seguridad Digital y se dictan otras disposiciones.

INFORME DE PONENCIA PARA PRIMER DEBATE PROYECTO DE LEY NO. 331 DE 2023 SENADO "POR MEDIO DEL CUAL SE CREA LA AGENCIA NACIONAL DE SEGURIDAD DIGITAL Y SE DICTAN OTRAS DISPOSICIONES"

Bogotá, D.C., junio de 2023

Señor
FABIO RAÚL AMÍN SALEME
Presidente
COMISIÓN PRIMERA
SENADO DE LA REPÚBLICA
Ciudad

Asunto: Ponencia para primer debate del Proyecto de Ley No. 331/2023 Senado "Por medio del cual se crea la Agencia Nacional de Seguridad Digital y se dictan otras disposiciones"

Respetado señor Presidente:

En cumplimiento del encargo recibido por parte de la honorable Mesa Directiva de la Comisión Primera del Senado de la República y de conformidad con lo establecido en el artículo 150 de la Ley 5ª de 1992, procedemos a rendir Informe de Ponencia positiva para primer debate del Proyecto de Ley 331/2023 Senado "Por medio del cual se crea la Agencia Nacional de Seguridad Digital y se dictan otras disposiciones"

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 23 de mayo 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.540 de 2023

1.3. La Secretaría de la Comisión Primera Constitucional del Senado de la República comunicó el 01 de junio de 2023, que de acuerdo con el Acta MD-31 de la Mesa Directiva de la Comisión se designó como ponentes al senador David Luna y al Senador Alfredo De Luque.

1.4. El Proyecto de Ley 331/2023 fue remitido a veintitrés (23) organizaciones expertas en la materia, para que emitieran observaciones al texto radicado. Algunas de las observaciones presentadas se incluyeron en el pliego de modificaciones. Las organizaciones y entidades a la cuales se les remitió para comentarios el PL 331/2023, 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

1.5 De las veintitrés (23) organizaciones mencionadas anteriormente se recibieron comentarios de:

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

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 el país.

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, Empresas Públicas de Medellín, 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.

Este Proyecto de Ley establece acciones para garantizar la coordinación entre el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT); Comando Conjunto Cibernético y el Centro Cibernético Policial, así como con el Ministerio de Tecnologías de la Información y las Comunicaciones; 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 significará 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 de Ley 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, en este caso, 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).

De esa manera, con la presentación de este Proyecto de Ley hacemos un llamado respetuoso al gobierno nacional a que avale la presente iniciativa de vital importancia para la seguridad del país, teniendo en cuenta los recientes ataques de los que hemos sido víctimas, y los riesgos de ataques futuros ante la falta de adopción de las medidas necesarias.

CONTEXTO ACTUAL:

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

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

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

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

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

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

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

Modelo de Gobernanza en Seguridad Digital Actual:

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

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

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

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

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

las Comunicaciones y establecer organismos de respuesta a los incidentes cibernéticos de la Nación.

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

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

Mediante la Resolución 05839 de 2015, la Policía Nacional de Colombia establece las funciones del Centro Cibernético Policial como una dependencia de la Dirección de Investigación Criminal *"encargada de desarrollar estrategias, programas, y proyectos para la ciberseguridad, ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal"* (Resolución 05839, 2015, art. 15).

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

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

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

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

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

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

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

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

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

Agencias Internacionales de Seguridad Digital:

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

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

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

NOMBRE	PAÍS	AÑO DE CREACIÓN	DESCRIPCIÓN
BSI - Bundesamt für Sicherheit in der Informationstechnik	Alemania	1991	Es responsable de la seguridad de la información y la ciberseguridad en el país. Tiene como objetivo proteger los sistemas de información y las infraestructuras críticas de Alemania, así como brindar asesoramiento y orientación a entidades públicas, privadas y ciudadanos en materia de seguridad cibernética.
ENISA - European Union Agency for Cybersecurity	Unión Europea	2004	Junto a la Red del Centro Nacional de Coordinación de la Unión Europea (NCCs) coordinan las políticas de innovación y política industrial en ciberseguridad de la Unión Europea. Busca fortalecer las capacidades en materia de tecnología para promover la economía y proteger a los ciudadanos de ataques cibernéticos.
ANSSI- Agence Nationale de la sécurité des systèmes d' information	Francia	2009	Creada por medio de la Ley de Programación Militar de Francia con el objetivo de proteger la información y la infraestructura crítica del país. Es la autoridad nacional en materia de seguridad cibernética y tiene la responsabilidad de cuidar los sistemas de información críticos del gobierno, empresas y organizaciones clave en Francia.
ACSC- Australian Cyber Security Agency	Australia	2014	Establecido como iniciativa del Gobierno para fortalecer y coordinar la ciberseguridad en el país. Se encarga de proporcionar orientación, inteligencia, asesoramiento y respuesta a incidentes de ciberseguridad.

NCSC- National Cyber Security Centre	Reino Unido	2016	Tiene la responsabilidad de proteger al Reino Unido contra amenazas cibernéticas proporcionando orientación y asesoramiento en Seguridad Digital y coordinar la respuesta a incidentes cibernéticos a nivel nacional.
CISA- Cybersecurity and Infraestructura Security Agency	Estados Unidos	2018	Es una Agencia adscrita al Departamento de Seguridad Nacional de los Estados Unidos y tiene la responsabilidad de proteger la infraestructura crítica del país, de promover la seguridad cibernética y coordinar la respuesta del país ante incidentes cibernéticos.
CCCS - Canadian Centre for Cyber Security	Canadá	2018	Tiene la responsabilidad de proteger y defender las redes de información y sistemas de Canadá ante amenazas cibernéticas. Proporciona asesoramiento y orientación en ciberseguridad tanto a entidades del estado, como al sector privado del país. Busca promover la colaboración y la cooperación en materia de ciberseguridad a nivel nacional e internacional.

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

REFERENCIAS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. CONFLICTOS DE INTERÉS:

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

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

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

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

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

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

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

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

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

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

5. PLIEGO DE MODIFICACIONES:

TEXTO DEFINITIVO PRIMER DEBATE SENADO DE LA REPÚBLICA	PROPUESTA DE MODIFICACIONES	JUSTIFICACIÓN
Artículo 1. Objeto. La presente Ley tiene por objeto la creación de la	Sin modificaciones	

Agencia Nacional de Seguridad Digital, establecer sus funciones y dictar otras disposiciones.		
Artículo 2. Definiciones. Para la aplicación de la presente ley se tendrán en cuenta las siguientes definiciones: *Seguridad Digital.* Políticas, medidas y prácticas diseñadas para proteger la información, infraestructura crítica, datos sensibles, sistemas de información y ciudadanos frente a amenazas cibernéticas. Tiene como objetivo salvaguardar la soberanía nacional, la estabilidad económica, la seguridad nacional y el bienestar de los ciudadanos en el ciberespacio. *Ciberdefensa*. Capacidad del Estado para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la soberanía nacional. *Ciberseguridad.* Adopción de medidas, prácticas y tecnologías, tales como firewalls, sistemas de detección, prevención de intrusiones, sistemas de autenticación y cifrado de datos que salvaguarden los sistemas informáticos, las redes y los datos de las infraestructuras críticas y	**Artículo 2. Definiciones.** Para la aplicación de la presente ley se tendrán en cuenta las siguientes definiciones: *Seguridad Digital.* ~~Políticas, medidas y prácticas diseñadas para proteger la información, infraestructura crítica, datos sensibles, sistemas de información y ciudadanos frente a amenazas cibernéticas. Tiene como objetivo salvaguardar la soberanía nacional, la estabilidad económica, la seguridad nacional y el bienestar de los ciudadanos en el ciberespacio.~~ **Situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (1) la gestión del riesgo de seguridad digital; (2) la implementación efectiva de medidas de ciberseguridad y (3) el uso efectivo de las capacidad de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.**	Se cambia la definición de protección de datos personales para que se encuentre acorde con la legislación previa. Se incluye la definición de CSIRT como un eje transversal en la creación de la Agencia Nacional de Seguridad Digital (ANSD). El concepto de delitos cibernéticos no se limita a la Ley 1273, pues deja por fuera delitos como la pornografía infantil, copyright, entre otros. En ese sentido, se plantea una definición acorde con el objetivo del proyecto de ley. En la definición del Grupo de Respuesta Emergencias Cibernéticas de Colombia ColCERT se elimina el término ciberdefensa, pues no cumple con estas funciones. Los conceptos de Seguridad Digital y Ciberseguridad son modificados para que tengan un propósito de confianza para la ciudadanía y fortalecimiento de las economías digitales y no un enfoque militarista, ya no usado en la concepción actual de ciberseguridad,

