

Bogotá D.C., 17 de septiembre de 2024

C-668-2024

Respetados

**COMISIÓN PRIMERA CONSTITUCIONAL PERMANENTE**

Cámara de Representantes

Carrera 7 # 8 – 68 Edificio Nuevo del Congreso

[comision.primer@camara.gov.co](mailto:comision.primer@camara.gov.co)

**Asunto:** Comentarios al Proyecto de Ley Estatutaria 152/2024 Cámara: *“Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales”*.

Respetados representantes.

Reciban un cordial saludo de la Asociación Colombiana de Administradoras de Fondos de Pensiones y de Cesantía -Asofondos- y de sus agremiadas.

De manera respetuosa nos permitimos manifestar los comentarios y observaciones efectuados por esta agremiación y por las Administradoras de Fondos de Pensiones (AFP) al proyecto de la referencia, relacionado con el Régimen General de Protección de Datos Personales.

En primer lugar, en Asofondos acompañamos todas y cada una de las iniciativas legislativas que tengan como objetivo brindar mayores garantías de protección a los ciudadanos y para el desarrollo sostenible de la economía digital. Con ello, a continuación, presentamos algunas consideraciones generales sobre el proyecto, para luego relacionar los comentarios que sobre el articulado estimamos pertinentes.

Como es sabido, la protección de datos personales está regulada principalmente por la Ley Estatutaria 1581 de 2012 -conocida como la Ley de Protección de Datos Personales-, y su reglamentación a través del Decreto 1377 de 2013. Esta ley establece un marco legal para la recolección, almacenamiento, uso, circulación y supresión de datos personales, garantizando los derechos de los ciudadanos a la privacidad y a la protección de su información.

Esta ley reconoció a la privacidad y la protección de datos como un derecho fundamental, en armonía con el Artículo 15 de la Constitución Política de Colombia. Con ello, se logró el establecimiento de las obligaciones que tienen las entidades que manejan datos personales (responsables y encargados del tratamiento) y la función de control y sanción de la Superintendencia de Industria y Comercio (SIC) como autoridad en materia de datos personales.

No obstante, aunque la Ley 1581 de 2012 ha traído consigo una categoría de derechos fundamentales, esta se ha quedado corta ante el rápido avance tecnológico y las nuevas

prácticas en el tratamiento de datos, como la inteligencia artificial, el big data<sup>1</sup>, y la protección de datos sensibles como los datos biométricos y genéticos.

El Proyecto de Ley representa una actualización del régimen de protección de datos personales vigente. No obstante, es fundamental no desestimar los avances y aprendizajes adquiridos bajo la Ley 1581 de 2012, por lo que, en lugar de optar por una derogación completa, sería más conveniente reformar, armonizar y fortalecer el marco jurídico actual. Lo anterior, con el objetivo de no generar inseguridad jurídica, dispersión normativa y duplicidad regulatoria innecesaria, lo que de suyo podría causar confusión entre los titulares de datos, los responsables y encargados de su tratamiento, así como entre las autoridades de supervisión.

La Ley 1581 de 2012 incorporó principios, reglas y conceptos que continúan vigentes, ya que, al estar estructurada sobre principios y reglas generales, ha demostrado también su capacidad para evolucionar y adaptarse a distintos contextos, gracias a la interpretación y aplicación que sobre el particular han realizado la SIC y Corte Constitucional, y que -dicho sea de paso- el proyecto recoge textualmente en varias de sus disposiciones. Bajo este contexto, evidenciamos que una reforma total resultaría inconveniente -incluso desde el punto de vista del trámite legislativo y de revisión constitucional-, ya que implicaría debatir, votar, aprobar y someter a revisión de la Corte Constitucional disposiciones que ya han pasado previamente por ese mismo proceso.

En cuanto a la armonización y fortalecimiento, es importante destacar que una de las grandes virtudes de la Ley 1581 de 2012 es su neutralidad temática y tecnológica, lo que le ha permitido adaptarse a diversas situaciones y mantenerse vigente a lo largo del tiempo. Desde su promulgación, los principios y conceptos de la Ley 1581 de 2012, han prevalecido sobre las disposiciones de la Ley 1266 de 2008 y han influido en otras normativas sectoriales, como la Ley 2015 de 2020 (Historia Clínica Electrónica Interoperable), la Ley 2097 de 2021 (Registro de Deudores Alimentarios Morosos - Redam), y más reciente, la Ley 2300 de 2023 (Medidas para proteger el derecho a la intimidad de los consumidores). Incluso en el régimen de Finanzas Abiertas, establecido por el Decreto 1297 de 2022 y la Circular Externa SFC 004 de 2024 (que trata sobre información financiera), los principios

---

<sup>1</sup> El término "big data" se refiere a los datos que son tan grandes, rápidos o complejos que es difícil o imposible procesarlos con los métodos tradicionales. El acto de acceder y almacenar grandes cantidades de información para la analítica ha existido desde hace mucho tiempo. Pero el concepto de big data cobró impulso a principios de la década de 2000 cuando el analista de la industria, Doug Laney, articuló la definición actual de grandes datos como las tres V:

**Volumen:** Las organizaciones recopilan datos de diversas fuentes, como transacciones comerciales, dispositivos inteligentes (IO), equipo industrial, vídeos, medios sociales y más. En el pasado, su almacenamiento habría sido un problema - pero el almacenamiento más barato en plataformas como los data lakes y el Hadoop han aliviado la carga.

**Velocidad:** Con el crecimiento del Internet de las Cosas, los datos llegan a las empresas a una velocidad sin precedentes y deben ser manejados de manera oportuna. Las etiquetas RFID, los sensores y los medidores inteligentes están impulsando la necesidad de manejar estos torrentes de datos en tiempo casi real.

**Variedad:** Los datos se presentan en todo tipo de formatos: desde datos numéricos estructurados en bases de datos tradicionales hasta documentos de texto no estructurados, correos electrónicos, vídeos, audios, datos de teletipo y transacciones financieras.

