



Bogotá, D. C., diciembre de 2020

Senador
MIGUEL ÁNGEL PINTO HERNÁNDEZ
Presidente de la Comisión Primera
Senado de la República
Ciudad

REF. Informe de ponencia para primer debate al Proyecto de Ley No. 339 de 2020 Senado “*Por medio de la cual se expiden lineamientos en torno a la seguridad digital, se modifica la Ley 599 de 2000, y se dictan otras disposiciones*”.

Respetado presidente Pinto:

Atendiendo la designación que la Mesa Directiva de la Comisión Primera Constitucional Permanente del Senado de la República nos hizo, de conformidad con lo dispuesto en la Constitución Política y en la Ley 5ª de 1992, me permito rendir Informe de Ponencia Positiva para Primer Debate en Senador al Proyecto de Ley de referencia.

Cordialmente


CARLOS EDUARDO GUEVARA VILLABÓN
Senador de La República



INFORME DE PONENCIA PARA EL PRIMER DEBATE AL PROYECTO DE LEY NO. 339 DE 2020 SENADO

“Por medio de la cual se expiden lineamientos en torno a la seguridad digital, se modifica la Ley 599 de 2000, y se dictan otras disposiciones”.

I. OBJETO DEL PROYECTO

La presente Ley tiene por objeto clasificar y tipificar como delitos cibernéticos nuevas acciones criminales ejecutadas en el ciberespacio, así como establecer acciones estatales para prevenirlos.

II. CONTENIDO

La iniciativa contra los ciberdelitos contempla nuevas modalidades que se han venido presentando desde tiempo atrás, y otras que por la pandemia se han intensificado. Se propone la protección de los NNA que son víctimas de ciberdelitos de índole sexual, así como la protección al patrimonio que se ve afectado por ciber conductas. También se proponen medidas procesales para fortalecer la investigación y protección preventiva. Así como acciones articuladas entre todo el Estado para hacer frente a estas conductas.

Se busca garantizar progresivamente una cobertura integral de Internet a toda la población colombiana. En este sentido, es claro que, aunque el Gobierno Nacional ha tomado acciones positivas e iniciativas claras destinadas al mismo logro, hoy en día más de la mitad de la población colombiana no cuenta con acceso a este servicio y se refuerzan los derechos digitales que tienen los niños, niñas y adolescentes.

Sobre los delitos creados, se crea el delito de Sexting: consiste en realizar alguna de estas conductas (1) Publicar, divulgar o revelar, imágenes o grabaciones audiovisuales de la actividad sexual o con contenido sexual de una persona, sin su autorización, en redes de información o comunicación. (2) Ofrecer o entregar a un tercero las imágenes o las grabaciones audiovisuales de la actividad sexual o con contenido sexual de una persona, sin su consentimiento, a un tercero. Es un delito pluriofensivo porque protege la integridad e intimidad sexual de las personas y la autonomía de la persona de decidir cuándo y con quien revelar la intimidad, esta situación no está contemplada en el ordenamiento legal vigente y para castigarla hay que hacer un salto a muchos tipos penales; esta situación dificulta la persecución criminal.

Se crea un agravante en el delito de extorsión: para aquellos casos en los que la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación o sistema de información, imágenes o grabaciones audiovisuales de actividades sexuales o con contenido sexual, pretenda la obtención de un beneficio económico. Es decir, para aquellos casos en que las personas sean extorsionadas para evitar la divulgación de imágenes o grabaciones audiovisuales relacionadas con su intimidad sexual. Si bien la jurisprudencia ha optado en algunos casos por señalar que este tipo de conductas constituye una injuria por vía de hecho, en otros, un acto sexual, no obstante, el hecho que se haya optado por esas formas no convencionales para no desproteger a las personas, no implica que esa sea la solución jurídica correcta.

Se busca penalizar la conducta del Grooming: una nueva “forma de acoso y abuso hacia niños y jóvenes, inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente por una de la misma edad del niño con el objetivo de obtener una satisfacción sexual, mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual”¹. Se crea el tipo penal de ciberacoso, también denominado, ciberbullying, como aquella forma de acoso que se produce de forma sistemática.

Se crea una calificante en el hurto: para aquellos casos en los que el delincuente tiene acceso a información personal de la víctima y en uso de ella comete el delito. Es decir, contempla aquellas conductas en las que los delincuentes se unen a las plataformas o redes de comunicación, de forma dolosa, con el único objetivo de conseguir información de potenciales víctimas.

Se regula el hurto usando marcas reconocidas: quienes, en uso y desprestigio de las marcas, cometen hurtos en las viviendas. Es decir, personas que portan un uniforme o un signo distintivo con el fin de generar que su víctima baje la guardia, abra la puerta, o permita su ingreso al conjunto a fin de hurtarle. Esto es diferente del uso de disfraz (agravante hoy vigente), toda vez que el disfraz consiste en hacerse parecer algo que no se es. Situación totalmente distinta, a cuando efectivamente lo es. Es decir, una cosa es aparentar ser de cierta plataforma, y otra es efectivamente serlo.

Se busca agravar los delitos de estafa: cuando los mismos se produzcan de forma online fundamentado en la facilidad que la tecnología y el anonimato le dan al delincuente de cometer el delito, y la dificultad para el Estado de perseguir y criminalizar estas conductas.

Se busca incluir dentro del tipo penal de software malicioso el “uso”, toda vez, que este verbo rector no se encontraba hoy regulado, siendo vital en la cadena de producción y comisión del delito. Y además, se busca castigar el morphing (alteración de imágenes con fines sexuales) o también conocidas como *Deep Faking* (alteración de imágenes en general). Finalmente, se agravan las conductas de corrupción de alimentos, simulación o fabricación de productos nocivos para la salud cuando se cometen de forma online.

Sobre las medidas procesales se crea una medida cautelar que permite a la Fiscalía solicitar a un juez de control de garantías el bloqueo preventivo de una URL, cuando estime que por medio de esta se está cometiendo una conducta punible.

Frente a las clases virtuales se busca regular aquellas situaciones en las que terceros ingresan a las clases virtuales con el fin de sabotearlas, o que mediante virus y demás artimañas logran infectar el equipo de los docentes, con el objetivo de impedir u obstaculizar dichas clases.

Sobre el comité interinstitucional: se propone la creación de un Comité Interinstitucional, que permita un trabajo articulado entre todos los organismos estatales involucrados para una mejor respuesta y formulación de lineamientos y estrategias, con miras a prevenir y reducir estos delitos. Tendría como objetivo la lucha específica contra los ciberdelitos teniendo en cuenta que son modalidades delictuales que se reinventan a diario.

¹ <https://www.mintic.gov.co/portal/inicio/5626:Grooming>

III. ASPECTOS GENERALES

La necesidad de regular y fortalecer los instrumentos en la lucha contra la cibercriminalidad nunca había sido tan clara, a nivel mundial, Interpol realizó un examen en el dos mil dieciocho (2018) encontrando las siguientes conclusiones:

- “Cuanto más joven era la víctima, más grave era el abuso;
- El ochenta y cuatro por ciento (84 %) de las imágenes contenía actividad sexual explícita
- Más del sesenta por ciento (60%) de las víctimas no identificadas eran pre pubescentes, inclusive bebés y niños pequeños”^[1].

Como si esto no fuera suficiente, desde la Sociedad para la Prevención de la Crueldad de los Niños se anuncia que con la llegada del Coronavirus se han incrementado exponencialmente los casos de “online child abuse”, igualmente, estiman que tan solo en el Reino Unido hay más de veinticinco mil trescientos (25,300) niños víctimas de ciberdelitos y que noventa (90) niños son víctimas cada día^[2]. Además, el FBI en E.E.U.U. ha encontrado un incremento alarmante en la comisión de estos delitos en un sesenta por ciento (60%) con una agravante, cada sujeto capturado realiza sus actos criminales con hasta trescientos (300) niños^[3].

Por otro lado, en países como España: se tiene que para el año dos mil dieciocho (2018) “las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de ocho millones cuatrocientos sesenta mil setecientos quince 8.460.715, es decir, un treinta y cinco coma cinco por ciento (35,5%) más que en el año dos mil diecisiete (2017)”, y hoy “Las Fuerzas de Seguridad detectaron doscientos dieciocho mil trescientos dos (218.302) ciberdelitos en dos mil diecinueve (2019)”^[4]. En Estados Unidos también se reportan cifras alarmantes, el Centro de Quejas por Delitos en Internet (IC3) recibió cuatrocientos sesenta y siete mil trescientos sesenta y un (467,361) quejas , en dos mil diecinueve (2019), un promedio de casi mil trescientas (1,300) por día, y registró más de tres punto cinco (\$ 3.5) mil millones en pérdidas para víctimas individuales y comerciales.^[5] En vista de esto, la UNCIRTRI (por sus siglas en inglés que significan: United Nations Interregional Crime and Justice Research Institute) señala que: “Las técnicas comunes de cibercrimen, como el phishing, han experimentado un aumento. (...) Según el informe, en enero, Google registró ciento cuarenta y nueve mil (149k) sitios web activos de phishing. En febrero, ese número casi se duplicó a doscientos noventa y tres mil (293k). Sin embargo, en marzo, ese número aumentó a quinientos veintidós mil (522k), un aumento del trescientos cincuenta por ciento (350%) desde enero.”^[6] (traducción propia), Informe que se representa en la siguiente tabla:



Como se establece en la imagen, en enero se detectaron ciento cuarenta y nueve mil ciento noventa y cinco (149.195) sitios dedicados al Phishing. En febrero se detectaron doscientos noventa y tres mil doscientos treinta y cinco (293.235), y en marzo se detectaron quinientos veintidós mil cuatrocientos noventa y cinco (522.495). Señala la UNCITRI que “Países de todo el mundo informan un aumento en el cibercrimen durante la pandemia. La INTERPOL a su vez, advierte que “Los delincuentes prolíficos y oportunistas se están aprovechando de la pandemia de coronavirus COVID-19 para lanzar una variedad de ataques cibernéticos”^[7]. Dentro de estos cibercrímenes la EUROPOL ha señalado que los crímenes de naturaleza sexual, se han encontrado nuevas formas de comisión de delitos contra menores: La transmisión de abuso en vivo a pedido”^[8].

Finalmente, señala la EUROPOL que “El creciente número de niños y adolescentes que poseen teléfonos inteligentes ha sido acompañado por la producción de material indecente autogenerado. Tal material, inicialmente compartido con intenciones inocentes, a menudo llega a los "recolectores", quienes a menudo proceden a explotar a la víctima, en particular mediante extorsión”^[9]

Ahora bien, en Colombia la Policía Nacional señala que entre el dos mil dieciséis (2016) y dos mil diecinueve (2019), se reportaron en el CAI virtual siete mil cuatrocientas trece (7.413) conductas de tipo sexual cometidas a través de la red en contra de niños, niñas y adolescentes. Tan solo en dos mil diecinueve (2019) se cometieron mil cuarenta y tres (1.043) conductas, siendo las conductas no tipificadas las cometidas en mayor medida. No obstante, no solamente preocupan las cifras de delitos sexuales cometidos a través de las redes, también la Cámara Colombiana de Informática y Telecomunicaciones ha encontrado un incremento del cincuenta y cuatro por ciento (54%) entre dos mil dieciocho (2018) y dos mil diecinueve (2019) de la comisión de ciberdelitos.^[10] que se pueden observar en el siguiente gráfico:



Como se evidencia en la imagen, en dos mil quince (2015) las denuncias equivalen a siete mil quinientos veintitrés (7.523), en dos mil dieciséis (2016) a once mil doscientos veinticinco (11.225), en dos mil diecisiete (2017) a quince mil ochocientos cuarenta (15.840), en dos mil dieciocho (2018) a veintidós mil quinientos veinticuatro (22.524), y en dos mil diecinueve (2019) a diecisiete mil quinientos treinta y uno (17.531).

