



GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXVII - N° 261

Bogotá, D. C., miércoles, 16 de mayo de 2018

EDICIÓN DE 30 PÁGINAS

DIRECTORES:

GREGORIO ELJACH PACHECO
SECRETARIO GENERAL DEL SENADO
www.secretariassenado.gov.co

JORGE HUMBERTO MANTILLA SERRANO
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

CÁMARA DE REPRESENTANTES

PONENCIAS

PONENCIA PARA PRIMER DEBATE AL PROYECTO DE LEY NÚMERO 201 DE 2018 SENADO, 219 DE 2018 CÁMARA

por la cual se reglamenta lo previsto en el párrafo 5° del artículo 361 de la Constitución Política relativo a los programas de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.

Doctores

MANUEL GUILLERMO MORA JARAMILLO

Presidente Comisión Quinta

Senado de la República

ÁNGEL MARÍA GAITÁN

Presidente Comisión Quinta

Cámara de Representantes

Honorables Presidentes:

Atendiendo la honrosa tarea que se nos ha encomendado, y en cumplimiento del mandato constitucional y de lo dispuesto por la Ley 5ª de 1992, por la cual se expide el Reglamento del Congreso de la República, nos permitimos rendir informe de ponencia para primer debate en las Comisiones Conjuntas del Congreso de la República, del **Proyecto de ley número 201 de 2018 Senado, 219 de 2018 Cámara**, por la cual se regula lo previsto en el párrafo 5° del artículo 361 de la Constitución Política relativo a los programas y proyectos de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.

I. ANTECEDENTES DEL TRÁMITE

El día 3 de abril de 2018, el Gobierno nacional, por medio del Ministro de Hacienda y Crédito Público, radicó en la Secretaría General del Senado de la República el proyecto de ley “por la cual se

*regula lo previsto en el párrafo 5° del artículo 361 de la Constitución Política relativo a los programas y proyectos de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías”, con el cumplimiento de los requisitos formales exigidos para el efecto por la Constitución Política, el cual fue publicado en la **Gaceta del Congreso** número 119 de 2018.*

El mencionado proyecto de ley se presentó teniendo en cuenta lo siguiente:

El 30 de noviembre de 2016, el honorable Congreso de la República refrendó el Acuerdo Final para la Terminación del Conflicto y la Construcción de una Paz Estable y Duradera entre el Gobierno nacional y el Grupo Fuerzas Armadas Revolucionarias de Colombia, Ejército del Pueblo (FARC-EP), en adelante, el Acuerdo Final.

El numeral 6.1.2. del Acuerdo Final estableció las “*Medidas para incorporar la implementación de los acuerdos con recursos territoriales*”, dentro de las cuales fijó la siguiente:

“Se promoverán mecanismos y medidas para que con recursos del Sistema General de Participaciones y el Sistema General de Regalías se contribuya a financiar la implementación de los acuerdos, incluyendo los territorios priorizados para los planes de acción para la transformación regional de los PDET. Los recursos de regalías serán una fuente más de las diferentes fuentes para la implementación del Acuerdo en los territorios, para que estos proyectos fortalezcan el desarrollo de sus municipios y departamentos”.

A partir de lo anterior y en el marco del procedimiento legislativo especial para la paz¹, el

¹ Definido mediante el Acto Legislativo 01 de 2016.

Congreso de la República expidió el Acto Legislativo número 04 de 2017 “por el cual se adiciona el artículo 361 de la Constitución Política”, para modificar y adicionar algunas disposiciones constitucionales sobre el Sistema General de Regalías (SGR). Dentro de dichas medidas, se establecieron reglas para dinamizar la ejecución de los recursos del Fondo de Ciencia, Tecnología e Innovación (FCTeI) del SGR, adicionando el parágrafo 5° al artículo 361 de la Constitución Política, el cual se transcribe a continuación:

“Parágrafo 5°. Los programas o proyectos de inversión que se financiarán con los recursos del Fondo de Ciencia, Tecnología e Innovación, serán definidos por el respectivo Órgano Colegiado de Administración y Decisión, a través de convocatorias públicas abiertas y competitivas, articuladas con los correspondientes planes de desarrollo. Para la presentación y ejecución de los proyectos la entidad deberá ser parte del Sistema Nacional de Ciencia, Tecnología e Innovación. Los programas o proyectos aprobados serán ejecutados por las entidades que los presentaron en la convocatoria.

Lo establecido en el presente parágrafo regirá desde la entrada en vigencia de la ley que lo reglamente”.

Este parágrafo surgió a partir de las necesidades de inversión en ciencia, tecnología e innovación pactadas en el Acuerdo Final, y previa realización de escenarios de socialización con la comunidad científica, congresistas, alcaldes, gobernadores, entidades del Estado y otros actores locales y nacionales, que hicieron evidente la necesidad de abordar y solucionar las problemáticas relativas a la ejecución de los recursos del Fondo de Ciencia, Tecnología e Innovación (FCTeI).

En ese sentido, se vio la necesidad de incorporar en el Acto Legislativo 04 de 2017, una modificación a las reglas del FCTeI con el fin de que las entidades que formularan los proyectos pudieran ser las ejecutoras de los mismos, garantizando, además, la realización de convocatorias públicas abiertas y competitivas, en las que pudieran participar tanto entidades públicas como privadas.

La aplicación de estas nuevas reglas, se condicionaron en el citado acto legislativo a la reglamentación que para el efecto expidiera el legislador, razón por la cual se presenta al Congreso de la República el presente proyecto de ley que reglamenta el parágrafo 5° del artículo 361 de la Constitución Política.

1. Antecedentes sobre las entidades ejecutoras de proyectos de ciencia, tecnología e innovación

Como se ha señalado, uno de los principales objetivos del parágrafo 5° del artículo 361 de la Constitución Política adicionado por el Acto Legislativo 04 de 2017 que se pretende regular mediante el presente proyecto de ley, es elegir los proyectos de inversión que se financian con recursos del FCTeI a través de convocatorias públicas abiertas

y competitivas, en donde participen las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e Innovación.

En ese sentido, se considera pertinente exponer en dos capítulos, por una parte, los resultados del desempeño en la gestión a cargo de las entidades ejecutoras de los proyectos financiados con recursos del SGR, en donde las entidades especializadas en ciencia, tecnología e innovación son las que cuentan con un desempeño sobresaliente, frente a las gobernaciones que no han demostrado tener una buena gestión. En el segundo capítulo, se explica de forma general cuáles son los actores y entidades especializados en actividades científicas, tecnológicas y de innovación.

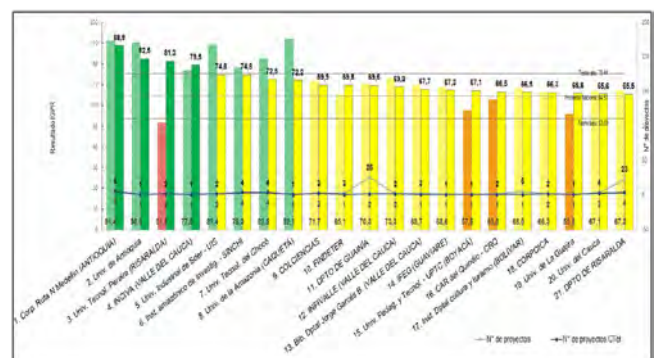
1.1. Entidades públicas

Según datos de la Secretaría Técnica del OCAD del FCTeI, el 71% de los proyectos aprobados actualmente tienen como ejecutor a la correspondiente gobernación que los presentó.

De acuerdo con el Índice de Gestión de Proyectos de Regalías (IGPR), herramienta del Sistema de Monitoreo, Seguimiento, Control y Evaluación (SMSCE) para medir y valorar trimestralmente la gestión de las entidades ejecutoras de los proyectos financiados con recursos del SGR², las gobernaciones de entidades territoriales no se destacan por su desempeño en la ejecución de los proyectos a su cargo.

Entre 64 entidades ejecutoras evaluadas, ninguna gobernación fue calificada con un desempeño sobresaliente y sólo dos contaron con calificación de desempeño “medio”, ubicándose la gobernación mejor calificada en el puesto 11. Con bajo desempeño se encuentran siete gobernaciones y 23 con desempeño crítico (ver gráficas 1, 2 y 3).

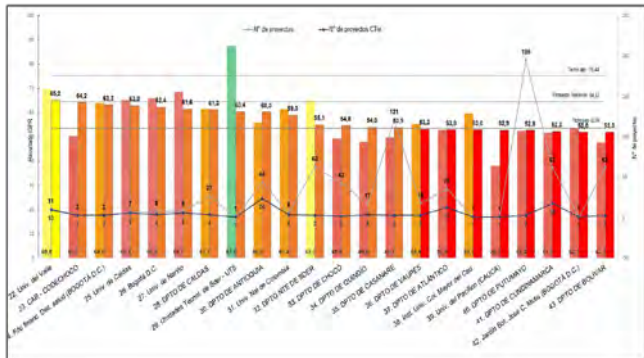
Gráfico 1. Índice de Gestión de Proyectos de Regalías - Entidades CTeI. Entidades 1-21. Corte septiembre 30 de 2017.



Fuente: Departamento Nacional de Planeación

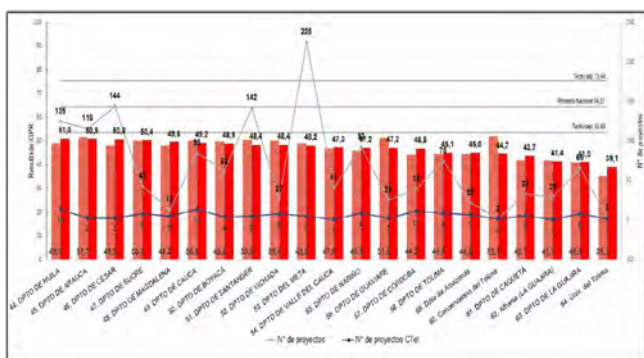
² El IGPR es calculado trimestralmente por el Departamento Nacional de Planeación (DNP) a partir de la información reportada en el SMSCE, con base en dos dimensiones: gestión administrativa y gestión del desempeño de los proyectos. A la primera se asocian las categorías de transparencia y “sin medidas del SMSCE” y a la segunda se asocian los criterios de eficiencia y eficacia.