los ciudadanos de una nación ante amenazas cibernéticas. *Ciberespacio.* Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética. *Ciberataque.* Acciones maliciosas con la intención de causar daño, interrupciones o conseguir acceso no autorizado a sistemas informáticos, redes o dispositivos mediante el uso de medios cibernéticos. *Delitos Cibernéticos.* Conductas ilícitas en las que los delincuentes utilizan programas informáticos y tecnologías de la información para cometer delitos, de conformidad con lo establecido en la Ley 1273 del 2009 o aquellas que la modifiquen deroguen o sustituyan. *Infraestructuras Críticas.* Sistemas, redes, instalaciones y servicios que son considerados esenciales para el funcionamiento y la seguridad de la Nación, tales como energía, transporte, comunicaciones, finanzas, salud y seguridad pública.	*Ciberdefensa*. Capacidad del Estado para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la soberanía nacional. *Ciberseguridad.* ~~Adopción de medidas, prácticas y tecnologías, tales como firewalls, sistemas de detección, prevención de intrusiones, sistemas de autenticación y cifrado de datos que salvaguarden los sistemas informáticos, las redes y los datos de las infraestructuras críticas y los ciudadanos de una nación ante amenazas cibernéticas.~~ **Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.** *Ciberespacio.* ~~Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la~~	apoyada por la OCDE. Se modifica la definición de ciberespacio, para hacerla acorde al propósito del proyecto de ley. Se incluye la definición de delito ciber habilitados o facilitados por la tecnologías, para demarcar su diferencia con los ciberdelitos. Se incluye el concepto de ciberdiplomacia.

Protección de Datos Personales. El derecho fundamental de las personas a la privacidad y control sobre sus datos personales. Implica deberes y responsabilidades de los encargados de los tratamientos de datos, así como los derechos de los titulares de los datos. *Comando Conjunto Cibernético (CCOCI).* Es el equipo encargado de la defensa del país en el ciberespacio y garante de la protección de las infraestructuras críticas cibernéticas nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional. *Centro Cibernético Policial (CCP).* Es el equipo encargado de la seguridad ciudadana en el ciberespacio. Es una unidad de la Policía Nacional de Colombia encargada de la investigación y la lucha contra delitos cibernéticos que afecten a la ciudadanía dentro del ciberespacio. Brinda capacitación y educación en materia de seguridad informática a otros	~~civilización de la electrónica, la informática y la cibernética.~~ **Ambiente formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos, usando redes computacionales.** *Ciberataque.* Acciones maliciosas con la intención de causar daño, interrupciones o conseguir acceso no autorizado a sistemas informáticos, redes o dispositivos mediante el uso de medios cibernéticos. *Delitos Cibernéticos.* ~~Conductas ilícitas en las que los delincuentes utilizan programas informáticos y tecnologías de la información para cometer delitos, de conformidad con lo establecido en la Ley 1273 del 2009 o aquellas que la modifiquen deroguen o sustituyan.~~ **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.** ***Delitos ciber habilitados:*** **Aquellos que existían de forma previa a las TIC's, pero que, con el desarrollo de éstas, ahora se desarrollan también**	

miembros de polícia y al público en general. *Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT.* Es el organismo coordinador a nivel nacional en temas de ciberseguridad y ciberdefensa, adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones e integrado por funcionarios civiles, personal militar y en comisión de otras entidades. Su misión es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que lo atenten o comprometan.	**mediante la modalidad cibernética.** *Infraestructuras Críticas.* Sistemas, redes, instalaciones y servicios que son considerados esenciales para el funcionamiento y la seguridad de la Nación, tales como energía, transporte, comunicaciones, finanzas, salud y seguridad pública. *Protección de Datos Personales.* ~~**El derecho fundamental de las personas a la privacidad y control sobre sus datos personales. Implica deberes y responsabilidades de los encargados de los tratamientos de datos, así como los derechos de los titulares de los datos.**~~ **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.** **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. **Autoridad de Protección de Datos Personales. Autoridad encargada de la protección de datos personales.** *Comando Conjunto Cibernético (CCOCI).* Es el equipo encargado de la defensa del país en el ciberespacio y garante de la protección de las infraestructuras críticas cibernéticas nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional. *Centro Cibernético Policial (CCP).* Es el equipo encargado de la seguridad ciudadana en el ciberespacio. Es una unidad de la Policía Nacional de Colombia encargada de la investigación y la lucha contra delitos cibernéticos que afecten a la ciudadanía dentro del ciberespacio. Brinda capacitación y educación en materia de seguridad informática a otros miembros de polícia y al público en general. *Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT.* Es el organismo coordinador a nivel nacional en temas de	

	ciberseguridad ~~y ciberdefensa~~, adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones e integrado por funcionarios civiles, personal militar y en comisión de otras entidades. Su misión es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que lo atenten o comprometan. **Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). Organización que tiene como misión responder de forma urgente y coordinada ante ataques cibernéticos.** **Ciberdiplomacia: Uso de herramientas diplomáticas para resolver asuntos relativos del ciberespacio.**	
Artículo 3. Creación de la Agencia Nacional de Seguridad Digital. Créase la Unidad Administrativa Especial denominada Agencia Nacional de Seguridad Digital y (ANSD), entidad descentralizada, del orden nacional, que forma parte de la Rama Ejecutiva, con personería jurídica, autonomía administrativa,	**Artículo 3.** Creación de la Agencia Nacional de Seguridad Digital. Créase la Unidad Administrativa Especial denominada Agencia Nacional de Seguridad Digital y (ANSD), entidad descentralizada, del orden nacional, **adscrita al Ministerio de Tecnologías de la Información y las**	Teniendo en cuenta la calidad de Unidad Administrativa, la agencia será adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

financiera y patrimonio propio.	**Comunicaciones**, que forma parte de la Rama Ejecutiva, con personería jurídica, autonomía administrativa, financiera y patrimonio propio.	
Artículo 4. Autoridad. La Agencia Nacional de Seguridad Digital (ANSD) es la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de seguridad digital y ciberdefensa nacional.	Sin modificaciones.	
Artículo 5. Funciones: La Agencia Nacional para la Seguridad Digital (ANSD) ejercerá las siguiente funciones: **1. Coordinación y colaboración:** 1.1 Trabajar en colaboración con las entidades del Estado, así como con el sector privado y los ciudadanos para mitigar los efectos de ciberataques. 1.2 Coordinar y gestionar la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que brinde información	**Artículo 5. Funciones:** La Agencia Nacional para la Seguridad Digital (ANSD) ejercerá las siguientes funciones: **Coordinación y colaboración:** 1.1 Trabajar en colaboración con las entidades del Estado, así como con el sector privado y los ciudadanos para **coordinar las acciones para mitigar los efectos de ciberataques**. 1.2 Coordinar y gestionar la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que	1.3 Se elimina la redacción que puede dar pie a sustituir funciones de la Fiscalía General de la Nación, propósito que no tendrá la Agencia y se establece el concepto de ciberdiplomacia en coordinación con el Ministerio de Relaciones Exteriores. 1.6. Se agregan funciones de vocería. 1.7 Se agrega la función de articulación con el Estado. 2.1 Se propone este cambio pues al ser un ente coordinador, no sería el encargado de mitigar el riesgo, sino de coordinar las acciones que realicen las entidades.