Con un aproximado de sesenta (60) denuncias diarias a nivel nacional, Bogotá encabeza el primer puesto como la ciudad con más cibercrimitos denunciados, con un total de cinco mil trescientos ocho casos (5.308) casos en dos mil diecinueve (2019). Lo que permite identificar también un incremento del seiscientos doce por ciento (612%) en conductas de Malware.

Por último, este informe de la Cámara Colombiana de Informática y Telecomunicaciones encuentra como tendencias del delito lo siguiente: Inteligencia Artificial y Malware; Uso de perfiles falsos en redes sociales para difusión de Malware; BEC basado en *Deepfake*^[11]; Uso de Botnet para difusión de correos extorsivos; Uso de mercados ilegales en DarkNet. Lo que también ha producido que a corte de noviembre de dos mil veinte (2020), según el INPEC hay actualmente doscientos treinta y dos (232) casos de pornografía con menores en las cárceles.

Según la más reciente estadística del Guala de la Policía, el delito de sexting ha tenido un incremento de más de ciento treinta por ciento (130%) en Colombia, durante lo corrido de la cuarentena por coronavirus. Y en el país, los ataques por malware durante lo corrido del año crecieron un seiscientos doce por ciento (612%), el monto pagado por rescate de información está entre los treinta y dos (32) millones y los ciento sesenta (160) millones de pesos. Frente a este escenario, Colombia se encuentra entre los países que recibió el mayor número de ataques por ransomware en Latinoamérica con un total de doscientos cincuenta y dos (252) lo que corresponde al treinta por ciento (30%) después de Brasil y Argentina. Frente a esto RANSOMWARE Colombia recibió el treinta por ciento (30%) de los ataques de Ransomware en Latinoamérica en el último año, seguido de Perú dieciséis por ciento (16%), México catorce por ciento (14%), Brasil once por ciento (11%) y Argentina nueve por ciento (9%).

IV. MARCO JURÍDICO

Frente a la materia, es válido resaltar que el legislador cuenta con un amplio margen de libertad en la configuración normativa de la política criminal y de los procedimientos aplicables, que le permite



adoptar medidas razonables para garantizar otros fines constitucionales. Las medidas penales y de procedimiento adoptadas para hacer frente a la *ciberdelincuencia* cumplen con estos requisitos constitucionales.

Ahora bien, dentro del marco normativo colombiano se encuentran el sustento constitucional y legal de la presente iniciativa, que otorga una sobresaliente protección a los derechos de las niñas, niños y adolescentes. A nivel constitucional la Carta Política de 1991 dispone los siguientes:

Artículo 1º. *Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general.*

Artículo 2º. Son fines esenciales del Estado. *Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.*

Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.

Artículo 44. Son derechos fundamentales de los niños: *la vida, la integridad física, la salud y la seguridad social, la alimentación equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado y amor, la educación y la cultura, la recreación y la libre expresión de su opinión. Serán protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos.*

Gozarán también de los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia. La familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral, y el ejercicio pleno de sus derechos. Cualquier persona puede exigir de la autoridad competente su cumplimiento y la sanción de los infractores. Los derechos de los niños prevalecen sobre los derechos de los demás.

Artículo 45. El adolescente tiene derecho a la protección y a la formación integral. *El Estado y la sociedad garantizan la participación activa de los jóvenes en los organismos públicos y privados que tengan a cargo la protección, educación y progreso de la juventud.*

A nivel legal se identifican varias leyes que se dirigen específicamente a la prevención de delitos sexuales contra niñas, niños y adolescentes, en las que se encuentran:

Ley 679 de 2001 Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución:

Artículo 4º. Comisión de Expertos. *Dentro del mes siguiente a la vigencia de la presente ley, el Instituto Colombiano de Bienestar Familiar conformará una Comisión integrada por peritos jurídicos y técnicos, y expertos en redes globales de información y telecomunicaciones, con el propósito de elaborar un catálogo de actos abusivos en el uso y aprovechamiento de tales redes, en lo relacionado con menores de edad. La*



Comisión propondrá iniciativas técnicas como sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos perjudiciales para menores de edad en las redes globales, que serán transmitidas al Gobierno Nacional con el propósito de dictar medidas en desarrollo de esta ley.

Artículo 12. Medidas de sensibilización. Las autoridades de los distintos niveles territoriales y el Instituto Colombiano de Bienestar Familiar, implementarán acciones de sensibilización pública sobre el problema de la prostitución, la pornografía y el abuso sexual de menores de edad. El Gobierno nacional, por intermedio del Ministerio de Educación, supervisará las medidas que a este respecto sean dictadas por las autoridades departamentales, distritales y municipales.

Parágrafo 1º. Por medidas de sensibilización pública se entiende todo programa, campaña o plan tendiente a informar por cualquier medio sobre el problema de la prostitución, la pornografía con menores de edad y el abuso sexual de menores de edad; sobre sus causas y efectos físicos y psicológicos y sobre la responsabilidad del Estado y de la sociedad en su prevención.

Artículo 15. Sistema de información sobre delitos sexuales contra menores. Para la prevención de los delitos sexuales contra menores de edad y el necesario control sobre quienes los cometen, promuevan o facilitan, el Ministerio de Justicia y del Derecho, el Departamento Administrativo de Seguridad, DAS, el Instituto Colombiano de Bienestar Familiar y la Fiscalía General de la Nación desarrollarán un sistema de información en el cual se disponga de una completa base de datos sobre delitos contra la libertad, el pudor y la formación sexual cometidos sobre menores de edad, sus autores, cómplices, proxenetas, tanto de condenados como de sindicados.

Ley 1098 de 2006, por la cual se expide el Código de la Infancia y la Adolescencia

Artículo 18. Derecho a la integridad personal. Los niños, las niñas y los adolescentes tienen derecho a ser protegidos contra todas las acciones o conductas que causen muerte, daño o sufrimiento físico, sexual o psicológico. En especial, tienen derecho a la protección contra el maltrato y los abusos de toda índole por parte de sus padres, de sus representantes legales, de las personas responsables de su cuidado y de los miembros de su grupo familiar, escolar y comunitario.

Ley 1336 de 2009, por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

Artículo 24. El artículo 218 de la Ley 599 quedará así:

Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, transmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro. La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

Asimismo, el país cuenta con normatividad para proteger a las niñas, niños y adolescentes del ciberacoso o cyberbullying y otros tipos de violencia escolar, ejemplo de ello es la Ley 1620 de 2013 “por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar”, que dispone:

Artículo 2º. En el marco de la presente ley se entiende por:

Competencias ciudadanas: Es una de las competencias básicas que se define como el conjunto de conocimientos y de habilidades cognitivas, emocionales y comunicativas que, articulados entre sí, hacen posible que el ciudadano actúe de manera constructiva en una sociedad democrática.



Educación para el ejercicio de los derechos humanos, sexuales y reproductivos: Es aquella orientada a formar personas capaces de reconocerse como sujetos activos titulares de derechos humanos, sexuales y reproductivos con la cual desarrollarán competencias para relacionarse consigo mismo y con los demás, con criterios de respeto por sí mismo, por el otro y por el entorno, con el fin de poder alcanzar un estado de bienestar físico, mental y social que les posibilite tomar decisiones asertivas, informadas y autónomas para ejercer una sexualidad libre, satisfactoria, responsable y sana en torno a la construcción de su proyecto de vida y a la transformación de las dinámicas sociales, hacia el establecimiento de relaciones más justas, democráticas y responsables.

Acoso escolar o bullying: *Conducta negativa, intencional metódica y sistemática de agresión, intimidación, humillación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra un niño, niña, o adolescente, por parte de un estudiante o varios de sus pares con quienes mantiene una relación de poder asimétrica, que se presenta de forma reiterada o a lo largo de un tiempo determinado.*

También puede ocurrir por parte de docentes contra estudiantes, o por parte de estudiantes contra docentes, ante la indiferencia o complicidad de su entorno. El acoso escolar tiene consecuencias sobre la salud, el bienestar emocional y el rendimiento escolar de los estudiantes y sobre el ambiente de aprendizaje y el clima escolar del establecimiento educativo.

Cyberbullying o ciberacoso escolar: *Forma de intimidación con uso deliberado de tecnologías de información (internet, redes sociales virtuales, telefonía móvil y videojuegos online), para ejercer maltrato psicológico y continuado.*

De otra parte, el marco legal colombiano otorga herramientas para proteger la información y los datos personales, aspecto que es protegido a través de la sanción penal, como se establece en los siguientes tipos penales:

Ley 1273 de 2009 “por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Artículo 269F: Violación de datos personales. *El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.*

Artículo 269G: Suplantación de sitios web para capturar datos personales. *El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.*

Además, se tiene la **Ley 1928 de 2018 por medio de la cual Colombia se adhirió al convenio sobre la ciberdelincuencia “convenio de Budapest”**. Finalmente, se tiene el CONPES 3995 que reguló la “Política Nacional De Confianza Y Seguridad Digital” el cual luego de un exhaustivo análisis sobre la situación actual de ciberseguridad en Colombia recomendó:



Solicitar a la **Presidencia de la República**: Establecer e implementar una ruta de acción que permita avanzar en el desarrollo de la normatividad en materia de seguridad digital. Formular el decreto reglamentario para la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permita la adecuada gestión de riesgos de seguridad digital y respuesta a incidentes del sector

Solicitar al **Ministerio de Educación Nacional** diseñar e implementar una estrategia que contemple acciones para la generación de hábitos de uso seguro y responsable de las TIC que posibilite generar en la trayectoria educativa completa el desarrollo de competencias y la formación en seguridad y confianza digital.

Solicitar al Ministerio de Justicia y del Derecho, realizar el diagnóstico y las consecuentes recomendaciones de solución de los posibles problemas existentes en el marco normativo vigente que puedan afectar: (i) el ejercicio libre y pacífico de la ciudadanía digital; (ii) la defensa y seguridad nacional y (iii) la persecución, investigación y sanción de la comisión de conductas punibles a través del uso de las Tecnologías de la Información y las Comunicaciones (TIC).