Gráfico 2. Resultados del IGPR –desempeño sobresaliente y medio Índice de Gestión de Proyectos de Regalías– Entidades CTeI. Entidades 22-43. Corte septiembre 30 de 2017



Fuente: Departamento Nacional de Planeación

Gráfico 3. Resultados del IGPR – desempeño sobresaliente y medio Índice de Gestión de Proyectos de Regalías- Entidades CTeI. Entidades 44-62. Corte septiembre 30 de 2017



Fuente: Departamento Nacional de Planeación

En la posición opuesta, se encuentran las entidades especializadas en CTeI, que son las únicas cuatro con desempeño sobresaliente en el citado índice.

En el mismo sentido, en el ranking de las 10 mejor calificadas a través del SMSCE, 9, corresponden a entidades de este tipo, es decir, especializadas en CTeI.

Este resultado es entonces coherente con el hecho de que los proyectos de ciencia, tecnología e innovación tienen diferentes particularidades y especificidades, que demandan capacidades especializadas y experiencia calificada para su adecuado manejo y gestión (ejecución del proyecto).

Así, el proyecto de ley que se presenta reviste gran importancia, pues la aplicación de las modificaciones introducidas mediante el parágrafo 5° del artículo 361 de la Constitución Política, permiten la participación desde la presentación de los proyectos hasta su ejecución, de entidades especializadas en CTeI³, exigiéndoles hacer parte del Sistema Nacional de Ciencia, Tecnología e Innovación.

³ En cuanto a mejorar la ejecución de los recursos de dicho fondo a través de un mecanismo de convocatoria pública, abierta y competitiva para seleccionar las mejores propuestas y proponentes, al tiempo que se asegura que las entidades que presenten los proyectos de inversión al OCAD sean las que los ejecuten.

1.2. Actores y entidades especializados en actividades científicas, tecnológicas y de innovación

La primera experiencia en procesos de reconocimiento de entidades especializadas en CTeI en el país, se dio en 1991 cuando Colciencias, mediante convocatoria dirigida a grupos de ciencia y tecnología tuvo como propósito identificar los “grupos estrella o de referencia” que tendrían prioridad para la asignación de recursos. Este proceso fue repetido en los años 1996, 1997 y 1998.

En el año 2001 surgieron las definiciones de centro de investigación, grupo de investigación y centro de desarrollo tecnológico y se establecieron las condiciones de su reconocimiento, las cuales fueron actualizadas en 2010, 2012 y 2017. Desde entonces, las convocatorias a estos actores han sido llevadas a cabo de manera periódica.

En este contexto, y con el propósito de promover un ambiente favorable para el ordenamiento del Sistema Nacional de Ciencia Tecnología e Innovación (SNCTeI), Colciencias adoptó mediante la Resolución número 1473 de 2016 la política de “Actores del Sistema Nacional de Ciencia, Tecnología e Innovación”.

Esta política surgió como respuesta a la necesidad de reconocer a actores de creciente relevancia para el SNCTeI, como los centros de ciencia, las oficinas de transferencia de resultados de investigación, las incubadoras de empresas y los centros regionales de productividad, entre otros.

Así, los procesos de reconocimiento cobran especial importancia en este punto, en cuanto constituyen la base para la participación de estos actores en convocatorias de Colciencias y otras entidades.

De esta manera, incorporando los principios de especialización y focalización, la política de “Actores del Sistema Nacional de Ciencia, Tecnología e Innovación” ofrece una serie de conceptualizaciones, claras (pero flexibles), para caracterizar el rol de los actores del SNCTeI a partir de la identificación de sus actividades principales y complementarias, así como de sus principales resultados.

Los actores contemplados inicialmente, pueden agruparse por la afinidad de su objeto social como se muestra a continuación:

Gráfica 4. Actores del SNCTeI agrupados por afinidad en su objeto social

Generación de conocimiento científico	Desarrollo tecnológico y transferencia de	Innovación y productividad	Mentalidad y Cultura de CTeI
<ul style="list-style-type: none"> Investigadores Grupos de investigación Centros e institutos de investigación 	<ul style="list-style-type: none"> Centros de desarrollo tecnológico Oficinas de Transferencia de Resultados de Investigación (OTRI) 	<ul style="list-style-type: none"> Empresas Altamente Innovadoras (EAI) Unidades empresariales de I-D+i Incubadoras de empresas de base tecnológicas Centros de innovación y productividad Parques científicos, tecnológicos o de innovación 	<ul style="list-style-type: none"> Centros de Ciencia Organizaciones que fomentan el uso y apropiación de la CTeI

Fuente: Colciencias.

Las Universidades por su parte, deben considerarse también como un actor de gran relevancia en el SNCTeI, pues son instituciones que acogen un número significativo de los actores enlistados, principalmente los denominados investigadores y grupos de investigación.

Por lo tanto, además de proponer una conceptualización para los actores más representativos de la CTeI en el país, Colciencias actualizó el proceso de reconocimiento para un conjunto específico de cinco actores en primera instancia⁴:

- Centros o institutos de investigación dependientes y/o autónomos.
- Centros e institutos públicos de I+D⁵.
- Centros de desarrollo tecnológico.
- Centros de innovación y de productividad.

- Unidades empresariales de I+D+i.
- Centros de ciencia.

Lo anterior corrobora el nivel de especialización y la especificidad de las capacidades que desarrollan individuos e instituciones en el área de la CTeI, haciendo que sean sus recursos y experiencia, factores que los habiliten para ejecutar de manera rigurosa y técnica los proyectos del FCTeI del SGR.

Un balance de las entidades que cuentan con actores reconocidos (grupos, centros, unidades de I+D+i), muestra que existen más de 1.000 entidades especializadas en CTeI, distribuidas en las seis regiones, que tienen la capacidad para formular y ejecutar proyectos del FCTeI (ver tabla número 2). Aproximadamente un 40% de las entidades se ubican en la región Centro-Oriente, seguida por la región Eje Cafetero con un 20%.

Tabla 2. Distribución regional de entidades especializadas en CTeI

Región	Número de entidades con grupos de investigación o investigadores	Número de centros autónomos*	Número de centros de investigación e institutos públicos	Número de entidades con unidades empresariales de I+D+i
Caribe (Atlántico; Bolívar; Cesar; Córdoba; La Guajira; Magdalena; San Andrés, Providencia y Santa Catalina; Sucre)	192		3	1
Centro-Oriente (Boyacá, Cundinamarca, Norte de Santander, Santander, Bogotá D.C.)	520	18	24	21
Eje Cafetero (Antioquia, Caldas, Quindío, Risaralda)	249	4	5	19
Pacífico (Cauca, Chocó, Nariño, Valle del Cauca)	167	3	4	4
Centro-Sur (Amazonas, Caquetá, Huila, Putumayo, Tolima)	58	3		
Llano (Arauca, Casanare, Guainía, Guaviare, Meta, Vaupés, Vichada)	38	1		
Total	1224	29	36	45

* Incluye centros de desarrollo tecnológico, de innovación

Notas: 1. Algunas entidades pueden estar incluida en más de una columna. 2. Entidades reconocidas a 1° de marzo de 2018.

Fuente: Colciencias

En este sentido, el proyecto de ley, en cumplimiento de lo dispuesto en el Acto Legislativo 04 de 2017, busca que de forma competitiva las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e innovación, puedan presentar y ejecutar los programas o proyectos de inversión que se financiarán con los recursos del FCTeI del SGR.

II. EL PROYECTO DE LEY

El proyecto de ley radicado por el Gobierno nacional propone reglamentar el parágrafo 5° del

artículo 361 de la Constitución Política, relativo a los programas de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, con la siguiente estructura:

Artículo 1°. Objeto.

Artículo 2°. Convocatorias públicas abiertas y competitivas.

Artículo 3°. Entidades del Sistema Nacional de Ciencia, Tecnología e Innovación.

Artículo 4°. Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación.

Artículo 5°. Condiciones de las convocatorias.

Artículo 6°. Ejecución de los programas y proyectos.

Artículo 7°. Del giro y la ordenación del gasto.

Artículo 8°. Régimen de transición.

Artículo 9°. Remisión normativa.

Artículo 10. Vigencia.

⁴ Cabe señalar, que este conjunto de actores reconocidos puede ser ampliado cuando se considere pertinente, de acuerdo con las necesidades del Sistema y los objetos de la política.

⁵ Entidades adscritas y/o vinculadas a Ministerios, Departamentos Administrativos, Unidades, Agencias o entidades descentralizadas de orden nacional, que han sido creadas para apoyar el cumplimiento de su misión institucional y mejorar la calidad técnica de las intervenciones con base en la generación de conocimiento científico, el desarrollo y absorción de tecnología.

El artículo primero contiene el *Objeto* del proyecto, consistente en establecer un régimen especial para las convocatorias públicas, abiertas y competitivas, mediante las cuales se van a financiar los programas y proyectos de inversión con recursos del Fondo de Ciencia, Tecnología e innovación (FCTeI) del Sistema General de Regalías (SGR), fijando a su vez, las reglas para el giro y ordenación del gasto de dichos recursos, de acuerdo con lo establecido en el parágrafo 5° del artículo 361 de la Constitución Política.

El artículo segundo se titula *Convocatorias públicas abiertas y competitivas*, en el cual se señala que: (i) los programas o proyectos de inversión que se financien con recursos del FCTeI del SGR, serán definidos por el Órgano Colegiado de Administración y Decisión (OCAD) de Ciencia, Tecnología e Innovación, a través de convocatorias públicas, abiertas y competitivas; y (ii) que para las convocatorias, la Secretaría Técnica del OCAD realizará invitaciones públicas y establecerá las condiciones que se deben cumplir para la presentación de las iniciativas a ser financiadas con estos recursos.