Definición tomada de SAS Institute: [https://www.sas.com/es\\_co/insights/big-data/what-is-big-data.html](https://www.sas.com/es_co/insights/big-data/what-is-big-data.html)

de la Ley 1581 de 2012 han prevalecido, a pesar de que este ámbito debería estar regido principalmente por la Ley 1266 de 2008.

Por lo anterior, no reviste de coherencia que, si se pretende equiparar el régimen de protección de datos colombiano con el europeo -como se sugiere en la exposición de motivos-, se mantenga una dispersión normativa estatutaria tan marcada en relación con el derecho de habeas data. Por ejemplo, en la Unión Europea la tendencia ha sido hacia la armonización y el establecimiento de normas marco que incorporan principios y reglas generales para la protección de datos personales, sujetas a posterior reglamentación e instrucción para casos específicos. Así, la normatividad sobre datos personales debe ser flexible, sin embargo, eso no puede entenderse que sea débil ni inaplicable, sino por el contrario, que debe permitirse su aplicación e interpretación en situaciones tan diversas como la gestión de información financiera y la historia clínica, que, aunque distintas, comparten la base común del tratamiento de datos personales.

Esta situación ha generado confusión incluso en la Corte Constitucional. Por ejemplo, al revisar la constitucionalidad de la Ley 2157 de 2021 (que modificó la Ley 1266 de 2008), la Corte acudió a los principios y conceptos de la Ley 1581 de 2012, a pesar de que esta última excluye explícitamente el tratamiento de bases de datos regulados por la Ley 1266 de 2008 en su artículo 2, literal e. De manera similar, en el régimen de finanzas abiertas, se observa un uso casi indistinto de las disposiciones de ambas leyes estatutarias.

Así las cosas, no tiene sentido que coexistan dos leyes estatutarias que regulen -en esencia- sobre el tratamiento de información en bases de datos personales, esto es la Ley 1266 de 2008 y la Ley 1581 de 2012. Como contexto, históricamente se entiende que la primera ley fue expedida para regular la información financiera, positivizando la jurisprudencia temprana de la Corte Constitucional sobre el artículo 15 de la Constitución Política de Colombia. Posteriormente, la Corte Constitucional solicitó en su jurisprudencia extender estas disposiciones a un marco general, lo que dio origen a la Ley 1581 de 2012. Para casos como la Ley 2015 de 2020 (Historia Clínica Electrónica Interoperable), la Ley 2097 de 2021 (Registro de Deudores Alimentarios Morosos - Redam), y la Ley 2300 de 2023 (Protección del derecho a la intimidad de los consumidores), no fue necesario crear nuevas leyes estatutarias, pues simplemente se adhirieron a las disposiciones generales de la Ley 1581 de 2012, con reglamentación e instrucción administrativa posterior.

Por lo tanto, Asofondos reitera la importancia de propender por un estatuto general basado en principios y reglas generales que absorba las normativas sectoriales innecesarias y difíciles de aplicar debido a la sobre-regulación actual. Luego, este estatuto debería ser objeto de reglamentación administrativa para casos específicos y de instrucción por parte de las autoridades competentes, facilitando así su implementación y cumplimiento. Esto cobra particular importancia dado que el tratamiento de datos se ve implicado en procesos altamente disruptivos, dinámicos y diversos. En consecuencia, bajo la premisa de necesitar leyes estatutarias y marcos normativos especiales para cada sector, podríamos terminar con un régimen de protección de datos fragmentado, difícil de aplicar y de entender.

Paralelamente, se identifican varias disposiciones que imponen cargas desproporcionadas e injustificadas, lo que dificultaría el cumplimiento por parte de responsables y encargados, además de desincentivar la oferta de bienes y servicios que involucren el tratamiento de

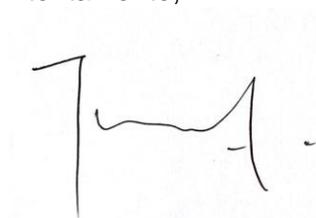
datos personales. Esto es particularmente relevante en el contexto de Open Finance y Open Data, que el Gobierno Colombiano<sup>2</sup> ha venido promoviendo.

Finalmente, a pesar de que la iniciativa busca alinearse con las nuevas tecnologías de la información, se recomienda abordar el análisis de regulación sobre las *cookies* o el *Web scraping*, siendo una técnica utilizada para extraer datos de sitios web de manera automatizada, por medio de *scripts* que recopilan la información de las páginas web estructurada en el formato deseado (por ejemplo, para hacer análisis o bases de datos). Esto puede plantear problemáticas jurídicas futuras, ya que algunos sitios web prohíben la recolección automática de datos en sus términos de servicio, por lo que las leyes de privacidad y protección de datos también juegan un papel importante en cómo se puede utilizar la información obtenida a través de esta técnica.

Es por lo anterior que, a continuación, se relaciona la tabla correspondiente al pliego de modificaciones del proyecto para que sea tenido en cuenta en el primer debate en la Comisión Primera Constitucional Permanente de la Cámara de Representantes, con el texto que esta agremiación considera pertinente modificar y la justificación.

Por lo anterior y de manera muy respetuosa, solicitamos que el debate al que se circunscriba el presente Proyecto de Ley se lleve a cabo de forma modificatoria, donde se concentren las posiciones de las entidades que tengan a su cargo el manejo de datos personales. Dicho lo anterior, agradecemos por el espacio y la oportunidad otorgada.