Solicitar al **Servicio Nacional de Aprendizaje (SENA)** diseñar programas de formación profesional con el enfoque de la formación para el trabajo y desarrollo humano, los cuales atenderán las necesidades sectoriales para fortalecer las competencias en áreas como la seguridad digital, seguridad de la información, ciberseguridad e infraestructuras críticas

V. EL PLIEGO DE MODIFICACIONES PROPUESTO

Texto Original	Ponencia propuesta para primer debate	Comentario
<p>Artículo 1. Objeto. La presente Ley tiene por objeto clasificar y tipificar nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos que afectan a los niños, niñas y adolescentes y a la población en general, y determinar aquellas acciones dirigidas a prevenir estos delitos.</p>	<p>Artículo 1. Objeto. La presente Ley tiene por objeto clasificar y tipificar nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos que afectan a los niños, niñas y adolescentes y a la población en general, y determinar aquellas acciones dirigidas a prevenir estos delitos.</p>	Sin modificaciones
<p>Artículo 2. Deberes del Estado. Con respecto a la digitalidad, son deberes del Estado, entre otros:</p> <p>1. Realizar capacitaciones y sensibilizar a todos los habitantes, con el fin de darles a conocer sus derechos y deberes digitales.</p>	<p>Artículo 2. Deberes del Estado. Con respecto a la digitalidad, son deberes del Estado, entre otros:</p> <p>1. Realizar capacitaciones y sensibilizar a todos los habitantes, con el fin de darles a conocer</p>	Sin modificaciones

<p>2. Generar políticas públicas de inclusión, a fin de lograr la mayor cobertura posible del servicio.</p> <p>3. Diseñar planes de estudio para que desde los colegios se logre la inserción de los estudiantes en el mundo digital. Particularmente, estos planes de estudio deberán preparar a los estudiantes para afrontar los retos en esta materia y prevenir los riesgos digitales.</p>	<p>sus derechos y deberes digitales.</p> <p>2. Generar políticas públicas de inclusión, a fin de lograr la mayor cobertura posible del servicio.</p> <p>3. Diseñar planes de estudio para que desde los colegios se logre la inserción de los estudiantes en el mundo digital. Particularmente, estos planes de estudio deberán preparar a los estudiantes para afrontar los retos en esta materia y prevenir los riesgos digitales.</p>	
<p>Artículo 3. Derechos digitales de los niños, niñas y adolescentes. Todos los niños, niñas y adolescentes tienen los siguientes derechos:</p> <p>1. A que el sistema educativo garantice su efectivo aprendizaje de los medios digitales, de forma segura y respetuosa con los derechos fundamentales.</p> <p>2. A acceder a actividades de prevención de los delitos cibernéticos, en los niveles de educación básica, media y superior.</p> <p>3. A conocer la problemática de los delitos cibernéticos que se produce, tanto dentro del territorio nacional como fuera de él, a través de medios de difusión masiva.</p>	<p>Artículo 3. Derechos digitales de los niños, niñas y adolescentes. Todos los niños, niñas y adolescentes tienen los siguientes derechos:</p> <p>9. A que el sistema educativo garantice su efectivo aprendizaje de los medios digitales, de forma segura y respetuosa con los derechos fundamentales.</p> <p>10. A acceder a actividades de prevención de los delitos cibernéticos, en los niveles de educación básica, media y superior.</p> <p>11. A conocer la problemática de los delitos cibernéticos que se produce, tanto dentro del territorio nacional como fuera de él, a través de medios de difusión masiva.</p>	Sin modificaciones

<p>4. A que sus profesores tengan las competencias digitales y la formación requerida para la enseñanza y transmisión de los valores y derechos.</p> <p>5. A una navegación segura en Internet que permita su libre desarrollo a la personalidad.</p> <p>6. A no ser constreñidos o incitados por terceros a realizar prácticas sexuales por Internet.</p> <p>7. A que sus datos personales sean tratados con máxima diligencia.</p> <p>8. Los demás que les asigne la ley.</p> <p>Parágrafo 1. El Ministerio de Educación expedirá la reglamentación para el cumplimiento de los derechos mencionados en el artículo 1, 2 y 3, dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.</p> <p>Parágrafo 2. El Ministerio del Trabajo reglamentará la forma en que se capacitará a los profesores conforme a lo reseñado en el numeral 4 dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.</p>	<p>12. A que sus profesores tengan las competencias digitales y la formación requerida para la enseñanza y transmisión de los valores y derechos.</p> <p>13. A una navegación segura en Internet que permita su libre desarrollo a la personalidad.</p> <p>14. A no ser constreñidos o incitados por terceros a realizar prácticas sexuales por Internet.</p> <p>15. A que sus datos personales sean tratados con máxima diligencia.</p> <p>16. Los demás que les asigne la ley.</p> <p>Parágrafo 1. El Ministerio de Educación expedirá la reglamentación para el cumplimiento de los derechos mencionados en el artículo 1, 2 y 3, dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.</p> <p>Parágrafo 2. El Ministerio del Trabajo reglamentará la forma en que se capacitará a los profesores conforme a lo reseñado en el numeral 4 dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.</p>	
<p>Artículo 4. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 210B. Difusión no consentida de imágenes con</p>	<p>Artículo 4. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 210B. Difusión no consentida de imágenes con</p>	<p>Se acogen sugerencias presentadas por MinTic.</p>

<p>contenido sexual. El que, con el fin de satisfacer sus deseos o los de un tercero o con la intención de castigar o silenciar publique, divulgue o revele, a través de cualquier medio o red de información o de comunicación, imágenes o grabaciones audiovisuales, o imágenes o videos generados artificialmente de la actividad sexual o con contenido sexual de una persona, sin su autorización, incurrirá en prisión de setenta y dos (72) a ciento veinte (120) meses.</p> <p>Cuando la conducta sea cometida por los cónyuges o compañeros permanentes, aunque se hubieren separado o divorciado, la pena se aumentará hasta en una tercera parte.</p> <p>No habrá lugar a responsabilidad penal cuando el agente utilice dichos contenidos con la intención de denunciar ante las autoridades competentes situaciones de agresión o acoso de las que ha sido o es víctima.</p>	<p>El que, con el fin de satisfacer sus deseos o los de un tercero o con la intención de castigar o silenciar publique, divulgue o revele, a través de cualquier medio o red de información o de comunicación o sistema informático, imágenes o grabaciones audiovisuales, o imágenes o videos generados artificialmente de la actividad sexual o con contenido sexual de una persona, sin su autorización, incurrirá en prisión de setenta y dos (72) a ciento veinte (120) meses.</p> <p>Cuando la conducta sea cometida por los cónyuges o compañeros permanentes, aunque se hubieren separado o divorciado, la pena se aumentará hasta en una tercera parte.</p> <p>No habrá lugar a responsabilidad penal cuando el agente utilice dichos contenidos con la intención de denunciar ante las autoridades competentes situaciones de agresión o acoso de las que ha sido o es víctima.</p>	<p>Se elimina la finalidad del tipo para evitar dificultades probatorias del tipo penal.</p> <p>Se añaden los sistemas informáticos para que el tipo penal quede completo.</p>
<p>Artículo 5. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 210C. Grooming. El que haciéndose pasar por otra persona, o habiendo mentido sobre sus datos personales obtenga imágenes o grabaciones audiovisuales de la actividad sexual o con</p>	<p>Artículo 5. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 210C. Grooming. El que haciéndose pasar por otra persona, o habiendo mentido sobre sus datos personales, obtenga imágenes o grabaciones audiovisuales de la actividad sexual o con</p>	<p>Sin modificaciones</p>

<p>contenido sexual de un menor de edad, incurrirá en prisión de setenta y dos (72), a ciento veinte (120) meses, sin perjuicio de la pena que le corresponda por los demás delitos que se ocasionen con esta conducta.</p>	<p>contenido sexual de un menor de edad, incurrirá en prisión de setenta y dos (72), a ciento veinte (120) meses, sin perjuicio de la pena que le corresponda por los demás delitos que se ocasionen con esta conducta.</p>	
<p>Artículo 6. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 228A. Ciber-acoso. El que, sistemáticamente, usando cualquier medio o red de información o de comunicación, con el fin de causar daño o intimidación a otro promueva o difunda noticias falsas, imágenes o grabaciones audiovisuales, con contenido sensible sin consentimiento de su titular, o que incentiven al odio, incurrirá en multa.</p>	<p>Artículo 6. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 228A. Ciber-acoso. El que, sistemáticamente, usando cualquier medio o red de información o de comunicación o sistema informático, con el fin de causar daño o intimidación promueva o difunda noticias falsas, imágenes o grabaciones audiovisuales, con contenido sensible sin consentimiento de su titular, o que incentiven al odio, incurrirá en multa.</p> <p>Parágrafo. Será contenido sensible todas aquellas imágenes o grabaciones audiovisuales de la persona en las que aparezca desnudo o semidesnudo o que hagan mención a la actividad sexual, orientación, género, religión o creencias.</p>	<p>Se añaden los sistemas informáticos para que el tipo penal quede completo.</p> <p>Se define qué se entiende por contenido sensible.</p>
<p>Artículo 7. Adiciónese un nuevo numeral al artículo 240 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 240. Hurto Calificado. (...)</p>	<p>Artículo 7. Adiciónese un nuevo numeral al artículo 240 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 240. Hurto Calificado. (...)</p>	<p>Sin modificaciones</p>

<p>5. Prevaliéndose de datos personales a los que tuviere acceso en razón o con ocasión de su empleo, oficio o profesión.</p>	<p>5. Prevaliéndose de datos personales a los que tuviere acceso en razón o con ocasión de su empleo, oficio o profesión.</p>	
<p>Artículo 8. Modifíquese el numeral 4 del artículo 241 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 241. Circunstancias de agravación punitiva. (...) 4. Por persona disfrazada, o aduciendo calidad supuesta, o simulando autoridad o invocando falsa orden de la misma, <u>o aprovechándose de uniforme o de signo distintivo de personas jurídicas, ONG's, empresas, o plataformas virtuales.</u></p>	<p>Artículo 8. Modifíquese el numeral 4 del artículo 241 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 241. Circunstancias de agravación punitiva. (...) 4. Por persona disfrazada, o aduciendo calidad supuesta, o simulando autoridad o invocando falsa orden de la misma, <u>o aprovechándose de uniforme o de signo distintivo de personas jurídicas, ONG's, empresas, o plataformas virtuales.</u></p>	<p>Sin modificaciones</p>
<p>Artículo 9. Adiciónese dos nuevos numerales al artículo 245 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 245. Circunstancias de agravación. (...) 12. Cuando el constreñimiento consiste en la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación, imágenes o grabaciones audiovisuales de la actividad sexual, o con contenido sexual de la víctima. 13. Cuando la conducta se cometa en persona menor de dieciocho (18) años.</p>	<p>Artículo 9. Adiciónese dos nuevos numerales al artículo 245 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 245. Circunstancias de agravación. (...) 12. Cuando el constreñimiento consiste en la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación o sistema de información, imágenes o grabaciones audiovisuales de la actividad sexual, o con contenido sexual de la víctima. 13. Cuando la conducta se cometa en persona menor de dieciocho (18) años.</p>	<p>Se añaden los sistemas informáticos para que el tipo penal quede completo.</p>

<p>Artículo 10. Adiciónese un nuevo numeral al artículo 247 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 247. <i>Circunstancias de agravación punitiva.</i> (...) 7. La conducta se realice a través de medios informáticos, electrónicos o telemáticos, o cualquier técnica de manipulación informática.</p>	<p>Artículo 10. Adiciónese un nuevo numeral al artículo 247 de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 247. <i>Circunstancias de agravación punitiva.</i> (...) 7. La conducta se realice a través de medios informáticos, electrónicos o telemáticos, o cualquier técnica de manipulación informática.</p>	Sin modificaciones
<p>Artículo 11. Modifíquese el artículo 269E de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 269E. <i>Uso de software malicioso.</i> El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, <u>use</u>, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.</p>	<p>Artículo 11. Modifíquese el artículo 269E de la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 269E. <i>Uso de software malicioso.</i> El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, <u>use</u>, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.</p>	Sin modificaciones
<p>Artículo 12. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 296A. <i>Falsedad personal usando medios tecnológicos.</i> El que, sin consentimiento del sujeto pasivo, y valiéndose de medios tecnológicos, creare imágenes o videos en los que</p>	<p>Artículo 12. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 296A. <i>Falsedad personal usando medios tecnológicos.</i> El que, sin consentimiento del sujeto pasivo, y valiéndose de medios tecnológicos, creare imágenes o videos en los que se simula</p>	Se mejora redacción para que se entienda que no es