Seguidamente, el artículo tercero se refiere a las *Entidades del Sistema de Ciencia, Tecnología e Innovación*, en la medida en que serán las habilitadas para participar en las convocatorias públicas abiertas y competitivas del FCTeI. Se señala que hacen parte del Sistema, aquellas entidades que se encuentren constituidas en el territorio nacional, que desarrollen actividades de Ciencia, Tecnología e Innovación; y que cuenten con la idoneidad y trayectoria. Todo lo anterior, de conformidad con lo dispuesto por el Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), de acuerdo con el reglamento que expida el Gobierno nacional para el efecto.

El artículo cuarto se titula *Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación*, e indica que Colciencias, en coordinación con el Departamento Nacional de Planeación, los departamentos y el Distrito Capital, estructurarán Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación (PAED) donde se establecerán los focos, líneas programáticas, tipologías de programas y tipologías de proyectos, para el cumplimiento de las metas señaladas en el Plan Nacional de Desarrollo.

El artículo quinto establece las *Condiciones de las convocatorias*, señalando que las mismas deberán: (i) estructurarse a partir de los PAED; (ii) establecer las condiciones de participación, las cuales contendrán como mínimo: los participantes a los que se dirige, las características de los programas y proyectos, los rangos de financiación y los criterios de selección y; (ii) considerar dentro de los criterios de selección, por lo menos: la idoneidad y trayectoria del proponente, calidad técnico-científica de los programas y proyectos, y su contribución al desarrollo regional y a las metas del país en materia de ciencia, tecnología e innovación.

El artículo sexto, titulado *Ejecución de los programas y proyectos*, establece que los ejecutores de los programas y proyectos, serán responsables (i) por la correcta ejecución de los recursos asignados, y (ii) por el suministro y registro de la información requerida por el Sistema de Monitoreo, Seguimiento Control y Evaluación (SMSCE) del SGR.

Asimismo, el artículo dispone que cuando los ejecutores sean entidades de naturaleza jurídica privada, Colciencias, con cargo a los recursos del programa o proyecto, vigilará la correcta ejecución del programa o proyecto directamente, o a través de terceros.

El artículo séptimo se refiere al *Giro y ordenación del gasto* de los recursos, señalando que las entidades designadas como ejecutoras de programas o proyectos de inversión, deberán hacer uso del Sistema de Presupuesto y Giro de Regalías (SPGR), para realizar la gestión de ejecución de estos recursos y ordenar el pago de las obligaciones directamente desde la Cuenta Única del SGR a las cuentas bancarias de los destinatarios finales.

El artículo precisa que cuando las entidades designadas como ejecutoras sean de naturaleza jurídica privada, Colciencias autorizará el giro de los recursos, función que en ningún momento generará gastos adicionales con cargo al Sistema General de Regalías y se harán con cargo a las apropiaciones que se incorporan en el presupuesto de la entidad.

Adicionalmente, se establece que corresponde al representante legal de la entidad ejecutora del proyecto, a quien haga sus veces, o a su delegado del nivel directivo, ordenar el gasto sobre las apropiaciones que se incorporan al presupuesto de la entidad y en consecuencia, serán responsables disciplinaria, fiscal y penalmente por el manejo de tales apropiaciones.

Finalmente, el artículo señala que el Ministerio de Hacienda y Crédito Público, adelantará los giros de los recursos del SGR observando los montos presupuestados, las disponibilidades de recursos en caja existentes y los requisitos que se establezcan.

Por su parte, el artículo octavo establece un *Régimen de transición*, según el cual, los programas o proyectos que se encuentren registrados en el banco de programas y proyectos del Sistema General de Regalías SUIFP-SGR, contarán con un plazo máximo de seis meses, contados desde la promulgación de la ley, para su viabilización, priorización y aprobación por parte del OCAD. Vencido este plazo, los programas y proyectos deberán tramitarse de acuerdo con las disposiciones contenidas en el proyecto de ley.

El artículo noveno realiza una *Remisión normativa*, al señalar que, en lo no previsto en el proyecto de ley, se aplicarán las normas del SGR y del SMSCE.

Finalmente, el artículo décimo define la entrada en vigencia del proyecto de ley, a partir de la fecha de su promulgación.

III. REUNIONES Y ESCENARIOS DE SOCIALIZACIÓN DEL PROYECTO DE LEY

1. Presentación del proyecto de ley en el Congreso: 17 de abril de 2018

El 17 de abril de 2018 se llevó a cabo la presentación del proyecto de ley en el Congreso de la República, a la cual asistieron, entre otros, el Ministro de Hacienda y Crédito Público y el Director del Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), con el propósito de socializar y resolver inquietudes relacionadas con el contenido del proyecto de ley, así como de conocer las apreciaciones de los honorables Congresistas sobre la propuesta.

En el curso de la reunión, el Ministro de Hacienda presentó el proyecto, expuso las líneas generales y objetivos más relevantes de la propuesta, y se resolvieron preguntas puntuales sobre los recursos del Fondo de Ciencia, Tecnología e Innovación, la participación de universidades públicas y de las entidades territoriales en las convocatorias, la vigilancia de los programas y proyectos que ejecuten las entidades privadas, las normas aplicables a los proyectos que se encuentran en proceso de aprobación ante el OCAD y que estén en ejecución al momento de la expedición del proyecto de ley, la vigencia de los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e innovación (PAED), entre otros.

2. Mesa de trabajo con la Federación Nacional de Departamentos: 18 de abril de 2018

La Federación Nacional de Departamentos invitó a los honorables Congresistas a llevar una mesa de

trabajo que se adelantó el día 18 de abril de 2018. En esa oportunidad, los gobernadores expusieron sus principales preocupaciones sobre el proyecto de ley radicado, que pueden resumirse así:

- 2.1. Posible interpretación de que los recursos del Fondo de Ciencia, Tecnología e Innovación se centralicen perdiendo la asignación presupuestal por departamento.
- 2.2. Exclusión de los departamentos en la presentación de programas y proyectos a las convocatorias públicas, abiertas y competitivas.
- 2.3. Pérdida de vigencia de los PAED que a la fecha se encuentran estructurados.

Estos comentarios fueron analizados para proponer las modificaciones al articulado que se proponen en la presente ponencia.

3. Reunión de ponentes: 25 de abril de 2018

Con el fin de revisar las diferentes propuestas y observaciones presentadas sobre el articulado del proyecto tanto por los honorables Congresistas como por otros interesados en el proyecto, se llevó a cabo el análisis del proyecto por parte de los ponentes, proponiendo modificaciones concretas sobre el articulado, tal como se expone en el siguiente punto de la ponencia.

IV. JUSTIFICACIONES AL PLIEGO DE MODIFICACIONES

Se propone modificar los artículos 2°, 3°, 4°, 5° y 8° del proyecto de ley, de acuerdo con las razones que se exponen a continuación:

Texto radicado	Modificación propuesta	Justificación
<p>Artículo 2°. Convocatorias públicas abiertas y competitivas. Los programas o proyectos de inversión que se financien con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, serán definidos por el Órgano Colegiado de Administración y Decisión (OCAD) de Ciencia, Tecnología e Innovación, a través de convocatorias públicas, abiertas y competitivas. Para las convocatorias, la Secretaría Técnica del OCAD realizará invitaciones públicas y establecerá las condiciones que se deben cumplir para la presentación de estas iniciativas.</p>	<p>Artículo 2°. Convocatorias públicas abiertas y competitivas. Los programas o proyectos de inversión que se financien con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, serán definidos por el Órgano Colegiado de Administración y Decisión (OCAD) de Ciencia, Tecnología e Innovación, a través de convocatorias públicas, abiertas y competitivas. Para las convocatorias, la Secretaría Técnica del OCAD de Ciencia, Tecnología e Innovación realizará invitaciones públicas y establecerá las condiciones que se deben cumplir para la presentación de estas iniciativas.</p> <p><u>En todo caso, las convocatorias deberán ajustarse a los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación y a los recursos asignados a cada departamento en el Fondo de Ciencia, Tecnología e Innovación.</u></p> <p><u>Parágrafo. Los departamentos podrán solicitarle a la Secretaría Técnica del OCAD de Ciencia, Tecnología e Innovación la realización de las convocatorias, caso en el cual podrán proponer las condiciones que se deben cumplir para la presentación de los programas o proyectos, conforme a lo establecido en el artículo 5° de la presente ley.</u></p>	<p>1. Se aclara que el OCAD es de ciencia, tecnología e innovación.</p> <p>2. Se precisa que las convocatorias siempre deben estar ajustadas a los PAED, de tal forma que correspondan a las necesidades en ciencia, tecnología e innovación de cada departamento.</p> <p>3. Se aclara que los recursos del Fondo de Ciencia, Tecnología e Innovación (FCTeI) seguirán siendo asignados a cada departamento.</p> <p>4. Parágrafo nuevo: permite que los departamentos soliciten a la Secretaría Técnica del OCAD la realización de convocatorias. En estos casos, los departamentos podrán proponer las condiciones de las convocatorias, siguiendo los lineamientos fijados por el artículo 5 del proyecto de ley (estar de acuerdo con los PAED, establecer las condiciones de participación y los criterios mínimos de selección).</p>
<p>Artículo 3°. Entidades del Sistema Nacional de Ciencia, Tecnología e Innovación. Solo podrán presentar y ejecutar programas o proyectos de inversión a los que se refiere la presente ley, las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e Innovación.</p>	<p>Artículo 3°. Entidades del Sistema Nacional de Ciencia, Tecnología e Innovación. Solo podrán presentar y ejecutar programas o proyectos de inversión a los que se refiere la presente ley, las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e Innovación, de conformidad con lo establecido en el artículo 20 de la Ley 1286 de 2009 o la que la modifique o sustituya.</p>	<p>La modificación propuesta responde a la preocupación sobre si las entidades territoriales pueden ser parte del SNCTI y si por lo tanto, pueden presentar programas o proyectos a financiarse con recursos del Fondo (FCTeI).</p> <p>Para el efecto, se ajusta la redacción, para que se aplique lo dispuesto en el artículo 20 de la Ley</p>