a los ciudadanos sobre los ciberataques y delitos cibernéticos perpetrados en el territorio nacional. 1.3 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 dar con el paradero de los responsables de ciberataques perpetrados contra las infraestructuras críticas de la Nación. 1.4 Promover la colaboración y cooperación entre entidades del Estado, el sector privado y los ciudadanos para recibir de manera oportuna cualquier información que salvaguarde la Seguridad Digital de la Nación. 1.5 Articular y apoyar las acciones que realicen las entidades del Estado para	brinde información a los ciudadanos sobre los ciberataques y delitos cibernéticos perpetrados en el territorio nacional. 1.3 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 dar con el paradero de los responsables de ciberataques perpetrados contra las infraestructuras críticas de la Nación.~~ **y coordinar con el Ministerio de Relaciones Exteriores, las acciones de ciberdiplomacia que se requieran para dicho fin.** 1.4 Promover la colaboración y cooperación entre entidades del Estado, el sector privado y los ciudadanos para recibir de manera oportuna cualquier información que salvaguarde la	3.1 Se incluye la función de concientización sobre las amenazas al ciberespacio en coordinación con el Ministerio de Educación Nacional. 3.4 Se propone la eliminación de la palabras investigar, pues la agencia no tiene un propósito de investigación y análisis del crimen, sino un rol de coordinación entre las entidades encargadas de dicho aspecto. Así mismo, la Agencia acompañará a las entidades públicas y las empresas privadas en el proceso de investigación de ciberataques con el fin de garantizar la rápida respuesta y toma de acciones sobre los hechos perpetrados. 3.6 Colombia debe fortalecer su investigación y desarrollo tecnológico en temas de ciberseguridad. La Agencia, en conjunto con el Ministerio de Ciencia, Tecnología e Innovación será la responsable de la creación de la hoja de ruta que seguirá el país para desarrollar estas habilidades necesarias para el desarrollo profesional de los colombianos. 3.7 Es importante disminuir las falencias en el número de

garantizar la Seguridad Digital y la Ciberdefensa del Estado. **2. Evaluación y mitigación de riesgos:** 2.1 Es la encargada de realizar la evaluación de riesgos en materia de Seguridad Digital de las entidades del Estado con el fin de identificar, mitigar y controlar riesgos identificados en materia de delitos cibernéticos. 2.2 Proporcionar orientación sobre la implementación de medidas de seguridad adecuadas en el ciberespacio y promover el cumplimiento de prácticas de ciberseguridad. 2.4 Realizar análisis de amenazas cibernéticas y ayuda a entidades del Estado, al sector privado y a los ciudadanos a comprender las tácticas, técnicas y procedimientos de los delincuentes ante eventuales ciberataques.	Seguridad Digital de la Nación. 1.5 Articular y apoyar las acciones que realicen las entidades del Estado para garantizar la Seguridad Digital y la Ciberdefensa del Estado. **1.6 Ejercer la vocería e informar los protocolos y medidas de seguridad implementadas en caso de ciberataques. Para ello, se delegará a funcionarios de la agencia o de alguna de las instancias nacionales públicas.** **1.7 Articular y apoyar las acciones que realicen las entidades del Estado para garantizar la Seguridad Digital y la Ciberdefensa del Estado.** **Evaluación y mitigación de riesgos:** 2.1 ~~**Es la encargada de realizar la evaluación de riesgos en materia de**~~ **Gestionar los planes y**	profesionales en las áreas de ciberseguridad y atender los requerimientos de la industria TIC. Esta función garantiza que los colombianos tengan facilidades a la hora de decidir un camino profesional en estas áreas del conocimiento. 4.1 Se acumulan los puntos 4.1 y 4.2, pues el Plan Nacional de Seguridad Digital definirá los estándares en materia de seguridad digital de entidades públicas y el sector privado. 4.3 Se incluyen las entidades del Estado que son claves para el desarrollo del Observatorio de Seguridad Digital y Ciberdefensa.
2.5 Ofrecer asesoramiento y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en Seguridad Digital y Ciberdefensa. **3. Educación y prevención:** 3.1 Ofrecer programas de educación y concientización para ayudar a entidades del Estado, al sector privado y a los ciudadanos a comprender cómo detectar amenazas cibernéticas y cómo proceder en caso de ellas. 3.2 Trabajar de manera conjunta con las comunidades educativas y de investigación en temas relacionados con la Seguridad Digital y la Ciberdefensa de la Nación con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar el riesgo ante ataques cibernéticos. 3.3 Colaborar con la industria, las instituciones	**controles de mitigación del riesgo en materia** de Seguridad Digital de ~~las entidades~~ del Estado, y **de apoyar a las entidades del Estado en la elaboración de evaluaciones de riesgo de seguridad digital con el fin de** identificar, ~~**mitigar**~~ y controlar riesgos identificados en materia de delitos cibernéticos. 2.2 Proporcionar orientación sobre la implementación de medidas de seguridad adecuadas en el ciberespacio y promover el cumplimiento de prácticas de ciberseguridad, **basado en los estándares y mejores prácticas internacionales reconocidos por la industria.** 2.~~4~~ **3** Realizar análisis de amenazas cibernéticas y ~~ayudar~~ **colaborar con entidades** del Estado, ~~al~~ sector privado y ~~a los~~ ciudadanos ~~a comprender~~ **en el entendimiento de** las tácticas, técnicas y procedimientos de los delincuentes, ante eventuales ciberataques. 2.~~5~~ **4** Ofrecer asesoramiento y apoyo técnico a las entidades del Estado, al sector privado y	

académicas y los centros de investigación de orden tanto nacional, como internacional, con el fin de promover la innovación y el avance de tecnologías y soluciones de Seguridad Digital y Ciberdefensa. 3.4 Desarrollar mecanismos de ciberseguridad con el fin de investigar responsables, causas y circunstancias de ciberataques y delitos cibernéticos que se perpetúen en el territorio nacional. 3.5 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.	a los ciudadanos en Seguridad Digital y Ciberdefensa. **3. Educación y prevención:** 3.1 Ofrecer **en coordinación con el Ministerio de Educación Nacional** programas de educación y concientización ~~para ayudar~~ **dirigidos** a entidades del Estado, al sector privado y a los ciudadanos~~ a comprender cómo~~ **sobre la** ~~detectar~~ **detección de** amenazas cibernéticas y cómo proceder en caso de ellas. 3.2 Trabajar de manera conjunta con las comunidades educativas y de investigación en temas relacionados con la seguridad digital y la ciberdefensa de la Nación, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar el riesgo ante ataques cibernéticos. 3.3 Colaborar con ~~la industria,~~ **los particulares**, las instituciones académicas y los centros de investigación de orden tanto nacional, como internacional, con el fin de promover la innovación y el avance de tecnologías y soluciones de seguridad digital y ciberdefensa.	
4. Planificación: 4.1. Diseñar y expedir los estándares en materia de seguridad digital que las entidades públicas y el sector privado deben adoptar en materia de seguridad digital. 4.2. Diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa de la Nación. 4.3. Crear y coordinar el Observatorio de Seguridad Digital y Ciberdefensa, el cual tiene como fin reunir información y presentarla, mínimo una vez al año, a los ciudadanos sobre los ataques cibernéticos	**3.4** ~~Desarrollar mecanismos de ciberseguridad con el fin de investigar~~ de **Colaborar con las entidades responsables en la investigación de los hechos,** las causas y circunstancias de ciberataques y delitos cibernéticos que se ~~perpetúen~~ **perpetren** en el territorio nacional. **Así mismo, proporcionará acompañamiento en el proceso de investigación a entidades públicas y empresas privadas.** 3.5 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. **3.6 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.**	