<p>se simula el rostro de otra persona, y posteriormente los difundiere o publicare o a través de cualquier medio o red de información o de comunicación, con el propósito de obtener algún provecho económico, social o político, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses.</p>	<p>el rostro de otra persona, y posteriormente los difundiere o sin haberla creado las publicare o las difundiere a través de cualquier medio o red de información o de comunicación o sistema de información, con el propósito de obtener algún provecho económico, social, o político o sexual, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses.</p>	<p>necesario que el sujeto activo haya creado el material delictivo Se agrega el verbo rector difundir Correcciones de forma</p>
<p>Artículo 13. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 374B. Disposiciones comunes. Cuando las conductas de los artículos 372, 373 y 374 se cometan a través de cualquier medio, red de información o de comunicación o plataforma digital destinada para tal fin, la pena se aumentará en una tercera parte.</p>	<p>Artículo 13. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:</p> <p>Artículo 374B. Disposiciones comunes. Cuando las conductas de los artículos 372, 373 y 374 se cometan a través de cualquier medio, red de información o de comunicación o plataforma digital destinada para tal fin, la pena se aumentará en una tercera parte.</p>	<p>Sin modificaciones</p>
<p>Artículo 14. Adiciónese un nuevo artículo a la Ley 906 de 2004, el cual quedará así:</p> <p>Artículo 91 A. Bloqueos de usuarios y dominios de internet. En cualquier momento a partir de la indagación, la Fiscalía General de la Nación podrá solicitar al juez de control de garantías que ordene a los proveedores de redes y servicios de telecomunicaciones, el bloqueo preventivo de los dominios de Internet, URL, cuentas y</p>	<p>Artículo 14. Adiciónese un nuevo artículo a la Ley 906 de 2004, el cual quedará así:</p> <p>Artículo 91 A. Bloqueos de usuarios y dominios de internet. En cualquier momento a partir de la indagación, la Fiscalía General de la Nación podrá solicitar al juez de control de garantías que ordene a los proveedores de redes y servicios de telecomunicaciones, el bloqueo preventivo de los dominios de Internet, URL, cuentas y</p>	<p>Sin modificaciones</p>

<p>usuarios cuando existan motivos fundados que permitan inferir que, a través de aquellos, continuaría el desarrollo total o parcial de actividades delictivas en detrimento de los derechos de los niños, niñas y adolescentes.</p> <p>El bloqueo se volverá definitivo cuando en la providencia que ponga fin al proceso resulte acreditada la materialidad de la infracción penal.</p> <p>El funcionario judicial informará al Ministerio de Tecnologías de la Información y las Comunicaciones, o a quien haga sus veces, y a las demás autoridades competentes las decisiones de bloqueo, preventivo o definitivo, para lo de su competencia.</p> <p>Parágrafo. El bloqueo preventivo o definitivo de los dominios de internet, URL, cuentas y usuarios deberá atender el principio de proporcionalidad, de manera tal que no vulnere derechos fundamentales como el de libertad de expresión y acceso a la información. Sobre esta decisión procede el recurso de reposición y de apelación.</p>	<p>usuarios cuando existan motivos fundados que permitan inferir que, a través de aquellos, continuaría el desarrollo total o parcial de actividades delictivas en detrimento de los derechos de los niños, niñas y adolescentes.</p> <p>Esta solicitud deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.</p> <p>El bloqueo se volverá definitivo cuando en la providencia que ponga fin al proceso resulte acreditada la materialidad de la infracción penal.</p> <p>El funcionario judicial informará al Ministerio de Tecnologías de la Información y las Comunicaciones, o a quien haga sus veces, y a las demás autoridades competentes las decisiones de bloqueo, preventivo o definitivo, para lo de su competencia.</p> <p>Parágrafo. El bloqueo preventivo o definitivo de los dominios de internet, URL, cuentas y usuarios deberá atender el principio de proporcionalidad, de manera tal que no vulnere derechos fundamentales como el de libertad de expresión y acceso a la información. Sobre esta decisión procede el recurso de reposición y de apelación.</p>	<p>Para que quede claro cuál será el tipo de control que requiere la medida.</p> <p>Sugerencia del Ministerio de las TIC</p>
--	--	--

<p>Artículo 15. Modifíquese el artículo 38 de la ley 1801 de 2016, el cual quedará así:</p> <p>Artículo 38. Comportamientos que afectan la integridad de niños, niñas y adolescentes. Los siguientes comportamientos afectan la integridad de los niños, niñas y adolescentes y por lo tanto no deben realizarse. Su incumplimiento da lugar a medidas correctivas, sin perjuicio de lo establecido por la normatividad vigente sobre la materia y de la responsabilidad penal a que haya lugar:</p> <p>1. Permitir, auspiciar, tolerar, inducir o constreñir el ingreso de los niños, niñas y adolescentes a los lugares donde:</p> <p>a) Se realicen espectáculos o actividades cinematográficas aptas solo para mayores de 18 años;</p> <p>b) Se preste el servicio de videojuegos, salvo que sean aptos para la edad del niño, niña o adolescente, en las condiciones establecidas por la Ley 1554 de 2012;</p> <p>c) Se practiquen actividades peligrosas, de acuerdo con la reglamentación establecida por el Gobierno Nacional;</p> <p>d) Se realicen actividades sexuales o pornográficas, o se ejerza la prostitución, o la explotación sexual;</p>	<p>Artículo 15. Modifíquese el artículo 38 de la ley 1801 de 2016, el cual quedará así:</p> <p>Artículo 38. Comportamientos que afectan la integridad de niños, niñas y adolescentes. Los siguientes comportamientos afectan la integridad de los niños, niñas y adolescentes y por lo tanto no deben realizarse. Su incumplimiento da lugar a medidas correctivas, sin perjuicio de lo establecido por la normatividad vigente sobre la materia y de la responsabilidad penal a que haya lugar:</p> <p>1. Permitir, auspiciar, tolerar, inducir o constreñir el ingreso de los niños, niñas y adolescentes a los lugares donde:</p> <p>a) Se realicen espectáculos o actividades cinematográficas aptas solo para mayores de 18 años;</p> <p>b) Se preste el servicio de videojuegos, salvo que sean aptos para la edad del niño, niña o adolescente, en las condiciones establecidas por la Ley 1554 de 2012;</p> <p>c) Se practiquen actividades peligrosas, de acuerdo con la reglamentación establecida por el Gobierno Nacional;</p> <p>d) Se realicen actividades sexuales o pornográficas, o se ejerza la prostitución, o la explotación sexual;</p>	<p>Sin modificaciones</p>
---	---	---------------------------

<p>e) Se realicen actividades de diversión destinadas al consumo de bebidas alcohólicas y consumo de cigarrillo, tabaco y sus derivados y sustancias psicoactivas;</p> <p>f) Se desarrollen juegos de suerte y azar localizados;</p> <p>2. Inducir, engañar o realizar cualquier acción para que los niños, niñas y adolescentes ingresen o participen de actividades que les están prohibidas por las normas vigentes.</p> <p>3. Permitir o inducir a los niños, niñas y adolescentes a utilizar las telecomunicaciones, publicaciones y documentos para acceder a material pornográfico.</p> <p>4. Emplear o inducir a los niños, niñas y adolescentes a utilizar indebidamente las telecomunicaciones o sistemas de emergencia.</p> <p>5. Facilitar, distribuir, ofrecer, comercializar, prestar o alquilar, cualquiera de los siguientes elementos, sustancias o bebidas, a niños, niñas o adolescentes:</p> <p>a) Material pornográfico;</p> <p>b) Bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;</p>	<p>e) Se realicen actividades de diversión destinadas al consumo de bebidas alcohólicas y consumo de cigarrillo, tabaco y sus derivados y sustancias psicoactivas;</p> <p>f) Se desarrollen juegos de suerte y azar localizados;</p> <p>2. Inducir, engañar o realizar cualquier acción para que los niños, niñas y adolescentes ingresen o participen de actividades que les están prohibidas por las normas vigentes.</p> <p>3. Permitir o inducir a los niños, niñas y adolescentes a utilizar las telecomunicaciones, publicaciones y documentos para acceder a material pornográfico.</p> <p>4. Emplear o inducir a los niños, niñas y adolescentes a utilizar indebidamente las telecomunicaciones o sistemas de emergencia.</p> <p>5. Facilitar, distribuir, ofrecer, comercializar, prestar o alquilar, cualquiera de los siguientes elementos, sustancias o bebidas, a niños, niñas o adolescentes:</p> <p>a) Material pornográfico;</p> <p>b) Bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;</p>	
---	---	--

<p>c) Pólvora o sustancias prohibidas; d) Armas, neumáticas o de aire, o que se asimilen a estas, elementos cortantes, punzantes, contundentes o sus combinaciones;</p> <p>6. Inducir a niños, niñas o adolescentes a: a) Consumir bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud; b) Participar en juegos de suerte y azar; c) Ingresar a fiestas o eventos similares en los cuales exista previa restricción de edad por parte de las autoridades de policía, o esté prohibido su ingreso por las normas vigentes. d) La explotación laboral.</p> <p>7. Permitir que los niños, niñas y adolescentes sean tenedores de animales potencialmente peligrosos.</p> <p>8. Ejercer, permitir, favorecer o propiciar el abuso, los actos y la explotación sexual de niños, niñas o adolescentes.</p> <p>9. Utilizar a niños, niñas y adolescentes para evitar el cumplimiento de una orden de policía.</p> <p>10. Permitir que los niños, niñas y adolescentes hagan uso de piscinas y estructuras</p>	<p>c) Pólvora o sustancias prohibidas; d) Armas, neumáticas o de aire, o que se asimilen a estas, elementos cortantes, punzantes, contundentes o sus combinaciones;</p> <p>6. Inducir a niños, niñas o adolescentes a: a) Consumir bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud; b) Participar en juegos de suerte y azar; c) Ingresar a fiestas o eventos similares en los cuales exista previa restricción de edad por parte de las autoridades de policía, o esté prohibido su ingreso por las normas vigentes. d) La explotación laboral.</p> <p>7. Permitir que los niños, niñas y adolescentes sean tenedores de animales potencialmente peligrosos.</p> <p>8. Ejercer, permitir, favorecer o propiciar el abuso, los actos y la explotación sexual de niños, niñas o adolescentes.</p> <p>9. Utilizar a niños, niñas y adolescentes para evitar el cumplimiento de una orden de policía.</p> <p>10. Permitir que los niños, niñas y adolescentes hagan uso de piscinas y estructuras</p>	
---	---	--

<p>similares, de uso colectivo o de propiedad privada unihabitacional, sin el cumplimiento de los requisitos establecidos por la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.</p> <p>11. Permitir que los niños, niñas y adolescentes sean parte de confrontaciones violentas que puedan derivar en agresiones físicas.</p> <p><u>12. Acceder a un sistema informático para impedir u obstaculizar el normal funcionamiento de las clases.</u></p> <p>Parágrafo 1o. En los comportamientos señalados en el literal b) del numeral 1 del presente artículo, se impondrá solo la medida correctiva de suspensión temporal de actividad y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1554 de 2012 y las normas que la adicionen o modifiquen.</p> <p>Parágrafo 2o. En los comportamientos señalados en el literal d) del numeral 1 del presente artículo, será procedente también la medida correctiva de suspensión definitiva de la actividad.</p> <p>Parágrafo 3o. En los comportamientos señalados en el literal d) del numeral 1 y en</p>	<p>similares, de uso colectivo o de propiedad privada unihabitacional, sin el cumplimiento de los requisitos establecidos por la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.</p> <p>11. Permitir que los niños, niñas y adolescentes sean parte de confrontaciones violentas que puedan derivar en agresiones físicas.</p> <p><u>12. Acceder a un sistema informático para impedir u obstaculizar el normal funcionamiento de las clases.</u></p> <p>Parágrafo 1o. En los comportamientos señalados en el literal b) del numeral 1 del presente artículo, se impondrá solo la medida correctiva de suspensión temporal de actividad y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1554 de 2012 y las normas que la adicionen o modifiquen.</p> <p>Parágrafo 2o. En los comportamientos señalados en el literal d) del numeral 1 del presente artículo, será procedente también la medida correctiva de suspensión definitiva de la actividad.</p> <p>Parágrafo 3o. En los comportamientos señalados en el literal d) del numeral 1 y en</p>	
--	--	--