Texto radicado	Modificación propuesta	Justificación
<p>Hacen parte del Sistema Nacional de Ciencia, Tecnología e Innovación, las entidades constituidas en el territorio nacional que desarrollen actividades de ciencia, tecnología e innovación y que cuenten con la idoneidad y la trayectoria, de conformidad con lo dispuesto por el Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), de acuerdo con el reglamento que expida el Gobierno nacional para el efecto.</p>	<p>Hacen parte del Sistema Nacional de Ciencia, Tecnología e Innovación, las entidades constituidas en el territorio nacional que desarrollen actividades de ciencia, tecnología e innovación y que cuenten con la idoneidad y la trayectoria, de conformidad con lo dispuesto por el Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), de acuerdo con el reglamento que expida el Gobierno nacional para el efecto.</p>	<p>1286 de 2009, el cual dispone quiénes componen el Sistema Nacional de Ciencia, Tecnología e Innovación, dentro del cual se encuentran las organizaciones públicas. Adicionalmente, el parágrafo 2° del referido artículo 20 dispone que las Asambleas Departamentales, los Concejos Distritales y los Concejos Municipales podrán ordenar la creación de unidades regionales de investigación científica e innovación con sus fondos regionales de fomento.</p>
<p>Artículo 4°. Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación. Colciencias, en coordinación con el Departamento Nacional de Planeación, los departamentos y el Distrito Capital, estructurarán Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación (PAED) donde se establecerán los focos, líneas programáticas, tipologías de programas y tipologías de proyectos, para el cumplimiento de las metas señaladas en el Plan Nacional de Desarrollo y los planes de desarrollo de las entidades territoriales.</p>	<p>Artículo 4°. Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación. Colciencias, en coordinación con el Departamento Nacional de Planeación, los departamentos y el Distrito Capital, estructurarán Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación (PAED) donde se establecerán los focos, y líneas programáticas; tipologías de programas y tipologías de proyectos, para el cumplimiento de las metas señaladas en el Plan Nacional de Desarrollo y los planes de desarrollo de las entidades territoriales.</p> <p><u>Parágrafo transitorio. Lo establecido en el presente artículo no afectará la vigencia de los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación, que se encuentren estructurados a la fecha de expedición de la presente ley.</u></p>	<p>1. Se elimina la referencia a las tipologías de programas y tipologías de proyectos para la estructuración de los PAED, pues son asuntos que puede ser desarrollados por el reglamento cuando se requieran.</p> <p>2. Parágrafo nuevo transitorio: busca aclarar que el proyecto de ley no va a afectar la vigencia de los PAED que ya se encuentran suscritos.</p>
<p>Artículo 5°. Condiciones de las convocatorias. Las convocatorias públicas abiertas y competitivas del Sistema General de Regalías (SGR) deberán:</p> <ol style="list-style-type: none"> 1. Estructurarse a partir de los PAED. 2. Establecer las condiciones de participación, las cuales contendrán, como mínimo: los participantes a los que se dirige, las características de los programas y proyectos, los rangos de financiación y los criterios de selección. 3. Considerar dentro de los criterios de selección, por lo menos: la idoneidad y trayectoria del participante, la calidad técnico-científica de los programas y proyectos, y su contribución al desarrollo regional y a las metas del país en materia de ciencia, tecnología e innovación. 	<p>Artículo 5°. Condiciones de las convocatorias. Las convocatorias públicas abiertas y competitivas del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías (SGR), deberán:</p> <ol style="list-style-type: none"> 1. Estructurarse a partir de los PAED. 2. Establecer las condiciones de participación, las cuales contendrán, como mínimo: los participantes a los que se dirige, las características de los programas y proyectos, los rangos de financiación y los criterios de selección. 3. Considerar dentro de los criterios de selección, por lo menos: la idoneidad y trayectoria del participante, la calidad técnico-científica de los programas y proyectos, y su contribución al desarrollo regional y a la creación y fortalecimiento de las correspondientes capacidades propias las metas del país en materia de ciencia, tecnología e innovación. 	<p>1. Se precisa que las convocatorias corresponden al Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.</p> <p>2. Se establece que dentro de los criterios de selección debe considerarse la creación y fortalecimiento de las capacidades propias de las regiones en materia de ciencia, tecnología e innovación.</p>
<p>Artículo 8°. Régimen de transición. Los programas y proyectos que se pretendan financiar con recursos del Fondo de Ciencia, Tecnología e Innovación del SGR, que al momento de la expedición de la presente ley se encuentren registrados en el Banco de Programas y Proyectos del Sistema General de Regalías (SUIFP-SGR), tendrán un plazo máximo de seis meses, contados desde la promulgación de la presente ley, para su viabilización, priorización y aprobación por parte del Órgano Colegiado de Administración y Decisión. Vencido el plazo, estos programas y proyectos deberán tramitarse de acuerdo con las disposiciones contenidas en la presente ley.</p>	<p>Artículo 8°. Régimen de transición. Los programas y proyectos que se pretendan financiar con recursos del Fondo de Ciencia, Tecnología e Innovación del SGR, que al momento de la expedición de la presente ley se encuentren registrados en el Banco de Programas y Proyectos del Sistema General de Regalías (SUIFP-SGR), podrán continuar con el trámite hasta el 31 de diciembre de 2019, como fecha máxima tendrán un plazo máximo de seis meses, contados desde la promulgación de la presente ley, para su viabilización, priorización y aprobación por parte del Órgano Colegiado de Administración y Decisión.</p> <p><u>Los departamentos podrán decidir cuáles de los proyectos y programas referidos en el inciso anterior no serán sometidos al régimen de transición, caso en el cual lo comunicarán a la Secretaría Técnica del OCAD.</u></p> <p><u>Vencido el plazo, estos programas y proyectos deberán tramitarse de acuerdo con las disposiciones contenidas en la presente ley.</u></p> <p><u>En todo caso, a partir del 01 de enero de 2020 todos los programas y proyectos deberán definirse a través de convocatorias, de acuerdo con las disposiciones establecidas en la presente ley.</u></p>	<p>1. Se establece un régimen de transición más amplio, de tal forma que coincida con la vigencia del periodo de gobierno de departamental, para facilitar el cumplimiento de las metas establecidas en los respectivos planes de desarrollo territoriales. Por lo tanto, se extiende la transición hasta el 31 de diciembre de 2019, dándole la posibilidad a los departamentos de renunciar a dicha transición para los programas y proyectos que quieran que sean definidos a través de convocatorias.</p> <p>Se aclara que en todo caso a partir del 01 de enero de 2020, todos los programas y proyectos del FC-Tel deberán definirse a través de las reglas previstas en el proyecto de ley (convocatorias).</p>

V. PLIEGO DE MODIFICACIONES

Con base en lo expuesto anteriormente se realizaron las siguientes modificaciones a la propuesta del articulado propuesto por el Gobierno nacional.

El artículo 2° quedará así:

Artículo 2°. Convocatorias públicas abiertas y competitivas. Los programas o proyectos de inversión que se financien con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, serán definidos por el Órgano Colegiado de Administración y Decisión (OCAD) de Ciencia, Tecnología e Innovación, a través de convocatorias públicas, abiertas y competitivas.

Para las convocatorias, la Secretaría Técnica del OCAD **de Ciencia, Tecnología e Innovación** realizará invitaciones públicas y establecerá las condiciones que se deben cumplir para la presentación de estas iniciativas.

En todo caso, las convocatorias deberán ajustarse a los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación y a los recursos asignados a cada departamento en el Fondo de Ciencia, Tecnología e Innovación.

Parágrafo. Los departamentos podrán solicitarle a la Secretaría Técnica del OCAD de Ciencia, Tecnología e Innovación la realización de las convocatorias, caso en el cual podrán proponer las condiciones que se deben cumplir para la presentación de los programas o proyectos, conforme a lo establecido en el artículo 5° de la presente ley.

El artículo 3° quedará así:

Artículo 3°. Entidades del Sistema Nacional de Ciencia, Tecnología e Innovación. Solo podrán presentar y ejecutar programas o proyectos de inversión a los que se refiere la presente ley, las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e Innovación, **de conformidad con lo establecido en el artículo 20 de la Ley 1286 de 2009 o la que la modifique o sustituya.**

Hacen parte del Sistema Nacional de Ciencia, Tecnología e Innovación, las entidades constituidas en el territorio nacional que desarrollen actividades de ciencia, tecnología e innovación y que cuenten con la idoneidad y la trayectoria, de conformidad con lo dispuesto por el Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), de acuerdo con el reglamento que expida el Gobierno nacional para el efecto.

El artículo 4° quedará así:

Artículo 4°. Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación. Colciencias, en coordinación con el Departamento Nacional de Planeación, los departamentos y el Distrito Capital, estructurarán Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación (PAED) donde

se establecerán los focos; ~~y~~ líneas programáticas; ~~tipologías de programas y tipologías de proyectos~~, para el cumplimiento de las metas señaladas en el Plan Nacional de Desarrollo y los planes de desarrollo de las entidades territoriales.

Parágrafo transitorio. Lo establecido en el presente artículo no afectará la vigencia de los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación, que se encuentren estructurados a la fecha de expedición de la presente ley.

El artículo 5° quedará así:

Artículo 5°. Condiciones de las convocatorias. Las convocatorias públicas abiertas y competitivas **del Fondo de Ciencia, Tecnología e Innovación** del Sistema General de Regalías (SGR), deberán:

1. Estructurarse a partir de los PAED.
2. Establecer las condiciones de participación, las cuales contendrán, como mínimo: los participantes a los que se dirige, las características de los programas y proyectos, los rangos de financiación y los criterios de selección.
3. Considerar dentro de los criterios de selección, por lo menos: la idoneidad y trayectoria del participante, la calidad técnico-científica de los programas y proyectos, y su contribución al desarrollo regional **y a la creación y fortalecimiento de las correspondientes capacidades propias** las metas del país en materia de ciencia, tecnología e innovación.

El artículo 8° quedará así:

Artículo 8°. Régimen de transición. Los programas y proyectos que se pretendan financiar con recursos del Fondo de Ciencia, Tecnología e Innovación del SGR, que al momento de la expedición de la presente ley se encuentren registrados en el Banco de Programas y Proyectos del Sistema General de Regalías (SUIFP-SGR), **podrán continuar con el trámite hasta el 31 de diciembre de 2019, como fecha máxima tendrán un plazo máximo de seis meses, contados desde la promulgación de la presente ley,** para su viabilización, priorización y aprobación por parte del Órgano Colegiado de Administración y Decisión.