presentados a las infraestructuras críticas de la Nación, así como a empresas privadas y entidades del sector público. 4.4. Reunir, procesar, interpretar y analizar la información suministrada por las entidades del Estado, el sector privado y los ciudadanos dados con el fin de identificar los responsables de ciberataques y delitos cibernéticos perpetrados en Colombia. **5. De ejecución:** 5.1. Implementar una estrategia de apoyo y asistencia técnica gradual al sector público para la debida implementación de los estándares y directrices en materia de	**3.7 Fomentar, en conjunto con el Ministerio de Educación Nacional, el estudio de carreras profesionales enfocadas en la ciberseguridad.** **4. Planificación:** 4.1 **Acorde con las recomendaciones y estándares internacionales,** diseñar **y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa de la Nación, el cual contendrá** los estándares en materia de seguridad digital que las entidades públicas y el sector privado deben adoptar ~~en materia de seguridad digital.~~ ~~**4.2 Diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa de la Nación.**~~ 4.3 ~~Crear~~ **Constituir** y coordinar el Observatorio de Seguridad Digital y Ciberdefensa, el cual tiene como fin reunir información ~~y presentarla, mínimo una vez al año, a los ciudadanos~~ sobre los ataques cibernéticos presentados a las infraestructuras críticas de la Nación, así como a	
Seguridad Digital. Para ello, la agencia promoverá la colaboración público privada con empresas especializadas que le permita generar las capacidades técnicas necesarias para ello. 5.2 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; servicios públicos; así como otros que considere pertinentes.	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 Internacionales, 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** 4.4 Reunir, procesar, interpretar y analizar la información suministrada por las entidades del Estado, el sector privado y los ciudadanos, ~~dados~~ con el fin de identificar los responsables de ciberataques y delitos cibernéticos perpetrados en Colombia. **5. De ejecución:** 5.1. Implementar una estrategia de apoyo y asistencia técnica gradual al sector público para la debida ~~implementación~~ **aplicación** de los estándares y directrices en materia de seguridad digital. Para ello, la agencia promoverá la colaboración público- privada con	

	empresas especializadas que le permita generar las capacidades técnicas necesarias para ello. 5.2 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.~~	
Artículo 6. Régimen jurídico. Los actos unilaterales que expida la Agencia Nacional de Seguridad Digital y Ciberdefensa (ANSD) son actos administrativos y se sujetan a las disposiciones del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.	Sin modificaciones	
Artículo 7. Protección de datos. El funcionamiento de la Agencia y demás órganos asociados creados mediante esta ley, se desarrollará en estricto cumplimiento del derecho a la protección de los datos personales, de conformidad con la Constitución y la Ley	**Artículo 7. Protección de datos.** El funcionamiento de la Agencia y demás órganos asociados creados mediante esta ley, se desarrollará en estricto cumplimiento del derecho a la protección de los datos personales, de conformidad con la Constitución y la Ley	Se incluye el parágrafo 1 con el fin de indicar que la Superintendencia de Industria y Comercio vigilará la protección de los datos personales de los colombianos por parte de la ANSD.

Estatutaria 1581 de 2012, o aquella que la modifique, reemplace o derogue.	Estatutaria 1581 de 2012, o aquella que la modifique, reemplace o derogue. **Parágrafo 1. La Superintendencia de Industria y Comercio vigilará el respeto del derecho a la protección de datos por parte de la ANSD.**	
Artículo 8. Estructura. La Agencia Nacional de Seguridad Digital (ANSD) tendrá la siguiente estructura para el cumplimiento de su objeto. 1. Consejo Directivo. 2. Dirección General. 3. Secretaría General. 4. Dirección de Investigación. 5. Dirección de Capacitación. 6. Dirección de Planificación. 7. Dirección del Observatorio Nacional de Seguridad Digital y Ciberdefensa. 8. Consejo Público - Privado contra los ciberataques y delitos cibernéticos. **Parágrafo 1.** Los Directores de Investigación, Capacitación y Planificación de la Agencia Nacional de Seguridad Digital (ANSD) serán de libre nombramiento y	**Artículo 8. Estructura.** La Agencia Nacional de Seguridad Digital (ANSD) tendrá la siguiente estructura: ~~para el cumplimiento de su objeto.~~ 1. Consejo Directivo - **Operacional** 2. Dirección General. 3. Secretaría General. 4. Dirección de Investigación. 5. Dirección de Capacitación. 6. Dirección de Planificación. 7. Dirección del Observatorio Nacional de Seguridad Digital y Ciberdefensa. 8. Consejo Público - Privado **de estrategia** contra los ciberataques y delitos cibernéticos. **9. Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT** **10. Equipo de Respuestas a**	1. Se tipifica la misión del Consejo Directivo, el cual tendrá un rol operativo. 8. Se tipifica la misión del Consejo Público Privado, el cual tendrá un rol estratégico. 9. El Grupo de Respuesta a Emergencias Cibernéticas colCERT y el CSIRT Gobierno harán parte de la agencia para garantizar las acciones de coordinación. En el parágrafo 2 se aclara que dichas entidades pasarán de ser parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a ser parte de la Agencia Nacional de Seguridad Digital (ANSD).

remoción por mandato del Director General de la Agencia Nacional de Seguridad Digital (ANSD). Sin embargo, los requisitos técnicos y profesionales y de experiencia para su nombramiento y posesión deberán establecerse vía decreto reglamentario, que será expedido a más tardar dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente Ley.	**Incidentes de Seguridad CSIRT gobierno.** **Parágrafo 1.** Los Directores de Investigación, Capacitación y Planificación de la Agencia Nacional de Seguridad Digital (ANSD) serán de libre nombramiento y remoción por mandato del Director General de la Agencia Nacional de Seguridad Digital (ANSD). Sin embargo, los requisitos técnicos y profesionales y de experiencia para su nombramiento y posesión deberán establecerse vía decreto reglamentario, que será expedido a más tardar dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente Ley. **Parágrafo 2. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) y el CSIRT Gobierno, adscritas hoy al Ministerio de Tecnologías de Información y Comunicaciones, pasarán a estar adscritas a la Agencia Nacional de Seguridad Digital.**	
Artículo 9. Órganos de Dirección y	**Artículo 9. Órganos de Dirección y**	Se establece la misión del Consejo Directivo, el cual tendrá un rol operativo.

Administración. La Dirección y la administración de recursos de la Agencia Nacional de Seguridad Digital (ANSD) estará a cargo del Consejo Directivo y el Director General. El Director General actuará como Representante Legal y será un funcionario de libre nombramiento y remoción por parte del Presidente de la República.	**Administración.** La Dirección y la administración de recursos de la Agencia Nacional de Seguridad Digital (ANSD) estará a cargo del Consejo Directivo **- Operacional** y el Director General. El Director General actuará como Representante Legal y será un funcionario de libre nombramiento y remoción por parte del Presidente de la República.	
Artículo 10. Integración del Consejo Directivo. El Consejo Directivo de la Agencia Nacional de Seguridad Digital (ANSD) estará integrado por los siguientes miembros: 1. El Ministro de Defensa o su delegado. 2. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado. 3. El Ministro de Ciencia, Tecnología e Innovación o su delegado. 4. El Director de la Policía Nacional o su delegado. 5. El Fiscal General de la República o su delegado. 6. El Director General de la Dirección	**Artículo 10. Integración del Consejo Directivo - Operacional** El Consejo Directivo **Operacional** de la Agencia Nacional de Seguridad Digital (ANSD) estará integrado por los siguientes miembros: 1. El Ministro de Defensa o su delegado. 2. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado. **~~3. El Ministro de Ciencia, Tecnología e Innovación o su delegado.~~ El Superintendente de Industria y Comercio o su delegado.**	3. Se elimina como integrante al Ministerio de Ciencia, Tecnología e Innovación, pues el Consejo Directivo Operacional será el encargado de reaccionar y analizar los ataques perpetrados en el país, no de planear estrategias a largo plazo. Se agrega como integrante al Superintendente de Industria y Comercio, pues se plantea que la SIC y la Agencia trabajarán en estrecha coordinación para garantizar la protección de los datos personales de los colombianos. 7. Se elimina el punto 7 y 8 y se deja abierto para que el CSIRT participante en el Consejo Directivo, sea el que corresponda, según la amenaza