<p>el numeral 8, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en las Leyes 679 de 2001, 1236 de 2008, 1329 de 2009 y las normas que las adicionen o modifiquen.</p> <p>Parágrafo 4o. En los comportamientos señalados en el numeral 10, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.</p> <p>Parágrafo 5o. En los casos en los que los derechos de los niños, niñas y adolescentes se encuentren amenazados, inobservados o vulnerados se aplicará lo dispuesto en la Ley 109 2006.</p> <p>Parágrafo 6o. A quien incurra en uno o más de los comportamientos antes señalados, se le aplicarán las siguientes medidas correctivas:</p> <p>COMPORTA MIENTOS MEDIDA CORRECTIVA A APLICAR</p>	<p>el numeral 8, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en las Leyes 679 de 2001, 1236 de 2008, 1329 de 2009 y las normas que las adicionen o modifiquen.</p> <p>Parágrafo 4o. En los comportamientos señalados en el numeral 10, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.</p> <p>Parágrafo 5o. En los casos en los que los derechos de los niños, niñas y adolescentes se encuentren amenazados, inobservados o vulnerados se aplicará lo dispuesto en la Ley 109 2006.</p> <p>Parágrafo 6o. A quien incurra en uno o más de los comportamientos antes señalados, se le aplicarán las siguientes medidas correctivas:</p> <p>COMPORTA MIENTOS MEDIDA CORRECTIVA A APLICAR</p>	
--	--	--

Numeral 1	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.	Numeral 1	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 2	Multa General tipo 4; Suspensión temporal de actividad.	Numeral 2	Multa General tipo 4; Suspensión temporal de actividad.
Numeral 3	Multa General tipo 4; Destrucción de bien.	Numeral 3	Multa General tipo 4; Destrucción de bien.
Numeral 4	Multa General tipo 1.	Numeral 4	Multa General tipo 1.
Numeral 5	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.	Numeral 5	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 6	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.	Numeral 6	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 7	Multa General tipo 2.	Numeral 7	Multa General tipo 2.
Numeral 8	Suspensión definitiva de actividad.	Numeral 8	Suspensión definitiva de actividad.

<p>Numeral 9 Multa General tipo 4.</p> <p>Numeral 10 Suspensión temporal de actividad.</p> <p>Numeral 11 Multa General tipo 4.</p> <p><u>Numeral 12 Multa General tipo 4; Participación en programa comunitario o actividad pedagógica de convivencia.</u></p> <p>Parágrafo 7o. Al menor de 18 años que cometa cualquiera de los anteriores comportamientos se le aplicarán las medidas previstas en el Código de infancia y adolescencia.</p> <p>Parágrafo 8o. Quien en el término de un año contado a partir de la aplicación de la medida, reincida en alguno de los comportamientos prohibidos en el presente capítulo que dan lugar a la medida de suspensión temporal, será objeto de suspensión definitiva de la actividad.</p> <p><u>Parágrafo 9o. En el comportamiento de sabotaje descrito en el numeral 12, se realizará la compulsión de copias a la Fiscalía General</u></p>	<p>Numeral 9 Multa General tipo 4.</p> <p>Numeral 10 Suspensión temporal de actividad.</p> <p>Numeral 11 Multa General tipo 4.</p> <p><u>Numeral 12 Multa General tipo 4; Participación en programa comunitario o actividad pedagógica de convivencia.</u></p> <p>Parágrafo 7o. Al menor de 18 años que cometa cualquiera de los anteriores comportamientos se le aplicarán las medidas previstas en el Código de infancia y adolescencia.</p> <p>Parágrafo 8o. Quien en el término de un año contado a partir de la aplicación de la medida, reincida en alguno de los comportamientos prohibidos en el presente capítulo que dan lugar a la medida de suspensión temporal, será objeto de suspensión definitiva de la actividad.</p> <p><u>Parágrafo 9o. En el comportamiento de sabotaje descrito en el numeral 12, se realizará la compulsión de copias a la Fiscalía General</u></p>	
---	---	--

<p><u>de la Nación, cuando como forma de sabotaje se reproduzca material pornográfico.</u></p>	<p><u>de la Nación, cuando como forma de sabotaje se reproduzca material pornográfico.</u></p>	
<p>CAPÍTULO III. DISPOSICIONES FINALES.</p> <p>Artículo 16. <i>Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos.</i> Créese el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Su integración y funciones se regirán por lo dispuesto en la presente ley. El Comité será el organismo consultivo del Gobierno Nacional y el ente coordinador de las acciones que desarrolle el estado colombiano, a través de la estrategia nacional para la lucha contra los delitos cibernéticos.</p>	<p>CAPÍTULO III. DISPOSICIONES FINALES.</p> <p>Artículo 16. <i>Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos.</i> Créese el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Su integración y funciones se regirán por lo dispuesto en la presente ley. El Comité será el organismo consultivo del Gobierno Nacional y el ente coordinador de las acciones que desarrolle el estado colombiano, a través de la estrategia nacional para la lucha contra los delitos cibernéticos.</p>	Sin modificaciones
<p>Artículo 17. <i>Integración del Comité.</i> El Comité estará integrado por los siguientes miembros:</p> <ol style="list-style-type: none"> 1. La Fiscalía General de la Nación o quien hiciera sus veces, quien lo presidirá. 2. El Ministerio de Relaciones Exteriores o el Director de Asuntos Consulares y de Comunidades Colombianas en el Exterior, o quien hiciera sus veces. 3. El Ministerio de Educación o quien hiciera sus veces. 4. La Comisión Reguladora de Comunicaciones o quien hiciera sus veces 	<p>Artículo 17. <i>Integración del Comité.</i> El Comité estará integrado por los siguientes miembros:</p> <ol style="list-style-type: none"> 1. La Fiscalía General de la Nación o quien hiciera sus veces, quien lo presidirá. 2. El Ministerio de Relaciones Exteriores o el Director de Asuntos Consulares y de Comunidades Colombianas en el Exterior, o quien hiciera sus veces. 3. El Ministerio de Educación o quien hiciera sus veces. 4. La Comisión Reguladora de Comunicaciones o quien hiciera sus veces 	Sin modificaciones

<p>5. La Policía Nacional o quien hiciera sus veces</p> <p>6. El Ministerio de las Tecnologías de la Información y de las Comunicaciones o quien hiciera sus veces.</p> <p>7. El Ministerio de Justicia y del Derecho o quien hiciera sus veces.</p> <p>8. La Procuraduría General de la Nación o quien hiciera sus veces.</p> <p>9. La Defensoría del Pueblo o quien hiciera sus veces.</p> <p>10. El Subdirector General de la Oficina de Interpol en Colombia o quien hiciera sus veces.</p> <p>11. El Instituto Colombiano de Bienestar Familiar o quien hiciera sus veces.</p> <p>12. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT o quien hiciera sus veces.</p> <p>13. Consejería Presidencial para la Niñez y Adolescencia o quien hiciera sus veces.</p> <p>14. Consejería Presidencial para los Derechos Humanos y Asuntos Internacionales quien hiciera sus veces.</p> <p>15. Consejería presidencial para asuntos económicos y transformación digital.</p> <p>Parágrafo 1. El Comité promoverá la creación de Comités Regionales departamentales y/o municipales contra los delitos cibernéticos, los cuales estarán presididos por los correspondientes</p>	<p>5. La Policía Nacional o quien hiciera sus veces</p> <p>6. El Ministerio de las Tecnologías de la Información y de las Comunicaciones o quien hiciera sus veces.</p> <p>7. El Ministerio de Justicia y del Derecho o quien hiciera sus veces.</p> <p>8. La Procuraduría General de la Nación o quien hiciera sus veces.</p> <p>9. La Defensoría del Pueblo o quien hiciera sus veces.</p> <p>10. El Subdirector General de la Oficina de Interpol en Colombia o quien hiciera sus veces.</p> <p>11. El Instituto Colombiano de Bienestar Familiar o quien hiciera sus veces.</p> <p>12. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT o quien hiciera sus veces.</p> <p>13. Consejería Presidencial para la Niñez y Adolescencia o quien hiciera sus veces.</p> <p>14. Consejería Presidencial para los Derechos Humanos y Asuntos Internacionales quien hiciera sus veces.</p> <p>15. Consejería presidencial para asuntos económicos y transformación digital.</p> <p>Parágrafo 1. El Comité promoverá la creación de Comités Regionales departamentales y/o municipales contra los delitos cibernéticos, los cuales estarán presididos por los correspondientes</p>	
---	---	--

<p>gobernadores o alcaldes, y que deberán contar también con una entidad que actuará como Secretaría Técnica. La Estrategia Nacional adoptada por el Comité será la base de su formulación de acción contra la Trata a nivel local haciendo los ajustes necesarios que consulten las especificidades del territorio y la población respectiva.</p> <p>Parágrafo 2. El Comité podrá invitar a sus sesiones a cualquier otra entidad del Estado, personas jurídicas de derecho privado y organizaciones internacionales, que tengan por objeto la lucha contra los delitos cibernéticos, o la protección de los Derechos Humanos de las víctimas del mismo, organizaciones que tengan por objeto la promoción y defensa de los derechos humanos, y a particulares cuya presencia sea conveniente para el cumplimiento de las funciones propias del Comité.</p> <p>Parágrafo 3. Los integrantes mencionados deberán mencionar las actividades que realizaren siendo parte del Comité, en su respectiva rendición de cuentas, cuando hubiere lugar a ello.</p>	<p>gobernadores o alcaldes, y que deberán contar también con una entidad que actuará como Secretaría Técnica. La Estrategia Nacional adoptada por el Comité será la base de su formulación de acción contra la Trata a nivel local haciendo los ajustes necesarios que consulten las especificidades del territorio y la población respectiva.</p> <p>Parágrafo 2. El Comité podrá invitar a sus sesiones a cualquier otra entidad del Estado, personas jurídicas de derecho privado y organizaciones internacionales, que tengan por objeto la lucha contra los delitos cibernéticos, o la protección de los Derechos Humanos de las víctimas del mismo, organizaciones que tengan por objeto la promoción y defensa de los derechos humanos, y a particulares cuya presencia sea conveniente para el cumplimiento de las funciones propias del Comité.</p> <p>Parágrafo 3. Los integrantes mencionados deberán mencionar las actividades que realizaren siendo parte del Comité, en su respectiva rendición de cuentas, cuando hubiere lugar a ello.</p>	
<p>Artículo 18. Funciones. El Comité Interinstitucional para la lucha contra los delitos cibernéticos ejercerá las siguientes funciones:</p>	<p>Artículo 18. Funciones. El Comité Interinstitucional para la lucha contra los delitos cibernéticos ejercerá las siguientes funciones:</p>	<p>Sin modificaciones</p>