Los departamentos podrán decidir cuáles de los proyectos y programas referidos en el inciso anterior no serán sometidos al régimen de transición, caso en el cual lo comunicarán a la Secretaría Técnica del OCAD.

~~Vencido el plazo, estos programas y proyectos deberán tramitarse de acuerdo con las disposiciones contenidas en la presente ley.~~

En todo caso, a partir del 1° de enero de 2020 todos los programas y proyectos deberán definirse a través de convocatorias, de

acuerdo con las disposiciones establecidas en la presente ley.

PROPOSICIÓN

Por lo anteriormente expuesto, y por cumplir el proyecto de ley con los requisitos constitucionales, los ponentes nos permitimos proponer:

Dese primer debate al **Proyecto de ley número 201 de 2018 Senado, 219 de 2018 Cámara**, por la cual se reglamenta lo previsto en el párrafo 5° del artículo 361 de la Constitución Política relativo a los programas de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.

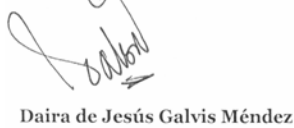
De los honorables Congresistas,

Comisión V Senado

Coordinadores:


Lidio García Turbay

Ponentes:


Daira de Jesús Galvis Méndez


Guillermo García Realpe


Maritza Martínez Aristizábal


Manuel Guillermo Mora Jaramill

Luis Emilio Sierra Grajales


Gloria Stella Díaz

Ernesto Macías Tovar

Jorge Enrique Robledo

Comisión V Cámara

Coordinadores:


Ángel María Gaitán Pulido

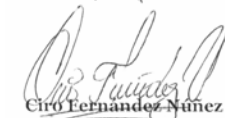

Alfredo Guillermo Molina Triana

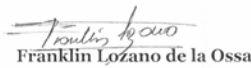

Arturo Yepes Alzate

Ponentes:


Inti Raúl Asprilla Reyes


Karen Violette Cure Corcione


Ciro Fernández Nuñez


Franklin Lozano de la Ossa

Rubén Darío Molano Piñeros


Crisanto Pizo Mazabuel

TEXTO PROPUESTO PARA PRIMER DEBATE AL PROYECTO DE LEY NÚMERO 201 DE 2018 SENADO, 219 DE 2018 CÁMARA

por la cual se regula lo previsto en el párrafo 5° del artículo 361 de la Constitución Política relativo a los programas y proyectos de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.

El Congreso de Colombia

DECRETA:

Artículo 1°. *Objeto.* La presente ley tiene por objeto regular lo previsto en el párrafo 5° del artículo 361 de la Constitución Política, relativo a los programas y proyectos de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.

Artículo 2°. *Convocatorias públicas abiertas y competitivas.* Los programas o proyectos de inversión que se financien con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, serán definidos por el Órgano Colegiado de Administración y Decisión (OCAD) de Ciencia, Tecnología e Innovación, a través de convocatorias públicas, abiertas y competitivas.

Para las convocatorias, la Secretaría Técnica del OCAD de Ciencia, Tecnología e Innovación realizará invitaciones públicas y establecerá las condiciones que se deben cumplir para la presentación de estas iniciativas.

En todo caso, las convocatorias deberán ajustarse a los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación y a los recursos asignados a cada departamento en el Fondo de Ciencia, Tecnología e Innovación.

Parágrafo. Los departamentos podrán solicitarle a la Secretaría Técnica del OCAD de Ciencia, Tecnología e Innovación la realización de las convocatorias, caso en el cual podrán proponer las condiciones que se deben cumplir para la presentación de los programas o proyectos, conforme a lo establecido en el artículo 5 de la presente ley.

Artículo 3°. *Entidades del Sistema Nacional de Ciencia, Tecnología e Innovación.* Solo podrán presentar y ejecutar programas o proyectos de inversión a los que se refiere la presente ley, las entidades que hagan parte del Sistema Nacional de Ciencia, Tecnología e Innovación, de conformidad con lo establecido en el artículo 20 de la Ley 1286 de 2009 o la que la modifique o sustituya.

Artículo 4°. *Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación.* Colciencias, en coordinación con el Departamento Nacional de Planeación, los departamentos y el Distrito Capital, estructurarán Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación (PAED) donde se establecerán los focos y líneas programáticas, para

el cumplimiento de las metas señaladas en el Plan Nacional de Desarrollo y los planes de desarrollo de las entidades territoriales.

Parágrafo transitorio. Lo establecido en el presente artículo no afectará la vigencia de los Planes y Acuerdos Estratégicos Departamentales en Ciencia, Tecnología e Innovación, que se encuentren estructurados a la fecha de expedición de la presente ley.

Artículo 5°. *Condiciones de las convocatorias.* Las convocatorias públicas abiertas y competitivas del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías (SGR), deberán:

1. Estructurarse a partir de los PAED.
2. Establecer las condiciones de participación, las cuales contendrán, como mínimo: los participantes a los que se dirige, las características de los programas y proyectos, los rangos de financiación y los criterios de selección.
3. Considerar dentro de los criterios de selección, por lo menos: la idoneidad y trayectoria del participante, la calidad técnico-científica de los programas y proyectos, y su contribución al desarrollo regional y a la creación y fortalecimiento de las correspondientes capacidades propias en materia de ciencia, tecnología e innovación.

Artículo 6°. *Ejecución de los programas y proyectos.* Los ejecutores de los programas y proyectos a los que se refiere esta ley serán responsables por la correcta ejecución de los recursos asignados al respectivo programa o proyecto de inversión, y por el suministro y registro de la información requerida por el Sistema de Monitoreo, Seguimiento, Control y Evaluación (SMSCE) del SGR.

Cuando los ejecutores sean entidades de naturaleza jurídica privada, Colciencias, con cargo a los recursos del programa o proyecto, vigilará la correcta ejecución del programa o proyecto directamente, o a través de terceros, en los términos del artículo 83 de la Ley 1474 de 2011, o la norma que la modifique o sustituya.

Artículo 7°. *Del giro y la ordenación del gasto.* Las entidades designadas como ejecutoras de programas o proyectos de inversión de los recursos provenientes del Fondo de Ciencia, Tecnología e Innovación del SGR deberán hacer uso del Sistema de Presupuesto y Giro de Regalías (SPGR), para realizar la gestión de ejecución de estos recursos y ordenar el pago de las obligaciones legalmente adquiridas directamente desde la Cuenta Única del SGR a las cuentas bancarias de los destinatarios finales.

Cuando las entidades designadas como ejecutoras de programas o proyectos de inversión de los recursos provenientes del Fondo de Ciencia, Tecnología e Innovación del SGR sean de naturaleza jurídica privada, Colciencias autorizará el giro de los recursos.

El Ministerio de Hacienda y Crédito Público - Dirección de Crédito Público y Tesoro Nacional

adelantará los giros de los recursos del SGR, observando los montos presupuestados, las disponibilidades de recursos en caja existentes y los requisitos que se establezcan.

Corresponde al representante legal de la entidad pública o privada ejecutora del proyecto o programa, a quien haga sus veces, o a su delegado del nivel directivo, ordenar el gasto sobre las apropiaciones que se incorporan al presupuesto de la entidad y, en consecuencia, serán responsables disciplinaria, fiscal y penalmente por el manejo de tales apropiaciones, en los términos de las normas que regulan la materia.

Artículo 8°. *Régimen de transición.* Los programas y proyectos que se pretendan financiar con recursos del Fondo de Ciencia, Tecnología e Innovación del SGR, que al momento de la expedición de la presente ley se encuentren registrados en el Banco de Programas y Proyectos del Sistema General de Regalías (SUIFP-SGR), podrán continuar con el trámite hasta el 31 de diciembre de 2019, como fecha máxima para su viabilización, priorización y aprobación por parte del Órgano Colegiado de Administración y Decisión.

Los departamentos podrán decidir cuáles de los proyectos y programas referidos en el inciso anterior no serán sometidos al régimen de transición, caso en el cual lo comunicarán a la Secretaría Técnica del OCAD.

En todo caso, a partir del 1° de enero de 2020 todos los programas y proyectos deberán definirse a través de convocatorias, de acuerdo con las disposiciones establecidas en la presente ley.

Artículo 9°. *Remisión normativa.* En lo no previsto en la presente ley, se aplicarán las normas del SGR y del SMSCE.

Artículo 10. *Vigencia.* La presente ley rige a partir de la fecha de su promulgación.

De los honorables Congressistas,

Comisión V Senado

Coordinadores:


Lidio García Turbay

Ponentes:


Daira de Jesús Galvis Méndez


Guillermo García Realpe


Maritza Martínez Aristizábal


Manuel Guillermo Mora Jaramillo


Luis Emilio Sierra Grajales

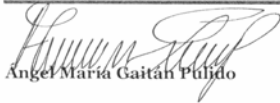

Gloria Stella Díaz


Ernesto Macías Tovar


Jorge Enrique Robledo

Comisión V Cámara

Coordinadores:



Ángel María Gaitán Pulido



Alfredo Guillermo Molina Triana



Arturo Yepes Alzate

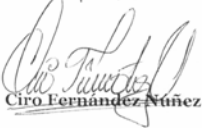
Ponentes:



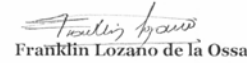
Inti Raúl Asprilla Reyes



Karen Violette Cure Corcione



Ciro Fernández Nuñez



Franklin Lozano de la Ossa



Rubén Darío Molano Piñeros



Crisanto Bizo Mazabuel

* * *

**PONENCIA PARA PRIMER DEBATE
AL PROYECTO DE LEY NÚMERO 230
DE 2018 CÁMARA, 58 DE 2017 SENADO**

por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001 en Budapest.

Bogotá, D. C., abril 24 de 2018

Señores

MESA DIRECTIVA

Comisión Segunda Constitucional Permanente

Honorable Cámara de Representantes

Ciudad

Referencia: Ponencia para primer debate al Proyecto de ley número 230 de 2018 Cámara, 58 de 2017 Senado, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest.