Atentamente,



**Juan Camilo Argote**  
Líder de Asuntos Legales Corporativos  
Vicepresidencia Jurídica | Asofondos

<sup>2</sup> Colombia avanza en la adopción de las finanzas abiertas. Superintendencia Financiera de Colombia. Febrero de 2024.  
<https://www.superfinanciera.gov.co/publicaciones/10114976/colombia-avanza-en-la-adopcion-de-las-finanzas-abiertas/>

**PLIEGO DE MODIFICACIONES DEL PROYECTO DE LEY ESTATUTARIA 152/2024  
CÁMARA: “POR LA CUAL SE DICTAN DISPOSICIONES PARA EL RÉGIMEN  
GENERAL DE PROTECCIÓN DE DATOS PERSONALES”.**

TEXTOS RADICADOS	TEXTOS PROPUESTOS PARA PRIMER DEBATE EN COMISIÓN PRIMERA DE CÁMARA	Justificación
<p><b>ARTÍCULO 1. Objeto.</b></p> <p>La presente ley establece las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos.</p> <p>De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.</p>	<p align="center">Sin modificación</p>	<p align="center">Sin modificación</p>
<p><b>ARTÍCULO 2. Ámbito de la aplicación material.</b></p> <p>1. La presente ley se aplica al tratamiento de los datos personales.</p> <p>2. El régimen de protección de datos personales establecido en la presente ley no será de aplicación:</p> <p>a) A los tratamientos efectuados por una persona natural en un ámbito exclusivamente personal o doméstico.</p> <p>b) A los tratamientos realizados por parte de las autoridades competentes con fines de prevención, investigación, detección, o procesamiento judicial de actos delictivos incluido el lavado de activos y el financiamiento del terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad y defensa nacional y su prevención.</p> <p>c) A los tratamientos que tengan como finalidad cumplir con la actividad periodística y</p>	<p align="center">Sin modificación</p>	<p align="center">Sin modificación</p>

<p>otros contenidos editoriales.</p> <p>d) A los tratamientos que tengan como fin y contengan información de inteligencia y contrainteligencia.</p> <p>e) A los tratamientos realizados en virtud de la Ley 1266 de 2008</p> <p><i>Parágrafo primero.</i> Cuando se traten datos de personas fallecidas, los causahabientes, que acrediten tal calidad, podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.</p> <p><i>Parágrafo segundo.</i> El Gobierno Nacional, reglamentará sobre el tratamiento de datos personales tratados para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos, la financiación del terrorismo y la ejecución de sanciones penales.</p> <p><i>Parágrafo tercero.</i> Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el presente artículo, con los límites dispuestos en la presente ley y sin refir con los datos que tienen características de estar amparados por la reserva legal.</p> <p>En el evento que la normatividad especial regule los tratamientos de datos personales exceptuados prevea principios que tengan en consideración la naturaleza especial de los datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.</p>		
<p><b>ARTÍCULO 3. Ámbito territorial.</b></p> <ol style="list-style-type: none"> <li>1. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia.</li> <li>2. La presente ley se aplica al tratamiento de datos personales de titulares que</li> </ol>	<p><b>ARTÍCULO 3. Ámbito territorial.</b></p> <ol style="list-style-type: none"> <li>3. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia.</li> <li>4. La presente ley se aplica al tratamiento de datos personales de titulares que</li> </ol>	<p>En el literal a) del numeral 2, se sugiere eliminar la frase “<i>independientemente de si estos son de carácter oneroso</i>”. La naturaleza onerosa o gratuita de los bienes o servicios no debería influir en el tratamiento de los datos, ya que el régimen de protección de datos no distingue esta condición.</p>

<p>residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con:</p> <ol style="list-style-type: none"> <li>a) La oferta de bienes o servicios a dichos titulares con residencia en Colombia, independientemente de si estos son de carácter oneroso o no.</li> <li>b) El control del comportamiento, en la medida en que este tenga lugar en Colombia.</li> </ol> <p>Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud del derecho internacional público.</p>	<p>residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con:</p> <ol style="list-style-type: none"> <li>a) La oferta de bienes o servicios a dichos titulares con residencia en Colombia. <del>independientemente de si estos son de carácter oneroso o no.</del></li> <li>b) El control del comportamiento, en la medida en que este tenga lugar en Colombia.</li> </ol> <p>Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud del derecho internacional público.</p>	
<p><b>ARTÍCULO 4. Definiciones.</b> A efectos de la presente ley se entenderá por:</p> <ol style="list-style-type: none"> <li>1. «Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular;</li> <li>2. «Autoridad de Protección de Datos»: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicionen o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales.</li> <li>3. «Base de datos»: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.</li> </ol>	<p><b>ARTÍCULO 4. Definiciones.</b> A efectos de la presente ley se entenderá por:</p> <ol style="list-style-type: none"> <li>1. «Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular;</li> <li>2. «Autoridad de Protección de Datos»: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicionen o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales.</li> <li>3. «Base de datos»: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.</li> <li>4. «Bloqueo de datos»: medidas técnicas y organizativas adoptadas por parte del</li> </ol>	<p>Se insiste en la necesidad de revisar conjuntamente lo ya dispuesto en la Ley 1266 de 2008 y la Ley 1581 de 2012, para no incurrir en duplicidades normativas, así como en trámites legislativos y de revisión constitucional innecesarios.</p> <p>En la definición de titular del numeral 23. se debe prever que las personas jurídicas también pueden ser titulares, lo que implicaría algunas disposiciones que refieran al tratamiento de estos datos. Esto de acuerdo con las tendencias modernas internacionales.</p> <p>De acuerdo con el numeral 24, se entiende que, la transferencia de datos solo se da a nivel internacional, siendo que esta transferencia es la remisión de datos por un canal de comunicación punto a punto o punto a multipunto</p>