<p>1. Desarrollar la estrategia nacional contra los delitos cibernéticos y realizar seguimiento a su ejecución</p> <p>2. Coordinar el proceso de revisión de los acuerdos y convenios internacionales relacionados con los delitos cibernéticos para supervisar su cumplimiento adecuado, y recomendar la firma de acuerdos, convenios o tratados necesarios para fortalecer la lucha contra la red.</p> <p>3. Actuar como órgano asesor y recomendar acciones a las entidades que se dedican directa o indirectamente a la lucha contra el delito cibernético.</p> <p>4. Actuar como organismo coordinador de entidades nacionales y organizaciones privadas involucradas en la implementación de la Estrategia Nacional, frente a las acciones interinstitucionales que deben tomarse.</p> <p>5. Formular recomendaciones en materia de persecución criminal de los delitos cibernéticos y del fortalecimiento de la capacidad del Estado en este campo.</p> <p>6. Recomendar la expedición de normas o regulaciones a las distintas entidades del Estado en materia de delitos cibernéticos.</p>	<p>1. Desarrollar la estrategia nacional contra los delitos cibernéticos y realizar seguimiento a su ejecución</p> <p>2. Coordinar el proceso de revisión de los acuerdos y convenios internacionales relacionados con los delitos cibernéticos para supervisar su cumplimiento adecuado, y recomendar la firma de acuerdos, convenios o tratados necesarios para fortalecer la lucha contra la red.</p> <p>3. Actuar como órgano asesor y recomendar acciones a las entidades que se dedican directa o indirectamente a la lucha contra el delito cibernético.</p> <p>4. Actuar como organismo coordinador de entidades nacionales y organizaciones privadas involucradas en la implementación de la Estrategia Nacional, frente a las acciones interinstitucionales que deben tomarse.</p> <p>5. Formular recomendaciones en materia de persecución criminal de los delitos cibernéticos y del fortalecimiento de la capacidad del Estado en este campo.</p> <p>6. Recomendar la expedición de normas o regulaciones a las distintas entidades del Estado en materia de delitos cibernéticos.</p>	
---	---	--

<p>7. Realizar estudios que permitan comprender las causas, consecuencias, formas de prevención y formas de protección a menores de edad en contra de los delitos cibernéticos.</p> <p>8. Realizar las respectivas compulsas de copias de conductas delictivas a las que tuvieren conocimiento.</p> <p>9. Diseñar estrategias internacionales que permitan la adecuada persecución criminal de los delitos cibernéticos.</p> <p>10. Diseñar su propio plan de acción y dictar su reglamento interno.</p> <p>Parágrafo. Podrán crearse grupos especializados en las distintas áreas de los delitos cibernéticos.</p>	<p>7. Realizar estudios que permitan comprender las causas, consecuencias, formas de prevención y formas de protección a menores de edad en contra de los delitos cibernéticos.</p> <p>8. Realizar las respectivas compulsas de copias de conductas delictivas a las que tuvieren conocimiento.</p> <p>9. Diseñar estrategias internacionales que permitan la adecuada persecución criminal de los delitos cibernéticos.</p> <p>10. Diseñar su propio plan de acción y dictar su reglamento interno.</p> <p>Parágrafo. Podrán crearse grupos especializados en las distintas áreas de los delitos cibernéticos.</p>	
<p>Artículo 19. Funcionamiento del Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Para el desarrollo de las funciones del Comité se creará la secretaría técnica a cargo del ministerio de justicia, quien podrá delegarla en la dependencia que para el efecto éste designe, sin que ello implique el incremento de funcionarios en su planta de personal. Esta secretaría es de carácter permanente. El Comité se reunirá en forma ordinaria por lo menos una vez cada dos</p>	<p>Artículo 19. Funcionamiento del Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Para el desarrollo de las funciones del Comité se creará la secretaría técnica a cargo del ministerio de justicia, quien podrá delegarla en la dependencia que para el efecto éste designe, sin que ello implique el incremento de funcionarios en su planta de personal. Esta secretaría es de carácter permanente. El Comité se reunirá en forma ordinaria por lo menos una vez cada dos</p>	Sin modificaciones

<p>meses, por convocatoria de la Secretaría Técnica. El Comité también se podrá reunir extraordinariamente cuando el presidente del Comité lo considere pertinente. La secretaría técnica rendirá informes bimestrales a los integrantes del Comité sobre su funcionamiento y las acciones adelantadas para dar cumplimiento a la presente ley. También rendirá informes anuales al Presidente de la República en el mismo sentido.</p>	<p>meses, por convocatoria de la Secretaría Técnica. El Comité también se podrá reunir extraordinariamente cuando el presidente del Comité lo considere pertinente. La secretaría técnica rendirá informes bimestrales a los integrantes del Comité sobre su funcionamiento y las acciones adelantadas para dar cumplimiento a la presente ley. También rendirá informes anuales al Presidente de la República en el mismo sentido.</p>	
<p>Artículo 20. Estrategia Nacional contra los Delitos Cibernéticos. El Gobierno Nacional adoptará mediante la Estrategia Nacional contra los Delitos Cibernéticos. El Comité Interinstitucional de que trata el artículo 16 de la presente ley, conformado para la Lucha contra los delitos cibernéticos formulará la estrategia nacional. Las ramas del poder público u órganos autónomos que deban intervenir en la implementación de las acciones de la presente estrategia, lo harán por medio del director correspondiente mediante acto administrativo. Los objetivos de la presente estrategia serán:</p> <p>1. Desarrollar marcos de información relativa a las causas, modalidades, particularidades regionales y consecuencias de los delitos cibernéticos.</p>	<p>Artículo 20. Estrategia Nacional contra los Delitos Cibernéticos. El Gobierno Nacional adoptará mediante la Estrategia Nacional contra los Delitos Cibernéticos. El Comité Interinstitucional de que trata el artículo 16 de la presente ley, conformado para la Lucha contra los delitos cibernéticos formulará la estrategia nacional. Las ramas del poder público u órganos autónomos que deban intervenir en la implementación de las acciones de la presente estrategia, lo harán por medio del director correspondiente mediante acto administrativo. Los objetivos de la presente estrategia serán:</p> <p>1. Desarrollar marcos de información relativa a las causas, modalidades, particularidades regionales y consecuencias de los delitos cibernéticos.</p>	Sin modificaciones

<p>2. Prevenir los delitos cibernéticos a través de medidas sociales y pedagógicas.</p> <p>3. Fortalecer las acciones de persecución a organizaciones criminales y, en general, la investigación, judicialización y sanción de los delitos cibernéticos.</p> <p>4. Proteger y asistir a las víctimas de los delitos cibernéticos, en los campos físico, psicológico, social, económico y jurídico.</p> <p>5. Promover el trabajo interinstitucional y la cooperación internacional en la lucha contra los delitos cibernéticos.</p> <p>6. Los demás que el Comité Interinstitucional considere necesarios.</p> <p>Parágrafo. La Estrategia Nacional medirá periódicamente el cumplimiento de los objetivos, así como el impacto, la eficacia y la eficiencia de la implementación de la estrategia mediante metas e indicadores de gestión.</p>	<p>2. Prevenir los delitos cibernéticos a través de medidas sociales y pedagógicas.</p> <p>3. Fortalecer las acciones de persecución a organizaciones criminales y, en general, la investigación, judicialización y sanción de los delitos cibernéticos.</p> <p>4. Proteger y asistir a las víctimas de los delitos cibernéticos, en los campos físico, psicológico, social, económico y jurídico.</p> <p>5. Promover el trabajo interinstitucional y la cooperación internacional en la lucha contra los delitos cibernéticos.</p> <p>6. Los demás que el Comité Interinstitucional considere necesarios.</p> <p>Parágrafo. La Estrategia Nacional medirá periódicamente el cumplimiento de los objetivos, así como el impacto, la eficacia y la eficiencia de la implementación de la estrategia mediante metas e indicadores de gestión.</p>	
<p>Artículo 21. Mecanismos de prevención de los delitos cibernéticos. La Estrategia Nacional contra los Delitos Cibernéticos establecerá la ejecución masiva de campañas y programas de prevención de</p>	<p>Artículo 21. Mecanismos de prevención de los delitos cibernéticos. La Estrategia Nacional contra los Delitos Cibernéticos establecerá la ejecución masiva de campañas y programas de prevención de</p>	<p>Sin modificaciones</p>

<p>los delitos cibernéticos, los cuales incluirán los factores más comunes, los medios de protección y la forma de denunciarlos. Estos mecanismos estarán a cargo del Gobierno Nacional, sus instituciones judiciales y de policía, y las autoridades nacionales y territoriales.</p>	<p>los delitos cibernéticos, los cuales incluirán los factores más comunes, los medios de protección y la forma de denunciarlos. Estos mecanismos estarán a cargo del Gobierno Nacional, sus instituciones judiciales y de policía, y las autoridades nacionales y territoriales.</p>	
<p>Artículo 22. Articulación en la investigación judicial y la acción policiva. El Ministerio de Defensa en coordinación con la Fiscalía General de la Nación realizarán capacitaciones especializadas para la investigación y persecución de los delitos cibernéticos, promoviendo la cooperación internacional en los ámbitos judiciales y policivos, respecto a los delitos cibernéticos. Estas entidades elaborarán informes anuales para el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos, con el objetivo de contribuir a una orientación de las decisiones.</p>	<p>Artículo 22. Articulación en la investigación judicial y la acción policiva. El Ministerio de Defensa en coordinación con la Fiscalía General de la Nación realizarán capacitaciones especializadas para la investigación y persecución de los delitos cibernéticos, promoviendo la cooperación internacional en los ámbitos judiciales y policivos, respecto a los delitos cibernéticos. Estas entidades elaborarán informes anuales para el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos, con el objetivo de contribuir a una orientación de las decisiones.</p>	Sin modificaciones
<p>Artículo 23. Vigencia y derogatorias. La presente ley rige a partir de su sanción y publicación, y deroga todas las normas que le sean contrarias.</p>	<p>Artículo 23. Vigencia y derogatorias. La presente ley rige a partir de su sanción y publicación, y deroga todas las normas que le sean contrarias.</p>	Sin modificaciones

VI. JUSTIFICACIÓN DE LAS MODIFICACIONES

El día 20 de noviembre del año en curso se sostuvo una mesa técnica con el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en la cual nos comunicaron algunas sugerencias de modificación al texto propuesto. En primer lugar respecto del artículo 4, sobre el sexting, fue puesto de presente que la exigencia de un ánimo subjetivo adicional al dolo en términos procesales implica el aumento de la carga de la prueba para la Fiscalía lo cual volvería

extremadamente difícil la persecución de estas graves conductas, razón por la cual proponemos eliminar el ánimo subjetivo adicional dejando en cabeza del ente acusador la obligación de determinar el dolo de la conducta además de los demás elementos típicos, antijurídicos y culpables.

En segundo lugar, los artículos 4, 6, 9 y 12 contemplan para la comisión de sus respectivas conductas la realización del injusto a través de cualquier medio o red de información o de comunicación, se estaban dejando por fuera los “sistemas de información” de esta forma se incluyen todos los conjuntos de datos que interactúan entre sí creando un sistema que no necesariamente se corresponden con las definiciones de medio o red de información o comunicación, de esta forma el tipo penal queda cubriendo todos aquellos supuestos en los que el sujeto activo comete la conducta a través de cualquiera de estos medios.

En tercer lugar, de cara al artículo 12 que vendría a tutelar aquellas conductas de DeepFaking o Morphing se realizan dos cambios, el primero que fue sugerido por el Ministerio de las TIC respecto a darle mayor alcance a los verbos rectores, en este sentido, no es necesario que quien publique las imágenes o videos sea quien las haya creado pues esto limitaría sobremanera el tipo penal. Luego, se agrega entre los fines del delito el fin sexual para que quede igualmente incluido el Morphing como aquella alteración de imágenes o videos donde el sujeto activo algunas veces coloca el rostro de su víctima en un cuerpo desnudo o con connotaciones sexuales, algunas veces de manera imperceptible, con un claro ánimo libidinoso.