Cordial saludo:

En cumplimiento a la honrosa designación realizada por la Mesa Directiva de la Comisión Segunda Constitucional Permanente de la Honorable Cámara de Representantes, y de conformidad con lo establecido en el artículo 150 de la Ley 5ª de 1992, sometemos a consideración de los Honorables Representantes a la Cámara, el informe de ponencia para primer debate al **Proyecto de ley número 230 de 2018 Cámara, 58 de 2017 Senado, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest.**

I. TRÁMITE DEL PROYECTO

Origen: Gobierno nacional

Autores: Ministerio de Relaciones Exteriores, Ministerio de Justicia y del Derecho, Ministerio de

Defensa Nacional y Ministerio de las Tecnologías de la Información y las Comunicaciones.

Ponentes para primer y segundo debate en Senado: Honorables Senadores José David Name Cardozo, Jaime Enrique Durán Barrera

II. ANTECEDENTES

Esta iniciativa fue radicada el 1º de agosto de 2017, cumpliendo los requisitos formales exigidos para el efecto, conforme a lo establecido en el artículo 154 de la Constitución Política y el artículo 217 de la Ley 5ª de 1992.

Este Convenio sobre la Ciberdelincuencia o Convenio de Budapest, fue aprobado por el Comité de Ministros del Consejo de Europa el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1º de julio de 2004.

Posteriormente, el día 3 del mes de octubre de 2017, la Comisión Segunda del Honorable Senado de la República aprobó en su primer debate la presente iniciativa legislativa. Finalmente, el día 4 de abril de 2018 la Plenaria de esa misma Corporación dio su visto bueno a este proyecto de ley.

Así las cosas, el presente proyecto comienza su tránsito por la Cámara baja del Parlamento Colombiano.

III. JUSTIFICACIÓN DEL PROYECTO

De la necesidad del proyecto

Los ataques cibernéticos que han ocurrido recientemente, como lo fue el ciberataque identificado como WannaCry que tuvo lugar en el mes de mayo de 2017 (*Semana*, 2017); han evidenciado los peligros que representa la ciberdelincuencia. Colombia no ha sido ajena a dichos ataques y según datos proporcionados por el Ministerio de Defensa, en lo corrido del año 2017 han sido atendidos 5.500 ataques cibernéticos que han afectado especialmente al sector privado, sin olvidar que desde el año 2014 al 2017 se han contabilizado más de 30.000 ataques (*El Colombiano*, 2017).

Por lo anterior, resulta importante que nuestro país se involucre en los espacios internacionales que propician la cooperación para combatir y evitar la comisión de delitos cibernéticos.

Desde el año 2011 el Estado colombiano ha procurado adelantar acciones para enfrentar de forma efectiva la ciberdelincuencia, razón por la cual promulgó el Documento Conpes 3701 sobre Ciberseguridad y Ciberdefensa, el Documento Conpes 3854 de Política Nacional de Seguridad Digital, la Ley Estatutaria 1621 sobre inteligencia y contrainteligencia, e inició la gestión para adherirse al principal convenio internacional sobre la materia, a saber, el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, al cual fue invitado a adherirse el 11 de septiembre del año 2013.

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest es el primer tratado internacional que aborda la definición de los delitos

cometidos a través de redes informáticas, incluyendo la pornografía infantil y la violación a los derechos de autor; que adicionalmente, contiene normas sobre procedimiento, cooperación internacional, extradición y asistencia mutua.

A pesar de la antigüedad del Convenio (fue aprobado en el año 2001), su ratificación permitirá a Colombia participar en el único marco internacional vigente que aplica una política penal común con el fin de proteger los derechos de las personas frente a los ataques de ciberdelinquentes por medio de la cooperación internacional.

a) Contexto internacional

El crecimiento de las amenazas en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado. Esto lo que pone de manifiesto es la necesidad de desarrollar de forma estricta políticas de seguridad necesarias para establecer controles que permitan proteger tanto a la ciudadanía sociedad, como al el Estado y sus infraestructuras críticas, ante estas nuevas amenazas. Tales políticas de seguridad han de ser respaldadas por un adecuado marco normativo sustancial y procesal de naturaleza penal, para que su implementación sea efectiva.

Por esta razón, en noviembre de 2001, producto de una reunión internacional de expertos celebrada en Budapest, Hungría, se creó el único marco existente para aplicar una política penal común para proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de legislación adecuada y el fortalecimiento de la cooperación internacional. En la actualidad, este documento es considerado como el estándar mundial en esta materia.

Varios Estados europeos, junto a otras naciones como Estados Unidos, Japón, Canadá y Sudáfrica, vieron con interés el contenido del Convenio en virtud de que representaba una oportunidad valiosa para contar con un instrumento aplicable en todos los países del mundo y así lograr consenso internacional en la persecución de las nuevas formas de delincuencia ejecutadas a través de los medios telemáticos, considerando que más que cualquier otro fenómeno criminal, la ciberdelincuencia no tiene fronteras.

En la actualidad, el Convenio de Budapest ha sido firmado por 45 de los 47 Estados miembros del Consejo de Europa. De ese grupo, 35 lo han ratificado. Estados no miembros del Consejo de Europa, como Australia, Estados Unidos, Japón, la Isla Mauricio, República Dominicana y Panamá, son Estados Parte del Convenio. Además, más de 24 países han sido invitados a adherirse al Convenio, por lo que en el momento se encuentran adelantando el proceso de ratificación interna en este sentido.

Por su parte, el 11 de septiembre de 2013, Colombia fue invitada por el Consejo de Europa a adherirse al Convenio de Budapest, gracias a las

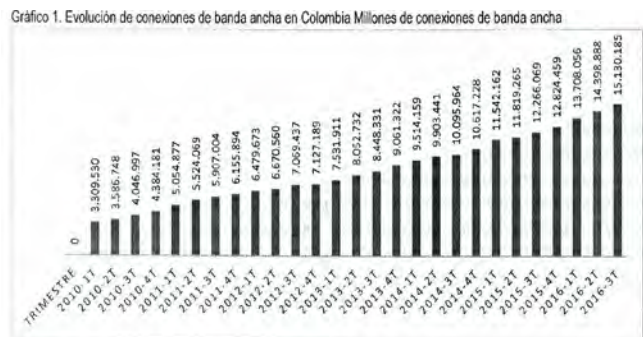
gestiones del Gobierno nacional encaminadas a contar con instrumentos jurídicos y de cooperación internacional para enfrentar de forma efectiva el delito cibernético. El término establecido para formalizar la adhesión es de 5 años por lo que solo hasta el año 2018 Colombia tiene la posibilidad de aceptar dicha invitación.

b) Contexto nacional

Colombia es el primer país de América Latina con Internet de alta velocidad que ha tenido como finalidad llevar este medio a todos sus ciudadanos a lo largo del territorio nacional. En el mismo sentido, aproximadamente desde el año 2005, Colombia se ha comprometido a fortalecer la seguridad de la información y desde 2010, cuando se implementó el Plan Vive Digital, el país ha experimentado una revolución digital que ha llevado el uso de las tecnologías de la información y las comunicaciones a ser una herramienta para el desarrollo del país.

Esta revolución digital implica que tanto los ciudadanos como el sector privado y las entidades públicas dependen cada día más de las tecnologías de la información y las comunicaciones, como lo evidencian las últimas cifras registradas, incluyendo las de conexiones de banda ancha en el país, las cuales se multiplicaron significativamente en los últimos años, pasando de 213 millones en 2010, a 15,130 millones en 2016, tal y como se ilustra en el Gráfico.

Gráfico 1. Evolución de conexiones de banda ancha en Colombia millones de conexiones de banda ancha



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2016.

Así mismo, el número de municipios conectados incrementó hasta llegar a 1.075 en el 2016 y el número de terminales en las instituciones educativas públicas también aumentó. En el pasado había 24 niños por terminal, y en la actualidad solo 4. Esta tendencia en el incremento del uso de las TIC también se ve evidenciada en el número de empresas de dicho sector, el cual pasó de 2.657 a 5.404, y las Mipymes se multiplicaron del 7 al 75%.

En el mismo sentido, aproximadamente desde el año 2005, Colombia se ha comprometido en la misma medida a fortalecer la seguridad de información, es por esto que a través del Decreto número 1078 de 2015 se da obligatoriedad a las Entidades del Estado para implementar el Modelo de Seguridad y Privacidad de TI del Ministerio TIC.

Si bien este aumento en la conectividad en Colombia ha traído consigo innumerables beneficios para el país, también se han incrementado las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales, afectando la seguridad de los ciudadanos, las organizaciones públicas y privadas, e incluso infraestructuras que hacen parte de los intereses de la Nación. Las técnicas y objetivos de los ataques cibernéticos se han sofisticado, teniendo como consecuencia una mayor dificultad para su oportuna detección.

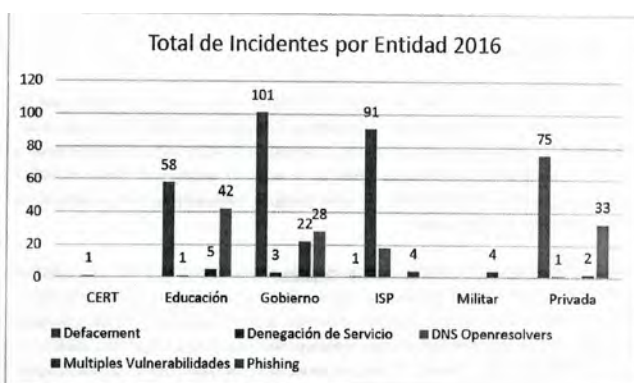
Durante los últimos años, Colombia ha sido foco de interés para distintos ataques cibernéticos, los cuales se han sofisticado trayendo consigo el incremento de la efectividad de los mismos y una mayor dificultad para su oportuna detección. Escenario que preocupa al Gobierno nacional toda vez que las condiciones para desarrollar actividades socioeconómicas en el país cada día se soportan más en el uso de las TIC, y los incidentes digitales en Colombia afectan a varios agentes y sectores (Gráficos 2 y 3).