Nacional de Inteligencia (DNI) o su delegado. 7. El Representante del CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) - Policía Nacional. 8. Los Representante de dos (2) CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) del Sector Privado **Parágrafo 1.** El Consejo Directivo de la Agencia Nacional de Seguridad Digital (ANSD) se reunirá por lo menos una vez al mes o cuando sea convocado ante eventuales riesgos en la materia.	4. El Director de la Policía Nacional o su delegado. 5. El Fiscal General de la ~~República~~ **Nación** o su delegado. 6. El Director General de la Dirección Nacional de Inteligencia (DNI) o su delegado. **7. El Comandante de las Fuerzas Militares o su delegado.** **~~8. El Representante del CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) Los representantes de los CSIRT, tanto públicos como privados que sean citados o necesarios para la atención de la amenaza detectada. Policía Nacional.~~** **9. ~~Los Representante de dos (2) CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) del Sector Privado~~** **Parágrafo 1.** El Consejo Directivo de la Agencia Nacional de Seguridad Digital (ANSD) se reunirá por lo menos una vez al mes o cuando sea	recibida. Parágrafo 2: Se establece el rol del Consejo Directivo - Operacional.

	convocado ante eventuales riesgos en la materia. **Parágrafo 2. El Consejo Directivo - Operacional de la Agencia Nacional de Seguridad Digital (ANSD) será el encargado de la toma de decisiones ante las amenazas que reciba el país en materia de ciberseguridad, así como de los procesos operacionales que se realicen para combatir los ataques cibernéticos.**	
Artículo 11. Fondo Nacional para la Seguridad Digital y Ciberdefensa. Créase el Fondo Nacional para la Seguridad Digital y Ciberdefensa como una cuenta especial de la Nación, sin personería jurídica, ni estructura administrativa, con independencia patrimonial, administrativa, contable y estadística para financiar el funcionamiento de la Agencia Nacional de Seguridad Digital (ANSD) El Fondo Nacional para la Seguridad Digital y Ciberdefensa se integrará de los recursos correspondientes al ColCert (Grupo de Respuesta a Emergencias Cibernéticas de Colombia; el 1% de los Fondos del FONTIC; donaciones del	**Artículo 11. Fondo Nacional para la Seguridad Digital y Ciberdefensa.** Créase el Fondo Nacional para la Seguridad Digital y Ciberdefensa como una cuenta especial de la Nación, sin personería jurídica, ni estructura administrativa, con independencia patrimonial, administrativa, contable y estadística para financiar el funcionamiento de la Agencia Nacional de Seguridad Digital (ANSD) El Fondo Nacional para la Seguridad Digital y Ciberdefensa se integrará de los recursos correspondientes al ColCert (Grupo de Respuesta a Emergencias Cibernéticas de Colombia, **al CSIRT Gobierno**; el 1% de los Fondos del FONTIC; **recursos de cooperación**	El CSIRT Gobierno será parte de la Agencia Nacional de Seguridad Digital, es por ello que sus recursos deben ser redistribuidos en la agencia para garantizar su presupuesto. Se asigna una distribución de las sanciones establecidas en el artículo 12. Los recursos producto de estas sanciones se destinarán al Fondo Nacional para la Seguridad Digital y Ciberdefensa, con el fin de garantizar su presupuesto y autonomía financiera.

sector privado, así como aportes voluntarios de los CSIRTS (Equipo de respuesta a incidentes de seguridad informática) del sector privado. De igual manera, el Fondo Nacional para la Seguridad Digital podrá recibir financiación extranjera bajo cooperación de países donantes. El Director General de la Agencia Nacional de Seguridad Digital (ANSD) será el ordenador del gasto de los recursos del Fondo Nacional para la Seguridad Digital y Ciberdefensa.	**internacional** ~~donaciones del sector privado~~; **el monto obtenido de las sanciones aplicables al sector privado mencionadas en el artículo 12 de la presente ley**, y ~~sí como~~ aportes voluntarios **en especie** de los CSIRTS (Equipo de respuesta a incidentes de seguridad informática) del sector privado. ~~De igual manera, el Fondo Nacional para la Seguridad Digital podrá recibir financiación extranjera bajo cooperación de países donantes.~~ El Director General de la Agencia Nacional de Seguridad Digital (ANSD) será el ordenador del gasto de los recursos del Fondo Nacional para la Seguridad Digital y Ciberdefensa.	
Artículo 12. Sanciones. Las entidades del Estado y las empresas del sector privado están en la obligatoriedad de informar a la Agencia Nacional de Seguridad Digital (ANSD) acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras. Así mismo, deberán informar en un plazo máximo de dos (2) días a la Agencia Nacional de Seguridad Digital (ANSD) cuando se perpetúen estos hechos, con el fin de que se realicen las investigaciones pertinentes y se informe a la opinión pública. **Parágrafo 1.** En caso de que las empresas del sector privado no informen de los riegos o delitos en el tiempo establecido en este artículo, se les podrá imponer las siguientes sanciones, previo desarrollo de proceso administrativo sancionatorio: 1. Multa de hasta mil (1.000) salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial. 2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años. 3. Publicación en medios de amplia circulación, con la periodicidad que la autoridad indique, del extracto de la decisión sancionatoria. Así mismo se hará la difusión en la página web del sancionado durante seis (6) meses hasta un tiempo máximo de un (1) año. El sancionado asumirá los costos de dichas publicaciones. 4. Prohibición de recibir cualquier tipo de incentivo o subsidios del Gobierno, en un plazo de cinco (05) años. **Parágrafo 2.** El Representante Legal de la entidad del Estado que no informe de los riegos o delitos en el tiempo establecido en este artículo, será objeto de una o varias de los siguientes sanciones disciplinarias, previo desarrollo de proceso disciplinario sancionatorio: 1. Destitución o inhabilidad general. 2. Suspensión en el ejercicio del cargo. 3. Amonestación escrita que debe registrarse en la hoja de vida.	**Artículo 12. Sanciones.** Las entidades del Estado y las empresas del sector 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**, están en la obligatoriedad de informar a la Agencia Nacional de Seguridad Digital (ANSD) 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.** Así mismo, deberán informar en un plazo máximo de ~~dos (2) días~~ **setenta y dos (72) horas** a la Agencia Nacional de Seguridad Digital (ANSD) cuando se perpetúen estos hechos, **contados desde que se tiene conocimiento de estos,** con el fin de que se ~~realicen las investigaciones~~ **pertinentes coordine la respuesta con los entes de investigación; se preste ayuda a la entidad o empresa atacada** 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 sensible, y/o sistemas de información.** **Parágrafo 1.** En caso de que las empresas del sector privado no informen de los riegos o delitos en el tiempo establecido en este artículo, se les podrá imponer las siguientes sanciones, previo desarrollo de proceso administrativo sancionatorio: 1. Multa de hasta mil (1.000) **500 salarios** mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial. 2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años. 3. Publicación en medios de amplia circulación, con la periodicidad que la autoridad indique, del extracto de la decisión sancionatoria. Así mismo se hará la difusión en la página web del sancionado durante seis (6) meses hasta un tiempo máximo de un (1) año. El sancionado asumirá los costos de dichas publicaciones. 4. Prohibición de recibir cualquier tipo de incentivo o subsidios del gobierno, en un plazo periodo de cinco (05) años contados desde la ejecutoria de la sanción. **Parágrafo 2.** El Representante Legal de la entidad del Estado que no informe de los riegos o delitos en el tiempo establecido en este artículo, será objeto de una o varias de los siguientes sanciones disciplinarias, previo desarrollo de proceso disciplinario sancionatorio: 1. Destitución o inhabilidad general. 2. Suspensión en el ejercicio del cargo. 3. Amonestación escrita que debe registrarse en la hoja de vida. **Parágrafo 3: La obligatoriedad de informar a la Agencia Nacional de Seguridad Digital (ANSD) acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados, se realizará con estricto cumplimiento del derecho a la protección de datos personales y demás disposiciones del artículo 7 de la presente ley.** **La Superintendencia de Industria y Comercio vigilará el cumplimiento del derecho a la**	Se establece un tiempo de 72 horas para informar a la Agencia Nacional de Seguridad Digital sobre los ataques o intentos de ciberataques recibidos, pues es el plazo en el cual se pueden tomar acciones de reacción y ayuda a las entidades o empresas afectadas. Así mismo, se contempla que la Agencia Nacional de Seguridad Digital tendrá la función de coordinar la respuesta de los entes de investigación. Se establece que únicamente las personas jurídicas domiciliadas en el país están en la obligación de informar a la Agencia Nacional de Seguridad Digital acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras. Esto a fin de dar cumplimiento al principio de aplicación territorial de la ley incorporado en el artículo cuarto de la Constitución Política. Así mismo, su ámbito de aplicación se reduce para evitar que micro, pequeñas y medianas empresas sean sancionadas y cuenten con cargas desproporcionadas en cuanto a seguridad digital, pues no suministran información sensible, de infraestructuras críticas, datos sensibles o sistemas de información sensible. Parágrafo 1. Se hace modificación de la cuantía de la sanción. Parágrafo 3. Se establece que el tratamiento de datos personales deberá realizarse con estricto cumplimiento del derecho a la protección de los datos personales y bajo la vigilancia de la Superintendencia de Industria y Comercio.