Finalmente sobre el artículo 16, se sugirió y así se modificó, para que fuera claro respecto a qué clase de control (previo o posterior) de legalidad tendría esta medida de bloqueo preventivo. Al respecto, y teniendo en cuenta posibles tensiones con el Derecho Fundamental a la libertad de expresión, consideramos que esta medida debe tener un control previo por parte del juez de garantías. Otro de los aspectos sugeridos fue eliminar el inciso que establecía una remisión al Ministerio para evitar confusiones respecto a los encargados del bloqueo de páginas.

VII. CONFLICTO DE INTERÉS

De acuerdo con el artículo 3 de la Ley 2003 de 2019, atentamente nos disponemos a señalar algunos criterios guías en los que se podría configurar conflictos de intereses, para que los congresistas tomen una decisión en torno a si se encuentran inmersos en alguna de estas causales, sin embargo, pueden existir otras causales en las que se pueda encontrar cada congresista, las cuales deberán ser determinadas para cada caso en particular por su titular, siendo estos criterios meramente informativos y que deben ser analizados teniendo en cuenta lo expresado en el artículo 1 de la Ley 2003 de 2019.

Entre las situaciones que señala el artículo 1o antes mencionado, se encuentran: 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;* y el 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.”. Toda vez que se están creando tipos penales nuevos, consideramos que el presente Proyecto de Ley no genera conflictos de interés.

VIII. REFERENCIAS

[1]

<https://www.interpol.int/es/Delitos/Delitos-contra-menores/Base-de-datos-internacional-sobre-explotacion-sexual-de-menores>

[2] <https://www.theguardian.com/world/2020/apr/02/coronavirus-lockdown-raises-risk-of-online-child-abuse-charity-says>

[3] <https://www.fbi.gov/audio-repository/ftw-podcast-sextortion-activity-on-rise-053019.mp3/view>

[4] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/11966023

[5] https://pdf.ic3.gov/2019_IC3Report.pdf

[6] http://www.unicri.it/news/article/covid19_cyber_crime

[7] <https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats>

[8] <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>

[9] <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>

[10] <https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf>

[11] Las empresas en Colombia podrán recibir audios e incluso videos, en los cuales los cibercriminales suplantan a ejecutivos, clientes y proveedores para conseguir transferencias de dinero o despacho de productos. La tecnología Deepfake es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces. Tomado de (<https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf>)

IX. PROPOSICIÓN

Por las anteriores consideraciones, solicitamos a los Senadores de la Comisión Primera del Senado de la República dar Primer Debate al Proyecto de Ley No. 339 de 2020 senado “por medio de la cual se expiden lineamientos en torno a la seguridad digital, se modifica la Ley 599 de 2000, y se dictan otras disposiciones” de acuerdo al pliego de modificaciones propuesto.

Del honorable Congresista,



CARLOS EDUARDO CUEVA VILLABÓN
Senador de la República



**TEXTO PROPUESTO PARA PRIMER DEBATE DEL
PROYECTO DE LEY NO. 339 DE 2020 SENADO**

“Por medio de la cual se expiden lineamientos en torno a la seguridad digital, se modifica la Ley 599 de 2000, y se dictan otras disposiciones”

El Congreso de Colombia
DECRETA:

Artículo 1. Objeto. La presente Ley tiene por objeto clasificar y tipificar nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos que afectan a los niños, niñas y adolescentes y a la población en general, y determinar aquellas acciones dirigidas a prevenir estos delitos.

Artículo 2. Deberes del Estado. Con respecto a la digitalidad, son deberes del Estado, entre otros:

Realizar capacitaciones y sensibilizar a todos los habitantes, con el fin de darles a conocer sus derechos y deberes digitales.

Generar políticas públicas de inclusión, a fin de lograr la mayor cobertura posible del servicio.

Diseñar planes de estudio para que desde los colegios se logre la inserción de los estudiantes en el mundo digital. Particularmente, estos planes de estudio deberán preparar a los estudiantes para afrontar los retos en esta materia y prevenir los riesgos digitales.

Artículo 3. Derechos digitales de los niños, niñas y adolescentes. Todos los niños, niñas y adolescentes tienen los siguientes derechos:

A que el sistema educativo garantice su efectivo aprendizaje de los medios digitales, de forma segura y respetuosa con los derechos fundamentales.

A acceder a actividades de prevención de los delitos cibernéticos, en los niveles de educación básica, media y superior.

A conocer la problemática de los delitos cibernéticos que se produce, tanto dentro del territorio nacional como fuera de él, a través de medios de difusión masiva.

A que sus profesores tengan las competencias digitales y la formación requerida para la enseñanza y transmisión de los valores y derechos.

A una navegación segura en Internet que permita su libre desarrollo a la personalidad.

A no ser constreñidos o incitados por terceros a realizar prácticas sexuales por Internet.

A que sus datos personales sean tratados con máxima diligencia.

Los demás que les asigne la ley.

Parágrafo 1. El Ministerio de Educación expedirá la reglamentación para el cumplimiento de los derechos mencionados en el artículo 1, 2 y 3, dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.



Parágrafo 2. El Ministerio del Trabajo reglamentará la forma en que se capacitará a los profesores conforme a lo reseñado en el numeral 4 dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.

Artículo 4. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 210B. Difusión no consentida de imágenes con contenido sexual. El que publique, divulgue o revele, a través de cualquier medio o red de información o de comunicación o sistema informático, imágenes o grabaciones audiovisuales, o imágenes o videos generados artificialmente de la actividad sexual o con contenido sexual de una persona, sin su autorización, incurrirá en prisión de setenta y dos (72) a ciento veinte (120) meses.

Cuando la conducta sea cometida por los cónyuges o compañeros permanentes, aunque se hubieren separado o divorciado, la pena se aumentará hasta en una tercera parte.

No habrá lugar a responsabilidad penal cuando el agente utilice dichos contenidos con la intención de denunciar ante las autoridades competentes situaciones de agresión o acoso de las que ha sido o es víctima.

Artículo 5. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 210C. Grooming. El que haciéndose pasar por otra persona, o habiendo mentido sobre sus datos personales, obtenga imágenes o grabaciones audiovisuales de la actividad sexual o con contenido sexual de un menor de edad, incurrirá en prisión de setenta y dos (72), a ciento veinte (120) meses, sin perjuicio de la pena que le corresponda por los demás delitos que se ocasionen con esta conducta.

Artículo 6. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 228A. Ciber-acoso. El que, sistemáticamente, usando cualquier medio o red de información o de comunicación o sistema informático, con el fin de causar daño o intimidación promueva o difunda noticias falsas, imágenes o grabaciones audiovisuales, con contenido sensible sin consentimiento de su titular, o que incentiven al odio, incurrirá en multa.

Parágrafo. Será contenido sensible todas aquellas imágenes o grabaciones audiovisuales de la persona en las que aparezca desnudo o semidesnudo o que hagan mención a la actividad sexual, orientación, género, religión o creencias.

Artículo 7. Adiciónese un nuevo numeral al artículo 240 de la Ley 599 de 2000, el cual quedará así:

Artículo 240. Hurto Calificado.

(...)

5. Prevaliéndose de datos personales a los que tuviere acceso en razón o con ocasión de su empleo, oficio o profesión.

Artículo 8. Modifíquese el numeral 4 del artículo 241 de la Ley 599 de 2000, el cual quedará así:

Artículo 241. Circunstancias de agravación punitiva.



(...)

4. Por persona disfrazada, o aduciendo calidad supuesta, o simulando autoridad o invocando falsa orden de la misma, o aprovechándose de uniforme o de signo distintivo de personas jurídicas, ONG's, empresas, o plataformas virtuales.

Artículo 9. Adiciónese dos nuevos numerales al artículo 245 de la Ley 599 de 2000, el cual quedará así:

Artículo 245. Circunstancias de agravación.

(...)

12. Cuando el constreñimiento consiste en la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación o sistema de información, imágenes o grabaciones audiovisuales de la actividad sexual, o con contenido sexual de la víctima.

13. Cuando la conducta se cometa en persona menor de dieciocho (18) años.

Artículo 10. Adiciónese un nuevo numeral al artículo 247 de la Ley 599 de 2000, el cual quedará así:

Artículo 247. Circunstancias de agravación punitiva.

(...)

7. La conducta se realice a través de medios informáticos, electrónicos o telemáticos, o cualquier técnica de manipulación informática.

Artículo 11. Modifíquese el artículo 269E de la Ley 599 de 2000, el cual quedará así:

Artículo 269E. Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, use, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 12. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 296A. Falsedad personal usando medios tecnológicos. El que, sin consentimiento del sujeto pasivo, y valiéndose de medios tecnológicos, creare imágenes o videos en los que se simula el rostro de otra persona, y posteriormente los difundiere o sin haberla creado las publicare a través de cualquier medio o red de información o de comunicación o sistema de información, con el propósito de obtener algún provecho económico, social, político o sexual, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses.

Artículo 13. Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 374B. Disposiciones comunes. Cuando las conductas de los artículos 372, 373 y 374 se cometan a través de cualquier medio, red de información o de comunicación o plataforma digital destinada para tal fin, la pena se aumentará en una tercera parte.

Artículo 14. Adiciónese un nuevo artículo a la Ley 906 de 2004, el cual quedará así:

Artículo 91 A. Bloqueos de usuarios y dominios de internet. En cualquier momento a partir de la indagación, la Fiscalía General de la Nación podrá solicitar al juez de control de garantías que ordene a los proveedores de redes y servicios de telecomunicaciones, el bloqueo preventivo de los dominios de Internet, URL, cuentas y usuarios cuando existan motivos fundados que permitan inferir que, a través de aquellos, continuaría el desarrollo total o parcial de actividades delictivas en detrimento de los derechos de los niños, niñas y adolescentes.

Esta solicitud deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

El bloqueo se volverá definitivo cuando en la providencia que ponga fin al proceso resulte acreditada la materialidad de la infracción penal.

Parágrafo. El bloqueo preventivo o definitivo de los dominios de internet, URL, cuentas y usuarios deberá atender el principio de proporcionalidad, de manera tal que no vulnere derechos fundamentales como el de libertad de expresión y acceso a la información. Sobre esta decisión procede el recurso de reposición y de apelación.

Artículo 15. Modifíquese el artículo 38 de la ley 1801 de 2016, el cual quedará así:

Artículo 38. Comportamientos que afectan la integridad de niños, niñas y adolescentes. Los siguientes comportamientos afectan la integridad de los niños, niñas y adolescentes y por lo tanto no deben realizarse. Su incumplimiento da lugar a medidas correctivas, sin perjuicio de lo establecido por la normatividad vigente sobre la materia y de la responsabilidad penal a que haya lugar:

1. Permitir, auspiciar, tolerar, inducir o constreñir el ingreso de los niños, niñas y adolescentes a los lugares donde:

- a) Se realicen espectáculos o actividades cinematográficas aptas solo para mayores de 18 años;
- b) Se preste el servicio de videojuegos, salvo que sean aptos para la edad del niño, niña o adolescente, en las condiciones establecidas por la Ley 1554 de 2012;
- c) Se practiquen actividades peligrosas, de acuerdo con la reglamentación establecida por el Gobierno Nacional;
- d) Se realicen actividades sexuales o pornográficas, o se ejerza la prostitución, o la explotación sexual;
- e) Se realicen actividades de diversión destinadas al consumo de bebidas alcohólicas y consumo de cigarrillo, tabaco y sus derivados y sustancias psicoactivas;
- f) Se desarrollen juegos de suerte y azar localizados;

2. Inducir, engañar o realizar cualquier acción para que los niños, niñas y adolescentes ingresen o participen de actividades que les están prohibidas por las normas vigentes.

3. Permitir o inducir a los niños, niñas y adolescentes a utilizar las telecomunicaciones, publicaciones y documentos para acceder a material pornográfico.