Gráfico 2. Sectores afectados en Colombia por incidentes digitales 2016

Tipo de Incidente	Tipo de Entidad						Total
	CERT	Educación	Gobierno	ISP	Militar	Privada	
Defacement		58	101	1		75	235
Denegación de Servicio	1	1	3	91		1	97
DNS Openresolvers				18			18
Múltiples Vulnerabilidades		5	22		4	2	33
Phishing		42	28	4		33	107
Total	1	106	154	114	4	111	490

Fuente: colCERT, 2016.

Gráfico 3. Total incidentes digitales por Entidad 2016



Fuente: colCERT, 2016

c) Marco normativo nacional

El país viene desarrollando Instrumentos Normativos que contemplan temáticas relacionadas con la seguridad de la información, la ciberseguridad y la ciberdefensa las cuales se relacionan en esta marco normativo.

En el año 2009 se expidió la Ley 1273 *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. Se crearon los siguientes tipos penales: Capítulo I *De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.* Este capítulo tipifica las siguientes conductas penales: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales. Capítulo II *De los atentados informáticos y otras infracciones,* este capítulo tipifica el: hurto por medios informáticos y semejantes, así como la transferencia no consentida de activos.

Por medio de la Ley 1273 se adoptan los lineamientos del Convenio de Budapest celebrado en el año 2001. La decisión, de proferir las leyes internas en concordancia al Convenio sobre Ciberdelincuencia, fue tomada por considerarse de vital importancia que los desarrollos normativos incluyeran esas directrices de la legislación europea que se habían empezado a introducir en los ordenamientos jurídicos de diferentes países; aun cuando Colombia no es parte del Consejo de Europa y aún no había sido invitada a adherirse al mismo.

Colombia cuenta con una legislación procesal penal integral y efectiva para abordar los delitos cibernéticos, reconoce los tratados internacionales con Interpol y Europol y, específicamente, la Ley 1581 de 2012 establece un marco básico para la protección de datos, divulgación y denuncia de las violaciones de seguridad. Por su parte, dentro de las leyes de carácter ordinario se encuentran unas que regulan diversos temas asociados con la seguridad digital, el comercio electrónico, la pornografía y la explotación sexual de menores en el ciberespacio, la racionalización de trámites y procedimientos, los derechos de autor y conexos, entre otros.

d) Política pública

En el año 2011, el Gobierno nacional aprobó el Conpes 3701 en el cual establecieron los lineamientos de política de ciberseguridad y ciberdefensa. Este documento establece las medidas que deben adoptar las entidades que tengan acceso al manejo de la información para contrarrestar el incremento de las amenazas informáticas, dentro de las cuales se establecieron normas técnicas y estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad.

En abril del 2016 se aprobó el Conpes 3854 de Seguridad Digital Integral, en el que se estableció la implementación en cinco ejes : i) Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos; ii) Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital; iii) Fortalecer

la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos; iv) Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos; y v) Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Dentro del Conpes 3854, se manifestó que la política de Ciberseguridad y Ciberdefensa adoptada por Colombia, debe ser complementada para responder adecuadamente a los nuevos tipos de incertidumbres e incidentes digitales y, adicional a lo anterior, se puso en evidencia que Colombia dispone de un marco normativo nacional disperso en torno a la seguridad digital que comprende leyes, decretos y otros actos expedidos bajo condiciones diferentes a las actuales, por lo cual se creó la política nacional de seguridad digital.

Para cumplir con los objetivos establecidos en los frentes expuestos en la Política Nacional de Seguridad Digital se establecieron diferentes estrategias. En concreto, para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional se planteó la búsqueda de la adhesión de Colombia a diferentes convenios internacionales, dentro del cual se resaltó el Convenio de Budapest.

IV. DESCRIPCIÓN DEL CONVENIO

a) Objeto del acuerdo

El Convenio de Budapest tiene por objeto la materialización de una política criminal común en materia de ciberdelincuencia mediante la adopción de los siguientes lineamientos:

- Intensificación de la cooperación entre Estados y su relación con el sector privado con el fin de prevenir la comisión de ilícitos en las redes informáticas.
- Adopción de la legislación interna pertinente, que permita combatir las amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

b) Explicación del articulado

El articulado del Convenio de Budapest está dividido en las siguientes secciones:

Legislación sustantiva

Con el objeto de construir una política criminal común, encaminada a sancionar la criminalidad en el ciberespacio, el Convenio de Budapest estipula en los artículos 2° a 12 los tipos penales pertinentes para enfrentar este fenómeno. Los Estados Parte adquieren la obligación de adecuar su legislación interna a las exigencias estipuladas en dicho instrumento, relativas a los temas de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de

los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual, y responsabilidad de las personas jurídicas.

En este tipo de conductas el sujeto pasivo, es decir la víctima del ilícito, puede ser cualquier persona natural o jurídica que sea dueña de un sistema de procesamiento de información.

Legislación procesal

En los artículos 16 a 21 del Convenio, se estipulan procedimientos y poderes para las autoridades públicas, que también deben ser adoptados por los Estados parte en su legislación procesal interna. Las obligaciones impuestas por la normatividad en mención, se resumen en los siguientes 4 puntos:

- Adoptar medidas para garantizar la conservación inmediata de datos informáticos almacenados y la divulgación de los denominados datos de tráfico;
- Otorgar facultades a las autoridades competentes, para que puedan solicitar a los proveedores de servicios y demás particulares la entrega de datos almacenados en su poder;
- Disponer de medios idóneos para interceptar y compendiar en tiempo real datos de tráfico asociados con una comunicación particular;
- Expedir la regulación pertinente, que habilite a sus autoridades a acceder y decomisar, cualquier sistema o soporte de almacenamiento informático.

Cooperación internacional

El Convenio estipula la aplicación de instrumentos para luchar de forma efectiva contra los delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable, tomando como base los acuerdos de legislación uniforme o recíproca de los Estados, y el propio derecho interno de las partes a efectos de investigar o realizar procedimientos conjuntos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de delitos.

En este sentido, busca instar a los Estados Parte a cooperar de la manera más amplia posible, lo que se traduce en el compromiso de Colombia de dar trámite a las solicitudes de asistencia para la investigación y recolección de materia probatoria. Asimismo, el Convenio obligaría a Colombia a conservar y comunicar datos informáticos almacenados de interés para los Estados partes; prestar asistencia concerniente al acceso transfronterizo de los mismos; y a establecer un punto de contacto localizable las 24 horas del día, los siete días de la semana.

c) Reservas

El Ministerio de Relaciones Exteriores ha informado que formulará una reserva al artículo 14 del tratado, para proteger los derechos constitucionales de hábeas data e intimidad personal. En el mencionado artículo 14 se faculta a los Estados a reservarse el derecho de aplicar las medidas establecidas en el artículo 20 del Convenio, relativo a Obtención en tiempo real de datos relativos al tráfico, pero únicamente para ciertas categorías de delitos especificados en la reserva. Al realizar esta reserva, se evitaría una posible declaratoria de inexecutable por parte de la Corte Constitucional, en el marco del control previo, automático e integral.

Igualmente, el Ministerio ha expuesto la posibilidad de reservar la aplicación del artículo 21, concerniente a la Interceptación de datos relativos al contenido en los casos en que un sistema informático:

- Se haya puesto en funcionamiento para un grupo restringido de usuarios;
- No emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado.

Estas reservas protegerían posibles vulneraciones a derechos establecidos como fundamentales en la Constitución Política de Colombia ampliamente desarrollados por la Corte Constitucional (Sentencia C-640 de 2010 y Sentencia T-358 de 2014).

V. IMPORTANCIA DEL CONVENIO DE BUDAPEST PARA COLOMBIA

La expansión de las amenazas en el ciberespacio, así como la utilización de nuevas tecnologías para cometer delitos informáticos, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado.

Los fenómenos de criminalidad que afectan la ciberseguridad son generados, en muchas ocasiones, por actores que se encuentran en una jurisdicción geográfica diferente en la que se cometen los delitos, por lo que las pruebas de un acto delictivo no son accesibles sin la colaboración judicial y técnica de las legítimas autoridades públicas que rigen sobre ese territorio. Por lo tanto, en este marco y en los casos que suponen la utilización de redes de comunicación, la cooperación internacional es esencial para prevenir y enfrentar cualquier acto delictivo de carácter cibernético. Por las razones anteriores, Colombia debe adherirse al Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

Este es el único instrumento internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia derecho penal, derecho procesal y cooperación internacional y trata con carácter prioritario una política penal contra la ciberdelincuencia en cada uno de los países miembros. El Convenio de Budapest, permite no solo avanzar en temas de cooperación internacional contra delitos informáticos, sino también fortalecer las leyes y regulaciones nacionales contra el ciberdelito de todo nivel.

VI. TEXTO DEL CONVENIO

PREÁMBULO

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio;

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los Derechos Humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de Derechos Humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la

libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las recomendaciones del Comité de Ministros n.º R (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, n.º R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, n.º R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, n.º R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, así como n.º R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y n.º R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución n.º 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución n.º 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus

esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocía la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

CAPÍTULO I

Terminología

Artículo 1º. *Definiciones.*

A los efectos del presente Convenio:

- a) Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;
- b) por “datos informáticos” se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;
- c) por “proveedor de servicios” se entenderá:
 - i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y
 - ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;
- d) por “datos sobre el tráfico” se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

CAPÍTULO II

Medidas que deberán adoptarse a nivel nacional

Sección 1. Derecho penal sustantivo

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2º. *Acceso ilícito.*

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como

delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3°. *Intercepción ilícita.*

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4°. *Interferencia en los datos.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5°. *Interferencia en el sistema.*

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6°. *Abuso de los dispositivos.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
 - a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
 - i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;
 - ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean

utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

- b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.
2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.
 3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Título 2. Delitos informáticos

Artículo 7°. *Falsificación informática.*

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8°. *Fraude informático.*

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

- a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;
- b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3. Delitos relacionados con el contenido

Artículo 9°. Delitos relacionados con la pornografía infantil.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
 - a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
 - b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
 - c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,
 - d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
 - e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.
2. A los efectos del anterior apartado 1, por “pornografía infantil” se entenderá todo material pornográfico que contenga la representación visual de:
 - a) Un menor comportándose de una forma sexualmente explícita;
 - b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
 - c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.
3. A los efectos del anterior apartado 2, por “menor” se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.
4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se

revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que esta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

Título 5. Otras formas de responsabilidad y de sanciones

Artículo 11. Tentativa y complicidad.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2° a 10 del presente Convenio, con la intención de que se cometa ese delito.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de los delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a)

y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.