	protección de datos personales.	
Artículo 13. Consejo Público - Privado contra los ciberataques y Delitos Cibernéticos. El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos será un órgano consejero de participación público y privada. Tiene como función realizar recomendaciones a la Agencia Nacional de Seguridad Digital (ANSD) con el fin de combatir los riesgos observados en materia de Seguridad Digital y mantener una constante actualización de los ataques observados a nivel mundial, así como la manera de combatirlos garantizando el uso de tecnologías modernas y vanguardistas. Estará integrado por: 1. El Director General del Comando Conjunto Cibernético (CCOCI) o su delegado. 2. El Director General del Centro Cibernético Policial (CCP) o su delegado. 3. El Viceministro de Transformación Digital del Ministerio de Tecnologías de la Información y las Comunicaciones o su delegado. 4. El Viceministro de Conocimiento, Innovación y Productividad del Ministerio de Ciencia, Tecnología e Innovación o su delegado. 5. El Director Nacional Especializado contra los Delitos Informáticos de la Fiscalía General de la Nación o su delegado. 6. Representantes de cinco (5) gremios tecnológicos que expresen su interés de participar en el Consejo. **Parágrafo 1.** El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos tendrá la potestad de convocar expertos o agencias internacionales a participar en sus sesiones cuando la técnica o estrategia a desarrollar requiera de la cooperación internacional. **Parágrafo 2.** El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos se reunirá por lo menos una vez al mes o cuando sea convocado ante eventuales riesgos en la materia.	**Artículo 13. Consejo Público - Privado <u>de estrategia</u> contra los ciberataques y Delitos Cibernéticos.** El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos será un órgano consejero de participación público - ~~y~~ privada. Tiene como función realizar recomendaciones a la Agencia Nacional de Seguridad Digital (ANSD) con el fin de combatir los riesgos observados en materia de seguridad digital y mantener una constante actualización de los ataques observados a nivel mundial, así como la manera de combatirlos garantizando el uso de tecnologías modernas y vanguardistas. <u>**De igual manera, será el encargado de la planeación de estrategias a largo plazo para potenciar el desarrollo de la industria de ciberseguridad en Colombia, así como de promover la educación de profesionales en el área.**</u> Estará integrado por: 1. El Director General del Comando Conjunto Cibernético (CCOCI) o su delegado. 2. El Director General del Centro Cibernético Policial (CCP) o su delegado. 3. El Viceministro de Transformación Digital del Ministerio de Tecnologías de la Información y las Comunicaciones o su delegado. 4. El Viceministro de Conocimiento, Innovación y Productividad del Ministerio de Ciencia, Tecnología e Innovación o su delegado. 5. El Director Nacional Especializado contra los Delitos Informáticos de la Fiscalía General de la Nación o su delegado. 6. Representantes de cinco (5) gremios tecnológicos que expresen su interés de participar en el Consejo. 7. **<u>El Viceministro de Educación Superior del Ministerio de Ciencia, Tecnología e Innovación o su delegado.</u>** **Parágrafo 1.** El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos tendrá la potestad de convocar expertos o agencias internacionales a participar en sus sesiones cuando la técnica o estrategia a desarrollar requiera de la cooperación internacional. **Parágrafo 2.** El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos se reunirá por lo menos una vez al mes o cuando sea	Se le asigna un rol estratégico y a largo plazo al Consejo Público y Privado.
Artículo 14. Observatorio Nacional de Seguridad Digital y Ciberdefensa. El Observatorio Nacional de Seguridad Digital y Ciberdefensa hará parte de la Agencia Nacional de Seguridad Digital (ANSD) y tendrá como función principal ser el órgano de investigación de la Agencia, monitoreando ataques, tanto a nivel nacional como internacional, esto con el fin de que la opinión pública tenga conocimiento de las cifras reales en cuánto a delitos informáticos y ciberataques dados dentro del territorio nacional. **Parágrafo 1.** La Agencia Nacional de Seguridad Digital (ANSD) definirá la conformación del Observatorio Nacional de Seguridad Digital y Ciberdefensa en el Plan Nacional de Seguridad Digital y Ciberdefensa.	**Artículo 14. Observatorio Nacional de Seguridad Digital y Ciberdefensa.** El Observatorio Nacional de Seguridad Digital y Ciberdefensa hará parte de la Agencia Nacional de Seguridad Digital (ANSD) y tendrá como función principal ser el órgano de **<u>recolección de información</u>** **~~investigación~~** ~~—~~de la Agencia~~—~~, monitoreando ataques, tanto a nivel nacional como internacional. **<u>El observatorio trabajará en coordinación con los entes de investigación de delitos cibernéticos y ciberataques,</u>** ~~esto~~ con el fin de que la opinión pública tenga conocimiento **<u>sobre</u>** ~~de~~ las cifras ~~reales en cuánto a~~ **<u>de</u>** delitos informáticos y ciberataques ~~dados dentro~~ **<u>que se ejecuten en el</u>** ~~del~~ territorio nacional.	El Observatorio Nacional de Seguridad Digital y Ciberdefensa no tendrá funciones de investigación, sino de recolección de información en coordinación con los entes encargados de la investigación.
Artículo 15. Vigencia y derogaciones. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias.	Sin modificaciones	

6. PROPOSICIÓN:

Con fundamento en las anteriores consideraciones, de manera respetuosa solicito a la Comisión Primera del Senado de la República, dar primer debate y aprobar el proyecto de Ley No. 331/2023 Senado "**Por medio del cual se crea la Agencia Nacional de Seguridad Digital y se crean otras disposiciones**", conforme al texto que se anexa.