4. Emplear o inducir a los niños, niñas y adolescentes a utilizar indebidamente las telecomunicaciones o sistemas de emergencia.

5. Facilitar, distribuir, ofrecer, comercializar, prestar o alquilar, cualquiera de los siguientes elementos, sustancias o bebidas, a niños, niñas o adolescentes:

- a) Material pornográfico;
- b) Bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;
- c) Pólvora o sustancias prohibidas;
- d) Armas, neumáticas o de aire, o que se asimilen a estas, elementos cortantes, punzantes, contundentes o sus combinaciones;

6. Inducir a niños, niñas o adolescentes a:

- a) Consumir bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;
- b) Participar en juegos de suerte y azar;
- c) Ingresar a fiestas o eventos similares en los cuales exista previa restricción de edad por parte de las autoridades de policía, o esté prohibido su ingreso por las normas vigentes.
- d) La explotación laboral.

7. Permitir que los niños, niñas y adolescentes sean tenedores de animales potencialmente peligrosos.

8. Ejercer, permitir, favorecer o propiciar el abuso, los actos y la explotación sexual de niños, niñas o adolescentes.

9. Utilizar a niños, niñas y adolescentes para evitar el cumplimiento de una orden de policía.

10. Permitir que los niños, niñas y adolescentes hagan uso de piscinas y estructuras similares, de uso colectivo o de propiedad privada unihabitacional, sin el cumplimiento de los requisitos establecidos por la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.

11. Permitir que los niños, niñas y adolescentes sean parte de confrontaciones violentas que puedan derivar en agresiones físicas.

12. Acceder a un sistema informático para impedir u obstaculizar el normal funcionamiento de las clases.

Parágrafo 1o. En los comportamientos señalados en el literal b) del numeral 1 del presente artículo, se impondrá solo la medida correctiva de suspensión temporal de actividad y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1554 de 2012 y las normas que la adicionen o modifiquen.

Parágrafo 2o. En los comportamientos señalados en el literal d) del numeral 1 del presente artículo, será procedente también la medida correctiva de suspensión definitiva de la actividad.

Parágrafo 3o. En los comportamientos señalados en el literal d) del numeral 1 y en el numeral 8, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en las Leyes 679 de 2001, 1236 de 2008, 1329 de 2009 y las normas que las adicionen o modifiquen.

Parágrafo 4o. En los comportamientos señalados en el numeral 10, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.

Parágrafo 5o. En los casos en los que los derechos de los niños, niñas y adolescentes se encuentren amenazados, inobservados o vulnerados se aplicará lo dispuesto en la Ley 109 2006.

Parágrafo 6o. A quien incurra en uno o más de los comportamientos antes señalados, se le aplicarán las siguientes medidas correctivas:

COMPORTAMIENTOS	MEDIDA CORRECTIVA A APLICAR
Numeral 1	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 2	Multa General tipo 4; Suspensión temporal de actividad.
Numeral 3	Multa General tipo 4; Destrucción de bien.
Numeral 4	Multa General tipo 1.
Numeral 5	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 6	Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien.
Numeral 7	Multa General tipo 2.
Numeral 8	Suspensión definitiva de actividad.
Numeral 9	Multa General tipo 4.
Numeral 10	Suspensión temporal de actividad.
Numeral 11	Multa General tipo 4.
Numeral 12	Multa General tipo 4; Participación en programa comunitario o actividad pedagógica de convivencia.

Parágrafo 7o. Al menor de 18 años que cometa cualquiera de los anteriores comportamientos se le aplicarán las medidas previstas en el Código de infancia y adolescencia.

Parágrafo 8o. Quien en el término de un año contado a partir de la aplicación de la medida, reincida en alguno de los comportamientos prohibidos en el presente capítulo que dan lugar a la medida de suspensión temporal, será objeto de suspensión definitiva de la actividad.

Parágrafo 9o. En el comportamiento de sabotaje descrito en el numeral 12, se realizará la compulsión de copias a la Fiscalía General de la Nación, cuando como forma de sabotaje se reproduzca material pornográfico.

CAPÍTULO III. DISPOSICIONES FINALES.

Artículo 16. Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Créese el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Su integración y funciones se



regirán por lo dispuesto en la presente ley. El Comité será el organismo consultivo del Gobierno Nacional y el ente coordinador de las acciones que desarrolle el estado colombiano, a través de la estrategia nacional para la lucha contra los delitos cibernéticos.

Artículo 17. Integración del Comité. El Comité estará integrado por los siguientes miembros:

1. La Fiscalía General de la Nación o quien hiciera sus veces, quien lo presidirá.
2. El Ministerio de Relaciones Exteriores o el Director de Asuntos Consulares y de Comunidades Colombianas en el Exterior, o quien hiciera sus veces.
3. El Ministerio de Educación o quien hiciera sus veces.
4. La Comisión Reguladora de Comunicaciones o quien hiciera sus veces
5. La Policía Nacional o quien hiciera sus veces
6. El Ministerio de las Tecnologías de la Información y de las Comunicaciones o quien hiciera sus veces.
7. El Ministerio de Justicia y del Derecho o quien hiciera sus veces.
8. La Procuraduría General de la Nación o quien hiciera sus veces.
9. La Defensoría del Pueblo o quien hiciera sus veces.
10. El Subdirector General de la Oficina de Interpol en Colombia o quien hiciera sus veces.
11. El Instituto Colombiano de Bienestar Familiar o quien hiciera sus veces.
12. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT o quien hiciera sus veces.
13. Consejería Presidencial para la Niñez y Adolescencia o quien hiciera sus veces.
14. Consejería Presidencial para los Derechos Humanos y Asuntos Internacionales quien hiciera sus veces.
15. Consejería presidencial para asuntos económicos y transformación digital.

Parágrafo 1. El Comité promoverá la creación de Comités Regionales departamentales y/o municipales contra los delitos cibernéticos, los cuales estarán presididos por los correspondientes gobernadores o alcaldes, y que deberán contar también con una entidad que actuará como Secretaría Técnica. La Estrategia Nacional adoptada por el Comité será la base de su formulación de acción contra la Trata a nivel local haciendo los ajustes necesarios que consulten las especificidades del territorio y la población respectiva.

Parágrafo 2. El Comité podrá invitar a sus sesiones a cualquier otra entidad del Estado, personas jurídicas de derecho privado y organizaciones internacionales, que tengan por objeto la lucha contra los delitos cibernéticos, o la protección de los Derechos Humanos de las víctimas del mismo, organizaciones que tengan por objeto la promoción y defensa de los derechos humanos, y a particulares cuya presencia sea conveniente para el cumplimiento de las funciones propias del Comité.

Parágrafo 3. Los integrantes mencionados deberán mencionar las actividades que realizaren siendo parte del Comité, en su respectiva rendición de cuentas, cuando hubiere lugar a ello.

Artículo 18. Funciones. El Comité Interinstitucional para la lucha contra los delitos cibernéticos ejercerá las siguientes funciones:

1. Desarrollar la estrategia nacional contra los delitos cibernéticos y realizar seguimiento a su ejecución

2. Coordinar el proceso de revisión de los acuerdos y convenios internacionales relacionados con los delitos cibernéticos para supervisar su cumplimiento adecuado, y recomendar la firma de acuerdos, convenios o tratados necesarios para fortalecer la lucha contra la red.
3. Actuar como órgano asesor y recomendar acciones a las entidades que se dedican directa o indirectamente a la lucha contra el delito cibernético.
4. Actuar como organismo coordinador de entidades nacionales y organizaciones privadas involucradas en la implementación de la Estrategia Nacional, frente a las acciones interinstitucionales que deben tomarse.
5. Formular recomendaciones en materia de persecución criminal de los delitos cibernéticos y del fortalecimiento de la capacidad del Estado en este campo.
6. Recomendar la expedición de normas o regulaciones a las distintas entidades del Estado en materia de delitos cibernéticos.
7. Realizar estudios que permitan comprender las causas, consecuencias, formas de prevención y formas de protección a menores de edad en contra de los delitos cibernéticos.
8. Realizar las respectivas compulsas de copias de conductas delictivas a las que tuvieren conocimiento.
9. Diseñar estrategias internacionales que permitan la adecuada persecución criminal de los delitos cibernéticos.
10. Diseñar su propio plan de acción y dictar su reglamento interno.

Parágrafo. Podrán crearse grupos especializados en las distintas áreas de los delitos cibernéticos.

Artículo 19. Funcionamiento del Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Para el desarrollo de las funciones del Comité se creará la secretaría técnica a cargo del ministerio de justicia, quien podrá delegarla en la dependencia que para el efecto éste designe, sin que ello implique el incremento de funcionarios en su planta de personal. Esta secretaría es de carácter permanente. El Comité se reunirá en forma ordinaria por lo menos una vez cada dos meses, por convocatoria de la Secretaría Técnica. El Comité también se podrá reunir extraordinariamente cuando el presidente del Comité lo considere pertinente. La secretaría técnica rendirá informes bimestrales a los integrantes del Comité sobre su funcionamiento y las acciones adelantadas para dar cumplimiento a la presente ley. También rendirá informes anuales al Presidente de la República en el mismo sentido.

Artículo 20. Estrategia Nacional contra los Delitos Cibernéticos. El Gobierno Nacional adoptará mediante la Estrategia Nacional contra los Delitos Cibernéticos. El Comité Interinstitucional de que trata el artículo 16 de la presente ley, conformado para la Lucha contra los delitos cibernéticos formulará la estrategia nacional. Las ramas del poder público u órganos autónomos que deban intervenir en la implementación de las acciones de la presente estrategia, lo harán por medio del director correspondiente mediante acto administrativo. Los objetivos de la presente estrategia serán:

1. Desarrollar marcos de información relativa a las causas, modalidades, particularidades regionales y consecuencias de los delitos cibernéticos.
2. Prevenir los delitos cibernéticos a través de medidas sociales y pedagógicas.
3. Fortalecer las acciones de persecución a organizaciones criminales y, en general, la investigación, judicialización y sanción de los delitos cibernéticos.
4. Proteger y asistir a las víctimas de los delitos cibernéticos, en los campos físico, psicológico, social, económico y jurídico.
5. Promover el trabajo interinstitucional y la cooperación internacional en la lucha contra los delitos cibernéticos.
6. Los demás que el Comité Interinstitucional considere necesarios.

Parágrafo. La Estrategia Nacional medirá periódicamente el cumplimiento de los objetivos, así como el impacto, la eficacia y la eficiencia de la implementación de la estrategia mediante metas e indicadores de gestión.

Artículo 21. Mecanismos de prevención de los delitos cibernéticos. La Estrategia Nacional contra los Delitos Cibernéticos establecerá la ejecución masiva de campañas y programas de prevención de los delitos cibernéticos, las cuales incluirán los factores más comunes, los medios de protección y la forma de denunciarlos. Estos mecanismos estarán a cargo del Gobierno Nacional, sus instituciones judiciales y de policía, y las autoridades nacionales y territoriales.

Artículo 22. Articulación en la investigación judicial y la acción policiva. El Ministerio de Defensa en coordinación con la Fiscalía General de la Nación realizarán capacitaciones especializadas para la investigación y persecución de los delitos cibernéticos, promoviendo la cooperación internacional en los ámbitos judiciales y policivos, respecto a los delitos cibernéticos. Estas entidades elaborarán informes anuales para el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos, con el objetivo de contribuir a una orientación de las decisiones.

Artículo 23. Vigencia y derogatorias. La presente ley rige a partir de su sanción y publicación, y deroga todas las normas que le sean contrarias.

Del Honorable Congresista,



CARLOS EDUARDO BUEVARA VILLABÓN
Senador de la República