<ol style="list-style-type: none"> <li>4. «Bloqueo de datos»: medidas técnicas y organizativas adoptadas por parte del responsable o encargado del tratamiento, que permitan la identificación y reserva de los datos para impedir y/o evitar su tratamiento.</li> <li>5. «Comunicación de datos»: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento.</li> <li>6. «Consentimiento del titular»: Toda manifestación de la voluntad expresa, libre, inequívoca, informada y específica por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.</li> <li>7. «Corresponsabilidad»: Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento.</li> <li>8. «Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.</li> <li>9. «Datos genéticos»: datos personales relativos a la información sobre las características hereditarias de una persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos de una muestra biológica, que proporcionen una información única sobre la fisiología o la salud de esa persona.</li> <li>10. «Datos personales»: toda información sobre una persona natural identificada o identificable (el titular) se considerará persona natural identificable toda persona cuya identidad pueda determinarse, directa o indirectamente,</li> </ol>	<p>responsable o encargado del tratamiento, que permitan la identificación y reserva de los datos para impedir y/o evitar su tratamiento.</p> <ol style="list-style-type: none"> <li>5. «Comunicación de datos»: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento.</li> <li>6. «Consentimiento del titular»: Toda manifestación de la voluntad expresa, libre, inequívoca, informada y específica por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.</li> <li>7. «Corresponsabilidad»: Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento.</li> <li>8. «Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.</li> <li>9. «Datos genéticos»: datos personales relativos a la información sobre las características hereditarias de una persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos de una muestra biológica, que proporcionen una información única sobre la fisiología o la salud de esa persona.</li> <li>10. «Datos personales»: toda información sobre una persona natural identificada o identificable (el titular) se considerará persona natural identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número</li> </ol>	<p>que puede hacerse tanto dentro del territorio nacional como fuera de este. Por lo tanto, la definición debe cobijar igualmente el territorio nacional.</p> <p>La definición de servicio de sociedad de la información es poco clara y no se entiende su inclusión. Planteados en el contexto del proyecto, se entiende que la definición de "Servicio de la sociedad de la información" es cualquier servicio que se presta a un consumidor mediante el uso de dispositivos electrónicos o tecnologías de la información, donde no es necesario que el proveedor y el consumidor estén presentes al mismo tiempo. Luego, incluye servicios que se proporcionan de forma remota o en línea, como el comercio electrónico, plataformas de redes sociales, aplicaciones móviles, almacenamiento en la nube, entre otros. Estos servicios permiten la creación, distribución y manejo de información digital sin que las personas involucradas en el servicio tengan que estar físicamente presentes en el mismo lugar o al mismo tiempo.</p> <p>Por ejemplo, una compra en una tienda en línea o el uso de una plataforma de streaming. Así, se sugiere una mejor redacción al numeral de manera que no pueda darse una interpretación errónea.</p> <p>Se sugiere incluir una definición de Transmisión y de Transferencia de Datos Personales. El Decreto 1074 de 2015 (Art. 2.2.2.25.1.3.), las define, pero conforme al</p>
--	---	--

<p>en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.</p> <p>11. «Datos relativos a la salud»: datos que revelan aspectos relativos al estado de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades de una persona natural. Estos datos incluyen, aunque no limitado a, la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; la información recolectada por dispositivos tecnológicos que busquen hacer mediciones sobre la condición física de su usuario, entre otros.</p> <p>12. «Datos sensibles»: son los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>13. «Destinatario o tercero»: persona natural o jurídica, pública o privada, a la que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. Una vez el destinatario se le ceden los datos se convierte en responsable. No se considerarán destinatarios a las autoridades públicas que puedan</p>	<p>de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.</p> <p>11. «Datos relativos a la salud»: datos que revelan aspectos relativos al estado de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades de una persona natural. Estos datos incluyen, aunque no limitado a, la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; la información recolectada por dispositivos tecnológicos que busquen hacer mediciones sobre la condición física de su usuario, entre otros.</p> <p>12. «Datos sensibles»: son los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>13. «Destinatario o tercero»: persona natural o jurídica, pública o privada, a la que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. Una vez el destinatario se le ceden los datos se convierte en responsable. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal b) y d) de la presente ley.</p>	<p>Art. 71 del presente proyecto de ley se entiende que quedaría derogado todo lo relativo a datos personales que derivó de la Ley 1581 de 2012:</p> <p><b>Es de anotar que el Art. 2.2.2.25.5.2. del mencionado decreto también regula el Contrato de transmisión de datos personales., el cual se encuentra en la Sección No-5 de “TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES”, por lo que se recomienda aclarar si (i) ¿Deberían tener reglas diferenciales las transmisiones nacionales vs. internacionales de datos personales? (Responsable a Encargado) (ii) ¿Qué requisitos deben de cumplirse de cara a la transferencia nacional vs. la internacional? (Responsable a Responsable)</b></p>
--	---	--

<p>recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal b) y d) de la presente ley.</p> <p>14. «Elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales con el fin de evaluar determinados aspectos de una persona natural. En particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, movimientos, entre otros, de dicha persona natural.</p> <p>15. «Encargado del tratamiento» o «Encargado»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.</p> <p>16. «Incidente de seguridad»: cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado, y que impacte en la confidencialidad, integridad y/o disponibilidad de dichos datos.</p> <p>17. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de <b>manera</b> que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.</p> <p>18. «Neurodato»: para los efectos de la presente ley, se refiere al conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, así como la información inferida de estos datos, de una persona natural identificada o identificable.</p>	<p>14. «Elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales con el fin de evaluar determinados aspectos de una persona natural. En particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, movimientos, entre otros, de dicha persona natural.</p> <p>15. «Encargado del tratamiento» o «Encargado»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.</p> <p>16. «Incidente de seguridad»: cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado, y que impacte en la confidencialidad, integridad y/o disponibilidad de dichos datos.</p> <p>17. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de <b>manera</b> que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.</p> <p>18. «Neurodato»: para los efectos de la presente ley, se refiere al conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, así como la información inferida de estos datos, de una persona natural identificada o identificable.</p> <p>19. «Representante»: persona natural o jurídica designada por escrito por parte <b>del</b> responsable o el encargado del tratamiento, de conformidad con esta ley, para que los represente en lo que</p>	
---	---	--

<p>19. «Representante»: persona natural o jurídica designada por escrito por parte <b>del</b> responsable o el encargado del tratamiento, de conformidad con esta ley, para que los represente en lo que respecta a sus obligaciones en virtud de la presente ley.</p> <p>20. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros determine los fines y medios del tratamiento.</p> <p>21. «Servicio de la sociedad de la información»: para efectos de la presente ley se entenderá como todo servicio prestado por solicitud de un consumidor de servicios, a través de equipos electrónicos y/o tecnologías que facilitan la creación, distribución y manipulación de la información, sin que las partes estén presentes simultáneamente.</p> <p>22. «Seudonimización»: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.</p> <p>23. «Titular»: persona natural cuyos datos personales son objeto de Tratamiento.</p> <p>24. «Transferencia internacional de datos personales»: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran están fuera del territorio nacional.</p> <p>25. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de</p>	<p>respecta a sus obligaciones en virtud de la presente ley.</p> <p>20. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros determine los fines y medios del tratamiento.</p> <p>21. «Servicio de la sociedad de la información»: <b><u>Se entenderá como cualquier servicio que, a solicitud de un usuario, sea prestado mediante el uso de equipos electrónicos o tecnologías de la información y las comunicaciones, permitiendo la creación, distribución y manipulación de información, sin requerir la presencia simultánea de las partes involucradas. Estos servicios pueden incluir, entre otros, el comercio electrónico, plataformas de redes sociales, aplicaciones móviles y servicios de almacenamiento en la nube.</u></b></p> <p>22. «Seudonimización»: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.</p> <p>23. «Titular»: persona natural <b><u>y jurídica</u></b> cuyos datos personales son objeto de Tratamiento.</p> <p>24. «Transferencia <del>internacional</del> de datos personales»: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran están <b><u>dentro y</u></b> fuera del territorio nacional.</p>	
---	--	--