Cordialmente,

DAVID LUNA SÁNCHEZ
Senador de la República

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

PROYECTO DE LEY No. 331 DE 2023

"Por medio de la cual se crea la Agencia Nacional de Seguridad Digital y se dictan otras disposiciones"

El Congreso de Colombia,

DECRETA:

Artículo 1. Objeto. La presente Ley tiene por objeto la creación de la Agencia Nacional de Seguridad Digital, establecer sus funciones y dictar otras disposiciones.

Artículo 2. Definiciones. Para la aplicación de la presente ley se tendrán en cuenta las siguientes definiciones:

Seguridad Digital. Situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (1) la gestión del riesgo de seguridad digital; (2) la implementación efectiva de medidas de ciberseguridad y (3) el uso efectivo de las capacidad de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Ciberdefensa. Capacidad del Estado para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la soberanía nacional.

Ciberseguridad. Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

Ciberespacio. Ambiente formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos, usando redes computacionales.

Ciberataque. Acciones maliciosas con la intención de causar daño, interrupciones o conseguir acceso no autorizado a sistemas informáticos, redes o dispositivos mediante el uso de medios cibernéticos.

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.

Delitos ciber habilitados: Aquellos que existían de forma previa a las TIC's, pero que, con el desarrollo de éstas, ahora se desarrollan también mediante la modalidad cibernética.

Infraestructuras Críticas. Sistemas, redes, instalaciones y servicios que son considerados esenciales para el funcionamiento y la seguridad de la Nación, tales como energía, transporte, comunicaciones, finanzas, salud y seguridad pública.

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.

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.

Comando Conjunto Cibernético (CCOCI). Es el equipo encargado de la defensa del país en el ciberespacio y garante de la protección de las infraestructuras críticas cibernéticas nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional.

Centro Cibernético Policial (CCP). Es el equipo encargado de la seguridad ciudadana en el ciberespacio. Es una unidad de la Policía Nacional de Colombia encargada de la investigación y la lucha contra delitos cibernéticos que afecten a la ciudadanía dentro del ciberespacio. Brinda capacitación y educación en materia de seguridad informática a otros miembros de polícia y al público en general.

Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT. Es el organismo coordinador a nivel nacional en temas de ciberseguridad adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones e integrado por funcionarios civiles, personal militar y en comisión de otras entidades. Su misión es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que lo atenten o comprometan.

Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). Organización que tiene como misión responder de forma urgente y coordinada ante ataques cibernéticos.

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

Artículo 3. Creación de la Agencia Nacional de Seguridad Digital. Créase la Unidad Administrativa Especial denominada Agencia Nacional de Seguridad Digital y (ANSD), entidad descentralizada, del orden nacional, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones, que forma parte de la Rama Ejecutiva, con personería jurídica, autonomía administrativa, financiera y patrimonio propio.

Artículo 4. Autoridad. La Agencia Nacional de Seguridad Digital (ANSD) es la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de seguridad digital y ciberdefensa nacional.

Artículo 5. Funciones: La Agencia Nacional para la Seguridad Digital (ANSD) ejercerá las siguientes funciones:

1. **Coordinación y colaboración:**

1.1 Trabajar en colaboración con las entidades del Estado, así como con el sector privado y los ciudadanos para coordinar las acciones para mitigar los efectos de ciberataques.

1.2 Coordinar y gestionar 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 y delitos cibernéticos perpetrados en el territorio nacional.

1.3 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.

1.4 Promover la colaboración y cooperación entre entidades del Estado, el sector privado y los ciudadanos para recibir de manera oportuna cualquier información que salvaguarde la Seguridad Digital de la Nación.

1.5 Articular y apoyar las acciones que realicen las entidades del Estado para garantizar la Seguridad Digital y la Ciberdefensa del Estado.

1.6 Ejercer la vocería e informar los protocolos y medidas de seguridad implementadas en caso de ciberataques. Para ello, se delegará a funcionarios de la agencia o de alguna de las instancias nacionales públicas.

1.7 Articular y apoyar las acciones que realicen las entidades del Estado para garantizar la Seguridad Digital y la Ciberdefensa del Estado.

2. **Evaluación y mitigación de riesgos:**

2.1 Gestionar los planes y controles de mitigación del riesgo de Seguridad Digital del Estado, y apoyar a las entidades del Estado en la elaboración de evaluaciones de riesgo de seguridad digital con el fin de identificar y controlar riesgos identificados en materia de delitos cibernéticos.

2.2 Proporcionar orientación sobre la implementación de medidas de seguridad adecuadas en el ciberespacio y promover el cumplimiento de prácticas de ciberseguridad, basado en los estándares y mejores prácticas internacionales reconocidos por la industria.

2.3 Realizar análisis de amenazas cibernéticas y colaborar con entidades del Estado, sector privado y ciudadanos en el entendimiento de las tácticas, técnicas y procedimientos de los delincuentes, ante eventuales ciberataques.

2.4 Ofrecer asesoramiento y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en Seguridad Digital y Ciberdefensa.

3. Educación y prevención:

3.1 Ofrecer en coordinación con el Ministerio de Educación Nacional programas de educación y concientización dirigidos a entidades del Estado, al sector privado y a los ciudadanos sobre la detección de amenazas cibernéticas y cómo———proceder en caso de ellas.

3.2 Trabajar de manera conjunta con las comunidades educativas y de investigación en temas relacionados con la seguridad digital y la ciberdefensa de la Nación, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar el riesgo ante ataques cibernéticos.

3.3 Colaborar con los particulares, las instituciones académicas y los centros de investigación de orden tanto nacional, como internacional, con el fin de promover la innovación y el avance de tecnologías y soluciones de seguridad digital y ciberdefensa.

3.4 Colaborar con las entidades responsables en la investigación de los hechos, las causas y circunstancias de ciberataques y delitos cibernéticos que se perpetren en el territorio nacional. Así mismo, proporcionará acompañamiento en el proceso de investigación a entidades públicas y empresas privadas.

3.5 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.

3.6 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.

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

4. Planificación:

4.1 Acorde con las recomendaciones y estándares internacionales, diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa de la Nación, el cual contendrá los estándares en materia de seguridad digital que las entidades públicas y el sector privado deben adoptar.

4.2 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 Internacionales, el Ministerio de Defensa Nacional, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Tecnologías de la Información, el Ministerio de Educación Nacional, la Fiscalía General de la Nación y la Dirección Nacional de Inteligencia

4.3 Reunir, procesar, interpretar y analizar la información suministrada por las entidades del Estado, el sector privado y los ciudadanos, con el fin de identificar los responsables de ciberataques y delitos cibernéticos perpetrados en Colombia.

5. De ejecución:

5.1. Implementar una estrategia de apoyo y asistencia técnica gradual al sector público para la debida aplicación de los estándares y directrices en materia de seguridad digital. Para ello, la agencia promoverá la colaboración público-privada con empresas especializadas que le permita generar las capacidades técnicas necesarias para ello.

5.2 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, los sectores de salud; energía; transporte y servicios públicos.

Artículo 6. Régimen jurídico. Los actos unilaterales que expida la Agencia Nacional de Seguridad Digital y Ciberdefensa (ANSD) son actos administrativos y se sujetan a las disposiciones del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Artículo 7. Protección de datos. El funcionamiento de la Agencia y demás órganos asociados creados mediante esta ley, se desarrollará en estricto cumplimiento del derecho a la protección de los datos personales, de conformidad con la Constitución y la Ley Estatutaria 1581 de 2012, o aquella que la modifique, reemplace o derogue.

Parágrafo 1. La Superintendencia de Industria y Comercio vigilará el respeto del derecho a la protección de datos por parte de la ANSD.