Artículo 12. Responsabilidad de las personas jurídicas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:
 - a) Un poder de representación de la persona jurídica;
 - b) una autorización para tomar decisiones en nombre de la persona jurídica;
 - c) una autorización para ejercer funciones de control en la persona jurídica.
2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.
3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.
4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13. Sanciones y medidas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.
2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las perso-

nas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2. Derecho procesal

Título 1. Disposiciones comunes

Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.
2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:
 - a) Los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;
 - b) otros delitos cometidos por medio de un sistema informático; y
 - c) la obtención de pruebas electrónicas de un delito.
- 3.a) Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.
- b) Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:
 - i) Utilizado en beneficio de un grupo restringido de usuarios, y
 - ii) que no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.

Artículo 15. Condiciones y salvaguardas.

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los

poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los Derechos Humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los Derechos Humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de Derechos Humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.
3. Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.

Título 2. Conservación rápida de datos informáticos almacenados

Artículo 16. Conservación rápida de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.
2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un

máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17. Conservación y revelación parcial rápidas de datos sobre el tráfico.

1. Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:
 - a) Para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y
 - b) para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.
2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3. Orden de presentación

Artículo 18. Orden de presentación.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:
 - a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y
 - b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.
2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.

3. A los efectos del presente artículo, por “datos relativos a los abonados” se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:
 - a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
 - b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
 - c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4. Registro y confiscación de datos informáticos almacenados

Artículo 19. Registro y confiscación de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:
 - a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y
 - b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para este, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes

a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 o 2. Estas medidas incluirán las siguientes facultades:

- a) Confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;
 - b) realizar y conservar una copia de dichos datos informáticos;
 - c) preservar la integridad de los datos informáticos almacenados de que se trate;
 - d) hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.
4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.
 5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5. Obtención en tiempo real de datos informáticos

Artículo 20. Obtención en tiempo real de datos sobre el tráfico.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:
 - a) Obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y
 - b) obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:
 - i) a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o
 - ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para ase-

gurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21. *Interceptación de datos sobre el contenido.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:
 - a) A obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y
 - b) a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:
 - i) A obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o
 - ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3. Jurisdicción

Artículo 22. *Jurisdicción.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:
 - a) En su territorio; o
 - b) a bordo de un buque que enarbole pabellón de dicha Parte; o
 - c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o
 - d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.
3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.
4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.
5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

CAPÍTULO III

Cooperación internacional

Sección 1. Principios generales

Título 1. Principios generales relativos a la cooperación internacional

Artículo 23. *Principios generales relativos a la cooperación internacional.*

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados

en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2. Principios relativos a la extradición.

Artículo 24. Extradición.

1. a) El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.
- b) Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE n.º 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.
2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.
3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.
4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.
5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.
6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera com-

petente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a) Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.
- b) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3. Principios generales relativos a la asistencia mutua

Artículo 25. Principios generales relativos a la asistencia mutua.

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.
2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículos 27 a 35.
3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.
4. Salvo que se establezca específicamente otra cosa en los artículos del presente ca-

pítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26. Información espontánea.

1. Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.
2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

Título 4. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

1. Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de

asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

- 2.a) Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.
- b) Las autoridades centrales se comunicarán directamente entre sí.
- c) En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.
- d) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.
3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.
4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:
 - a) La solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;
 - b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.
5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.
6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si

puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7. La Parte requerida informará sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.
8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.
9. a) En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.
- b) Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).
- c) Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.
- d) Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.
- e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central.

Artículo 28. Confidencialidad y restricción de la utilización.

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.
2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:
 - a) Se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o
 - b) no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.
3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.
4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

Sección 2. Disposiciones especiales

Título 1. Asistencia mutua en materia de medidas provisionales

Artículo 29. Conservación rápida de datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.
2. En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:
 - a) La autoridad que solicita dicha conservación;

- b) el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;
 - c) los datos informáticos almacenados que deben conservarse y su relación con el delito;
 - d) cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;
 - e) la necesidad de la conservación; y
 - f) que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.
3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.
 4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.
 5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:
 - a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
 - b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.
 6. Cuando la Parte requerida considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30. Revelación rápida de datos conservados sobre el tráfico.

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.
2. La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:
 - a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
 - b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2. Asistencia mutua en relación con los poderes de investigación

Artículo 31. Asistencia mutua en relación con el acceso a datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.
2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.
3. Se dará respuesta lo antes posible a la solicitud cuando:
 - a) Existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o

- b) los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida.

Artículo 32. Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público.

Una Parte podrá, sin la autorización de otra Parte:

- a) Tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o
- b) tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33. Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico.

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.
2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34. Asistencia mutua relativa a la interceptación de datos sobre el contenido.

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3. Red 24/7

Artículo 35. Red 24/7.

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendientes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:
 - a) El asesoramiento técnico;

- b) la conservación de datos en aplicación de los artículos 29 y 30;
 - c) la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.
2. a) El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.
 - b) Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.
 3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

CAPÍTULO IV

Disposiciones finales

Artículo 36. Firma y entrada en vigor.

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.
2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.
3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.
4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, este entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37. Adhesión al Convenio.

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su

elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38. Aplicación territorial.

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.
2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.
3. Toda declaración formulada en virtud de los dos apartados anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39. Efectos del Convenio.

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:
 - El Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE n.º 24);
 - el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE n.º 30);
 - el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE n.º 99).
2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto,

o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40. Declaraciones.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41. Cláusula federal.

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.
2. Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.
3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42. Reservas.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma

o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4°, apartado 3 del artículo 6°, apartado 4 del artículo 9°, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43. Situación de las reservas y retirada de las mismas.

1. La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y esta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.
2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.
3. El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44. Enmiendas.

1. Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.
2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentará al Comité de Ministros su opinión sobre la enmienda propuesta.
3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.
4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo será remitido a las Partes para su aceptación.

5. Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45. Solución de controversias.

1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.
2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, estas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46. Consultas entre las Partes.

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:
 - a) La utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;
 - b) el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;
 - c) el estudio de la conveniencia de ampliar o enmendar el presente Convenio.
2. Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.
3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.
4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que estas determinen.
5. Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para des-

empeñar sus funciones en aplicación del presente artículo.

Artículo 47. Denuncia.

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.
2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48. Notificación.

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

- a) Cualquier firma;
- b) el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
- c) cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
- d) cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42;
- e) cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

VII. ARTICULADO DEL PROYECTO DE LEY NÚMERO 230 DE 2018 CÁMARA, 58 DE 2017 SENADO

por medio de la cual se aprueba el convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest.

El Congreso de Colombia

DECRETA:

Artículo 1°. Apruébase el *Convenio sobre la Ciberdelincuencia*, adoptado el 23 de noviembre de 2001, en Budapest.

Artículo 2°. De conformidad con lo dispuesto en el artículo 1° de la Ley 7ª de 1944, el *Convenio sobre la Ciberdelincuencia*, adoptado el 23 de noviembre de 2001, en Budapest, que por el artículo primero de esta ley se aprueba, obligará a la República de Colombia a partir de la fecha en que se perfeccione el vínculo internacional respecto del mismo.


Artículo 3°. La presente ley rige a partir de la fecha de su publicación.

VII. PROPOSICIÓN

En consecuencia, por las razones anteriormente expuestas nos permitimos rendir ponencia positiva y le solicitamos muy respetuosamente a los miembros

de la Comisión Segunda Constitucional Permanente de la honorable Cámara de Representantes, **dar primer debate al Proyecto de ley número 230 de 2018 Cámara, 58 de 2017, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest.**

De los honorables Congressistas,


 EFRAÍN ANTONIO TORRES MONSALVO
 Ponente


 JOSÉ CARLOS MIZGER PACHECO
 Ponente

TEXTO PROPUESTO PARA PRIMER DEBATE AL PROYECTO DE LEY NÚMERO 230 DE 2018 CÁMARA, 58 DE 2017 SENADO

por medio de la cual se aprueba el convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest

El Congreso de Colombia

DECRETA:

Artículo 1°. Apruébase el *Convenio sobre la Ciberdelincuencia*, adoptado el 23 de noviembre de 2001, en Budapest.

Artículo 2°. De conformidad con lo dispuesto en el artículo 1° de la Ley 7ª de 1944, el *Convenio sobre la Ciberdelincuencia*, adoptado el 23 de noviembre de 2001, en Budapest, que por el artículo primero de esta ley se aprueba, obligará a la República de Colombia a partir de la fecha en que se perfeccione el vínculo internacional respecto del mismo.

Artículo 3°. La presente ley rige a partir de la fecha de su publicación.

Atentamente,


 EFRAÍN ANTONIO TORRES MONSALVO
 Ponente


 JOSÉ CARLOS MIZGER PACHECO
 Ponente

CONTENIDO

Gaceta número 261 - Miércoles, 16 de mayo de 2018

CÁMARA DE REPRESENTANTES

Págs.

PONENCIAS

Ponencia para primer debate y texto propuesto al Proyecto de ley número 201 de 2018 Senado, 219 de 2018 Cámara, por la cual se reglamenta lo previsto en el parágrafo 5° del artículo 361 de la Constitución Política relativo a los programas de inversión que se financiarán con recursos del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías.....	1
Ponencia para primer debate y texto propuesto al Proyecto de ley número 230 de 2018 Cámara, 58 de 2017 Senado, por medio de la cual se aprueba el <i>Convenio sobre la Ciberdelincuencia</i> , adoptado el 23 de noviembre de 2001 en Budapest.....	11