<p>datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</p> <p>26. «Tratamiento a gran escala: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.</p>	<p>25. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</p> <p>26. «Tratamiento a gran escala: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.</p> <p>27. <u>Transferencia. La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.</u></p> <p>28. <u>Transmisión. Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el encargado por cuenta del Responsable.</u></p>	
<p><b>ARTÍCULO 5. Principios relativos al tratamiento.</b></p>	<p><b>ARTÍCULO 5. Principios relativos al tratamiento.</b></p>	<p>El principio de lealtad es redundante frente a los principios de legalidad y</p>

1. El tratamiento de datos personales debe darse en virtud de los siguientes principios:

- a) «Principio de Legalidad»: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
- b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.
- c) «Principio de transparencia»: exige que la Información facilitada a los titulares sea concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo.
- d) «Principio de limitación de la finalidad»: los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento ulterior de los datos personales con fines de archivo en interés público, investigación científica, histórica o estadística no se considerará incompatible con los fines iniciales.
- e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

2. El tratamiento de datos personales debe darse en virtud de los siguientes principios:

- a) «Principio de Legalidad»: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
- b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.
- c) «Principio de transparencia»: **exige que el tratamiento de datos personales debe garantizar que el titular pueda obtener, en cualquier momento y sin restricciones, información clara, concisa y accesible sobre la existencia, el uso y la finalidad de los datos que le conciernan. La información proporcionada por el responsable o encargado del tratamiento debe ser presentada en un lenguaje claro y sencillo, de manera que sea fácilmente comprensible para el titular. Este principio asegura el derecho del titular a conocer y controlar sus datos personales, promoviendo un manejo transparente y accesible de la información**
- d) «Principio de limitación de la finalidad»: **Los datos personales deben ser recolectados únicamente para fines específicos, explícitos y**

**transparencia. A consideración, son estos dos últimos los que deben prevalecer por ser aceptados y tener un tratamiento considerable actual en la jurisprudencia y en la práctica.**

La redacción del principio de transparencia de la Ley 1581 de 2012 debe mantenerse, el cambio propuesto no genera ningún valor adicional. Por ello, se sugiere un texto robustecido tomando tanto los preceptos de la Ley 1581 de 2012 como la intención de la autora del proyecto.

Se debe realizar una revisión a la redacción del principio de limitación de la finalidad, luego, se propone una redacción menos confusa.

En cuanto al principio de responsabilidad demostrada es desproporcional y no se adecua a los estándares internacionales. La obligación de rendir cuentas a titulares y autoridades supera lo pretendido por el concepto de accountability.

Es pertinente reconsiderar la necesidad de modificar los principios de la Ley 1581 de 2012 que tan bien han funcionado hasta hoy en día. Se sugiere solo agregar principios pertinentes como el de responsabilidad demostrada, aplicabilidad y proporcionalidad. Se echa de menos una redacción clara de los principios de una norma marco como pretende el proyecto, la interpretación y adecuación es tema de la Corte y jueces

<p>f) «Principio de exactitud»: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, actualizados; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.</p> <p>g) « Principio de limitación del plazo de conservación»: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares.</p>	<p><b><u>legítimos. No podrán ser tratados posteriormente para otros fines que no se ajusten a los objetivos originales. Sin embargo, el uso posterior de los datos para fines de archivo en interés público, investigación científica, histórica o estadística se considerará adecuado y permitido, incluso si no coincide exactamente con el propósito inicial.</u></b></p> <p>e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.</p> <p>f) «Principio de exactitud»: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, actualizados; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.</p> <p>g) « Principio de limitación del plazo de conservación»: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en</p>	<p>constitucionales.</p>
---	--	--------------------------

h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

i) «Principio de confidencialidad»: los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento.

El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.

j) «Principio de seguridad»: los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración,

cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares.

h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

i) «Principio de confidencialidad»: los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento.

El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.

<p>pérdida, consulta, uso o acceso no autorizado o fraudulento.</p> <p>k) «Principio de proporcionalidad»: durante el ciclo de vida de los datos, el responsable velará porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de protección de datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación,</p>	<p>j) «Principio de seguridad»: los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.</p> <p>k) «Principio de proporcionalidad»: durante el ciclo de vida de los datos, el responsable velará porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: <b><u>los encargados y responsables que intervengan en el Tratamiento de datos personales deben ser capaces de demostrar cuando el titular o alguna autoridad lo requiera</u></b></p>	
--	--	--

sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

que han implementado medidas apropiadas, efectivas y verificables para cumplir con las obligaciones establecidas en la presente ley y sus normas reglamentarias.

**ARTÍCULO 6. Bases que legitiman el tratamiento.**

1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:
  - a) El titular dio su consentimiento previo para el tratamiento de sus datos personales para uno o varios fines específicos.
  - b) El tratamiento es necesario para la ejecución de un contrato en el que el titular es parte o para la aplicación de medidas precontractuales solicitadas por el titular. .
  - c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.
  - d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.
  - e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.
  - f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan **sobre** los

**ARTÍCULO 6. Bases que legitiman el tratamiento.**

1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:
  - a) El titular dio su consentimiento previo para el tratamiento de sus datos personales para uno o varios fines específicos.
  - b) El tratamiento es necesario para la ejecución de un contrato en el que el titular es parte o para la aplicación de medidas precontractuales solicitadas por el titular. .
  - c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.
  - d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.
  - e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.
  - f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan **sobre** los intereses, derechos y garantías fundamentales del titular que requieran la

En lo correspondiente al literal F del numeral 1 del artículo 6 del proyecto, no es claro qué es un interés legítimo perseguido por el Responsable o por un tercero. Por ello, se sugiere incluir una definición o parametría para que todos los Responsables y terceros de estos tengan unas reglas de aplicación claras.