Artículo 8. Estructura. La Agencia Nacional de Seguridad Digital (ANSD) tendrá la siguiente estructura:

1. Consejo Directivo - Operacional
2. Dirección General.
3. Secretaría General.
4. Dirección de Investigación.
5. Dirección de Capacitación.
6. Dirección de Planificación.
7. Dirección del Observatorio Nacional de Seguridad Digital y Ciberdefensa.
8. Consejo Público - Privado de estrategia contra los ciberataques y delitos cibernéticos.
9. Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT
10. Equipo de Respuestas a Incidentes de Seguridad CSIRT gobierno.

Parágrafo 1. Los Directores de Investigación, Capacitación y Planificación de la Agencia Nacional de Seguridad Digital (ANSD) serán de libre nombramiento y remoción por mandato del Director General de la Agencia Nacional de Seguridad Digital (ANSD). Sin embargo, los requisitos técnicos y profesionales y de experiencia para su nombramiento y posesión deberán establecerse vía decreto reglamentario, que será expedido a más tardar dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente Ley.

Parágrafo 2. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) y el CSIRT Gobierno, adscritas hoy al Ministerio de Tecnologías de Información y Comunicaciones, pasarán a estar adscritas a la Agencia Nacional de Seguridad Digital.

Artículo 9. Órganos de Dirección y Administración. La Dirección y la administración de recursos de la Agencia Nacional de Seguridad Digital (ANSD) estará a cargo del Consejo Directivo - Operacional y el Director General.

El Director General actuará como Representante Legal y será un funcionario de libre nombramiento y remoción por parte del Presidente de la República.

Artículo 10. Integración del Consejo Directivo - Operacional El Consejo Directivo **Operacional** de la Agencia Nacional de Seguridad Digital (ANSD) estará integrado por los siguientes miembros:

1. El Ministro de Defensa o su delegado.
2. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado.
3. El Superintendente de Industria y Comercio o su delegado.
4. El Director de la Policía Nacional o su delegado.
5. El Fiscal General de la Nación o su delegado.
6. El Director General de la Dirección Nacional de Inteligencia (DNI) o su delegado.
7. El Comandante de las Fuerzas Militares o su delegado.
8. Los representantes de los CSIRT, tanto públicos como privados que sean citados o necesarios para la atención de la amenaza detectada.

Parágrafo 1. El Consejo Directivo de la Agencia Nacional de Seguridad Digital (ANSD) se reunirá por lo menos una vez al mes o cuando sea convocado ante eventuales riesgos en la materia.

Parágrafo 2. El Consejo Directivo - Operacional de la Agencia Nacional de Seguridad Digital (ANSD) será el encargado de la toma de decisiones ante las amenazas que reciba el país en materia de ciberseguridad, así como de los procesos operacionales que se realicen para combatir los ataques cibernéticos.

Artículo 11. Fondo Nacional para la Seguridad Digital y Ciberdefensa. Créase el Fondo Nacional para la Seguridad Digital y Ciberdefensa como una cuenta especial de la Nación, sin personería jurídica, ni estructura administrativa, con independencia patrimonial, administrativa, contable y estadística para financiar el funcionamiento de la Agencia Nacional de Seguridad Digital (ANSD).

El Fondo Nacional para la Seguridad Digital y Ciberdefensa se integrará de los recursos correspondientes al ColCert (Grupo de Respuesta a Emergencias Cibernéticas de Colombia, al CSIRT Gobierno; el 1% de los Fondos del FONTIC; recursos de cooperación internacional; el monto obtenido de las sanciones aplicables al sector privado mencionadas en el artículo 12 de la presente ley, y aportes voluntarios en especie de los CSIRTS (Equipo de respuesta a incidentes de seguridad informática) del sector privado.

El Director General de la Agencia Nacional de Seguridad Digital (ANSD) será el ordenador del gasto de los recursos del Fondo Nacional para la Seguridad Digital y Ciberdefensa.

Artículo 12. Sanciones. Las entidades del Estado y las empresas del sector 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, están en la obligatoriedad de informar a la Agencia Nacional de Seguridad Digital (ANSD) 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.

Así mismo, deberán informar en un plazo máximo de setenta y dos (72) horas a la Agencia Nacional de Seguridad Digital (ANSD) cuando se perpetúen estos hechos, contados desde que se tiene conocimiento de estos, con el fin de que se coordine la respuesta con los entes de investigación; se preste ayuda a la entidad o empresa atacada 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 sensible, y/o sistemas de información.

Parágrafo 1. En caso de que las empresas del sector privado no informen de los riegos o delitos en el tiempo establecido en este artículo, se les podrá imponer las siguientes sanciones, previo desarrollo de proceso administrativo sancionatorio:

- Multa de hasta quinientos 500 salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial.
- Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años.
- Publicación en medios de amplia circulación, con la periodicidad que la autoridad indique, del extracto de la decisión sancionatoria. Así mismo se hará la difusión en la página web del sancionado durante seis (6) meses hasta un tiempo máximo de un (1) año. El sancionado asumirá los costos de dichas publicaciones.
- Prohibición de recibir cualquier tipo de incentivo o subsidios del gobierno, en un periodo de cinco (05) años contados desde la ejecutoria de la sanción.

Parágrafo 2. El Representante Legal de la entidad del Estado que no informe de los riegos o delitos en el tiempo establecido en este artículo, será objeto de una o varias de los siguientes sanciones disciplinarias, previo desarrollo de proceso disciplinario sancionatorio:

- Destitución o inhabilidad general.
- Suspensión en el ejercicio del cargo.
- Amonestación escrita que debe registrarse en la hoja de vida.

Parágrafo 3: La obligatoriedad de informar a la Agencia Nacional de Seguridad Digital (ANSD) acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados, se realizará con estricto cumplimiento del derecho a la protección de datos personales y demás disposiciones del artículo 7 de la presente ley.

La Superintendencia de Industria y Comercio vigilará el cumplimiento del derecho a la protección de datos personales.

Artículo 13. Consejo Público - Privado de estrategia contra los ciberataques y Delitos Cibernéticos. El Consejo Público - Privado contra los Ciberataques y Delitos Cibernéticos será un órgano consejero de participación público - ~~y~~ privada.

Tiene como función realizar recomendaciones a la Agencia Nacional de Seguridad Digital (ANSD) con el fin de combatir los riesgos observados en materia de seguridad digital y mantener una constante actualización de los ataques observados a nivel mundial, así como la manera de combatirlos garantizando el uso de tecnologías modernas y vanguardistas.

De igual manera, será el encargado de la planeación de estrategias a largo plazo para potenciar el desarrollo de la industria de ciberseguridad en Colombia, así como de promover la educación de profesionales en el área.

Estará integrado por:

1. El Director General del Comando Conjunto Cibernético (CCOCI) o su delegado.
2. El Director General del Centro Cibernético Policial (CCP) o su delegado.
3. El Viceministro de Transformación Digital del Ministerio de Tecnologías de la Información y las Comunicaciones o su delegado.
4. El Viceministro de Conocimiento, Innovación y Productividad del Ministerio de Ciencia, Tecnología e Innovación o su delegado.
5. El Director Nacional Especializado contra los Delitos Informáticos de la Fiscalía General de la Nación o su delegado.
6. Representantes de cinco (5) gremios tecnológicos que expresen su interés de participar en el Consejo.
7. El Viceministro de Educación Superior del Ministerio de Educación Nacional.

Artículo 14. Observatorio Nacional de Seguridad Digital y Ciberdefensa. El Observatorio Nacional de Seguridad Digital y Ciberdefensa hará parte de la Agencia Nacional de Seguridad Digital (ANSD) y tendrá como función principal ser el órgano de recolección de información de la Agencia–, monitoreando ataques, tanto a nivel nacional como internacional.

Artículo 15. Vigencia y derogaciones. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias.

Cordialmente,

Cordialmente,

CONTENIDO

IMPRENTA NACIONAL DE COLOMBIA - 2023