Según definiciones encontradas en la Revista Chilena de Derecho y Tecnología (Vol 8, No. 1 de 2019) en materia de protección de datos personales, el interés legítimo se ha configurado como una base jurídica que permite al responsable de una base de datos personales o a otro tercero el tratamiento de dicha información sin necesidad de recabar previamente el consentimiento del titular de la misma ( Ferretti, 2014 : 14). En este sentido, este interés vendría a atribuir y determinar una cierta calidad especial que un tercero, como sujeto interesado, tendría respecto de datos personales ajenos.

De la misma manera, según el concepto de interés legítimo sobre protección de datos propuesto por el Grupo de Trabajo, como órgano consultivo europeo independiente en materia de protección de datos y privacidad (Página web:

intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.

Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.

2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.

*Parágrafo primero:* La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo. La normativa vigente cumplirá un objetivo de

protección de datos personales. Es fundamental que exista una relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.

**Entiéndase como intereses legítimos del tratamiento por el responsable del tratamiento o por un tercero como la finalidad legal por la cual se toman los datos de los usuarios.**

Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.

3. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.

*Parágrafo primero:* La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo. La

[http://ec.europa.eu/justice/data-protection/index\\_es.htm](http://ec.europa.eu/justice/data-protection/index_es.htm) y [https://www.aepd.es/documento/wp217\\_es\\_interes\\_legitimo.pdf](https://www.aepd.es/documento/wp217_es_interes_legitimo.pdf)) en términos de protección de datos, «finalidad» es la razón específica por la que se tratan los datos: el objetivo o la intención del tratamiento de los datos. Un interés, por otro lado, se refiere a una mayor implicación que el responsable del tratamiento pueda tener en el tratamiento, o al beneficio que el responsable del tratamiento obtenga —o que la sociedad pueda obtener— del tratamiento.

Por lo anterior, la definición debe ser discutida y concertada pues puede estar abierta a una interpretación equivocada sobre el tratamiento de datos.

<p>interés público y será proporcional al fin legítimo perseguido.</p> <p><i>Parágrafo segundo:</i> Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.</p>	<p>normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.</p> <p><i>Parágrafo segundo:</i> Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.</p>	
<p><b>ARTÍCULO 7. Tratamientos con finalidades diferentes a las iniciales.</b></p> <p>Cuando se quiera tratar los datos personales para una finalidad diferente a la que fueron recogidos, y ese nuevo tratamiento no esté basado en el consentimiento del titular o en una norma específica que sea necesaria y proporcional en una sociedad democrática, el responsable del tratamiento deberá considerar si el nuevo tratamiento es compatible con la finalidad original. Para ello, tomará en cuenta lo siguiente:</p> <ul style="list-style-type: none"> <li>a) La relación entre la finalidad original y la nueva finalidad de tratamiento de los datos personales.</li> <li>b) El contexto en que se recogieron los datos personales, especialmente la relación entre los titulares y el responsable del tratamiento.</li> <li>c) La naturaleza de los datos personales, especialmente si son datos sensibles o relacionados con antecedentes penales, anotaciones judiciales o contravencionales.</li> <li>d) Las posibles consecuencias para los titulares por el nuevo tratamiento de sus datos.</li> </ul>	<p>Sin modificación</p>	<p>Sin modificación</p>

<p>e) La existencia de garantías adecuadas, como el cifrado o la seudonimización de los datos.</p>		
<p><b>ARTÍCULO 8. Condiciones para el consentimiento.</b></p> <ol style="list-style-type: none"> <li>1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.</li> <li>2. Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.</li> <li>3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.</li> <li>4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.</li> <li>5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y</li> </ol>	<p><b>ARTÍCULO 8. Condiciones para el consentimiento.</b></p> <ol style="list-style-type: none"> <li>1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.</li> <li><del>2. Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.</del></li> <li><del>3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.</del></li> <li>4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas <b>no marcadas</b> ya <del>marcadas</del> o la inacción no deben constituir consentimiento.</li> <li>5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el</li> </ol>	<p>Lo dispuesto en los numerales 3 y 4 es desproporcional, para un responsable y/o encargado será imposible solicitar múltiples consentimientos para múltiples tratamientos pactados en una misma transacción. Para ello, se requeriría formatos confusos y demasiado largos. Lo viable es que, al momento de solicitar la autorización se redirija al titular al sitio donde puede encontrar y conocer la información detallada del tratamiento, así como los mecanismos para modular o revocar la autorización. Esto lo reconoce el numeral 5 y 6 del proyecto, de forma correcta y razonable, así como lo previsto en el artículo 14 numerales 2 y 3.</p> <p>Además, se debe eliminar que las casillas “ya marcadas” no constituyen consentimiento, ya que puede ocurrir que estén pre marcadas pero el titular puede desactivarlas, así mismo al continuar con la navegación se entiende como una acción afirmativa inequívoca del consentimiento de tratamiento de datos.</p>

<p>este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.</p> <p>6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.</p>	<p>mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.</p> <p>6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.</p>	
<p><b>ARTÍCULO 9. Consentimiento de niños, niñas y adolescentes.</b></p> <p>1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.</p> <p>2. El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.</p> <p>3. En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concurra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.</p>	<p><b>ARTÍCULO 9. Consentimiento de niños, niñas y adolescentes.</b></p> <p>1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.</p> <p>2. El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.</p> <p>3. En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concurra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.</p> <p>6. El numeral 1 no afectará las disposiciones especiales referentes al</p>	<p>En lo relativo al numeral 2 del artículo, debería tenerse en cuenta el Artículo 2.2.2.25.2.9 del Decreto Único Reglamentario 1074 de 2015 de cara a la consulta a los niños, niñas y adolescentes.</p> <p><i>“... 2.2.2.25.2.9. Requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes. El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:</i></p> <p><i>1. Que responda y respete el interés superior de los niños, niñas y adolescentes.</i></p> <p><i>2. Que se asegure el respeto de sus derechos fundamentales.</i></p> <p><u>Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio</u></p>

<p>4. El numeral 1 no afectará las disposiciones especiales referentes al establecimiento de edades mínimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.</p> <p>5. El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.</p> <p><i>Parágrafo:</i> En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto <b>de</b> que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.</p>	<p>establecimiento de edades mínimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.</p> <p>7. El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.</p> <p><i>Parágrafo 1:</i> En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto <b>de</b> que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.</p> <p><b><u>Parágrafo 2: El representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.</u></b></p>	<p><u>del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto....” (subrayado fuera de texto)</u></p> <p>En virtud de lo anterior, se añade un segundo parágrafo al artículo.</p>
<p><b>ARTÍCULO 10. Tratamiento de datos sensibles.</b></p> <p>1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

género y orientación sexual de una persona natural.

2. El numeral 1 no será de aplicación cuando concurra alguna de las siguientes excepciones:

- a) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al titular levantar la prohibición mencionada en el numeral 1.
- b) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o una convención colectiva de trabajo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del titular.
- c) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento.
- d) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera

exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares.

- e) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria.
- f) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones y/o procedimientos administrativos y/o judiciales, así como procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función.
- g) Cuando el tratamiento sea necesario por razones de interés público, para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, sobre la base de la normativa que los faculta para ejercer dichas funciones; el tratamiento debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos, **estableciendo** medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular.

- |   |  |  |
|---|--|--|
| <p>h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud, sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo.</p> <p>i) Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales.</p> <p>j) El tratamiento es necesario con fines de archivo en interés público, investigación científica, histórica o estadística; este debe ser proporcional al objetivo</p> |  |  |
|---|--|--|

perseguido, respetar en lo esencial el derecho a la protección de datos, establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

3. Los datos personales a los que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia.

*Parágrafo:* Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.

**ARTÍCULO 11. Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.**

El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley,

**ARTÍCULO 11. Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.**

El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley, sólo podrá realizarse bajo la supervisión de las

Este artículo deja por fuera de su ámbito el cumplimiento de requisitos y usos el SARLAFT (para el caso de las entidades vigiladas por la Superintendencia Financiera de Colombia) o SAGRILAFT (para las entidades vigiladas por la Superintendencia de Sociedades) y concluye que ya no se deberán establecer

<p>sólo podrá realizarse bajo la supervisión de las entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.</p>	<p>entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.</p> <p><b><u>Para efectos de aplicación del presente artículo, se incluyen las sociedades que tienen obligación de dar cumplimiento a la normativa SARLAFT (para el caso de las entidades vigiladas por la Superintendencia Financiera de Colombia) o SAGRILAFT (para las entidades vigiladas por la Superintendencia de Sociedades).</u></b></p>	<p>los protocolos de conocimiento del cliente, que implican en todo caso un tratamiento, sino exclusivamente acudir a registros que tengan las entidades competentes sobre la materia. Adicionalmente, no habría deber de conocimiento del cliente ni de reporte/aviso a las autoridades, ya que precisamente el tratamiento es ante quien lo realiza son las entidades competentes.</p> <p>Bajo esta interpretación se podría acudir a servicios de motores de búsqueda de empresas que consultan los antecedentes en bases de datos públicos en los términos de la definición actual define del numeral 2 del Artículo 2.2.2.25.1.3 Decreto Único Reglamentario 1074 de 2015, o en su lugar deberá acudirse directamente a las entidades competentes para la prevención del LA/FT.</p> <p>Al requerir que el tratamiento se realice bajo la supervisión de las entidades competentes en el caso de las entidades vigiladas por la SFC se generarían cambios en la Circular Básica Jurídica de la SFC en materia SARLAFT o la C.E. 027 de 2020 de la SFC.</p>
<p><b>ARTÍCULO 12. Tratamiento de datos relativos a sanciones administrativas y/o disciplinarias.</b></p> <p>1. El tratamiento de datos <b>relativo a</b> sanciones administrativas y/o disciplinarias, incluido el mantenimiento de registros relacionados con las mismas, exigirá:</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>a) Que los responsables de dichos tratamientos sean los organismos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.</p> <p>b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.</p> <p>2. Cuando no se cumpla alguna de las condiciones previstas en el numeral anterior, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias, habrán de contar con el consentimiento del titular o estar autorizados por una norma, en la que se regularán, en su caso, garantías adicionales para los derechos de los titulares.</p> <p>3. Fuera de los supuestos señalados en los numerales anteriores, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias sólo serán posibles cuando sean llevados a cabo por abogados y/o agentes oficiosos y que tengan por objeto recoger la información facilitada por sus representados para el ejercicio de sus funciones.</p> <p><i>Parágrafo:</i> Lo descrito en el presente artículo se aplicará igualmente a las sanciones disciplinarias de los servidores públicos.</p>		
<p><b>ARTÍCULO 13. Transparencia e información al titular.</b></p> <p>1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación</p>	<p><b>ARTÍCULO 13. Transparencia e información al titular.</b></p> <p>1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación <b>correspondiente</b> a los</p>	<p>La potestad de presentar queja ante la autoridad debe estar sujeta al agotamiento previo de reclamación directa ante el responsable, esto evitará la congestión de tramites de la autoridad competente y la solución</p>

<p><b>correspondiente</b> a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.</p> <p>2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.</p> <p>3. El responsable del tratamiento facilitará al titular información <b>relativa</b> a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo.</p> <p>Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.</p> <p>Cuando el titular presente la solicitud por medios electrónicos, la información</p>	<p>ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.</p> <p>2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.</p> <p>3. El responsable del tratamiento facilitará al titular información <b>relativa</b> a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo.</p> <p>Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.</p> <p>Cuando el titular presente la solicitud por medios electrónicos, la información se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no</p>	<p>eficiente de solicitudes</p>
--	---	---------------------------------

se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no represente una carga desproporcionada para el responsable.

4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y **de fondo**. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.
5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito.

Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.

6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.
7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente

represente una carga desproporcionada para el responsable.

4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y **de fondo**. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.

**La potestad de presentar queja ante la autoridad debe estar sujeta al agotamiento previo de reclamación directa ante el responsable de los datos con el fin de obtener una solución eficiente de la solicitud.**

5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito.

Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.

6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.
7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible,

<p>visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.</p> <p>8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.</p>	<p>inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.</p> <p>8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.</p>	
<p><b>ARTÍCULO 14. Información que deberá facilitarse cuando los datos personales se obtengan del titular.</b></p> <p>1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará toda la información indicada a continuación:</p> <ol style="list-style-type: none"> <li>Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</li> <li>Los datos de contacto del oficial de protección de datos o área encargada de la protección de datos personales.</li> <li>Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</li> </ol>	<p><b>ARTÍCULO 14. Información que deberá facilitarse cuando los datos personales se obtengan del titular.</b></p> <p>1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará <del>toda</del> la información <del>indicada a continuación</del> <b><u>requerida específica y separada que se describe a continuación:</u></b></p> <ol style="list-style-type: none"> <li>Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</li> <li>Los datos de contacto del oficial de protección de datos o área encargada de la protección de datos personales.</li> <li>Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</li> <li>Los destinatarios de los datos personales, si los hubiera.</li> </ol>	<p>lo requerido en el numeral 1 es virtualmente imposible. Es difícil que, en la solicitud de una autorización de tratamiento de datos, que en la práctica se da con una firma o un clic, se de toda la información relacionada con el detalle requerido en el proyecto. Lo aconsejable es solicitar la autorización, presentar un sitio o lugar de consulta de la información requerida y disponer de mecanismos ágiles para la modulación y/o revocación de la autorización.</p>

- d) Los destinatarios de los datos personales, si los hubiera.
- e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado.
- f) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- g) La descripción y ejercicio de los derechos que le asisten al titular.
- h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.
- i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.
- j) Cuando la comunicación de datos personales sea un

- e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado.
- f) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- g) La descripción y ejercicio de los derechos que le asisten al titular.
- h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.
- i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.
- j) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles

<p>requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.</p> <p>k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo.</p> <p>3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.</p>	<p>consecuencias de no facilitar tales datos.</p> <p>k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo.</p> <p>3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.</p>	
<p><b>ARTÍCULO 15. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del titular.</b></p> <p>1. Cuando los datos personales no se hayan obtenido del titular, el responsable del tratamiento le facilitará a este la siguiente información:</p> <p>a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

- b) Los datos de contacto del oficial de protección de datos o área encargada de datos personales.
- c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.
- d) Las categorías de datos personales de que se trate.
- e) Los destinatarios de los datos personales, si aplica.
- f) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel de adecuado de protección de la autoridad de protección de datos, o, en el caso de las transferencias indicadas en la presente ley referente a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
- g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- h) La descripción y ejercicio de los derechos que le asisten al titular.
- i) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el

consentimiento previo a la revocación.

- j) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.
- k) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de **no** facilitar tales datos.
- l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

2. El responsable del tratamiento facilitará al titular la información indicada en el numeral 1:

- a) Dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se trate dichos datos.
- b) Si los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular.
- c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2.
4. Las disposiciones de los apartados 1 a 4 no serán aplicables en la medida en que:
  - a) El titular ya disponga de la información.
  - b) La comunicación de dicha información resulte imposible o suponga una carga desproporcionada, en particular para el tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, a reserva de las condiciones y garantías indicadas en la presente ley, o en la medida en que la obligación mencionada en el numeral 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos y garantías fundamentales del titular, inclusive haciendo pública la información.
  - c) La obtención o la comunicación esté expresamente establecida por la legislación nacional que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los derechos y

<p>garantías fundamentales del titular.</p> <p>Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por la legislación nacional.</p>		
<p><b>ARTÍCULO 16. Aviso de privacidad</b></p> <ol style="list-style-type: none"> <li>1. Cuando los datos personales sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en la presente ley, facilitando al titular la información básica a la que se refiere el numeral siguiente e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.</li> <li>2. La información básica a la que se refiere el numeral anterior deberá contener, al menos:             <ol style="list-style-type: none"> <li>a) La identidad del responsable del tratamiento y de su representante legal, si aplica.</li> <li>b) La finalidad del tratamiento.</li> <li>c) La posibilidad de ejercer los derechos establecidos en los artículos 18 al 27 de la presente ley.</li> </ol> <p>Si los datos obtenidos del titular fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre éste o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo</p> </li> </ol>	<p><b>ARTÍCULO 16. Aviso de privacidad</b></p> <ol style="list-style-type: none"> <li>1. Cuando los datos personales sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en la presente ley, facilitando al titular la información básica a la que se refiere el numeral siguiente e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.</li> <li>2. La información básica a la que se refiere el numeral anterior deberá contener, al menos:             <ol style="list-style-type: none"> <li>a) La identidad del responsable del tratamiento y de su representante legal, si aplica.</li> <li>b) La finalidad del tratamiento.</li> <li>c) La posibilidad de ejercer los derechos establecidos en los artículos 18 al 27 de la presente ley.</li> </ol> <p>Si los datos obtenidos del titular fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre éste o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 25 de la presente ley.</p> <p><b><u>d) Los mecanismos dispuestos por el responsable para que el titular</u></b></p> </li> </ol>	<p>Se sugiere acotar la redacción de este artículo, considerando lo dispuesto en el Capítulo III del Decreto 1377 de 2013, particularmente lo dispuesto en los artículos 14, 15 y 16 de la norma citada.</p> <p><b>Artículo 14. Aviso de privacidad.</b> <i>En los casos en los que no sea posible poner a disposición del Titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.</i></p> <p><b>Artículo 15. Contenido mínimo del Aviso de Privacidad.</b> <i>El aviso de privacidad, como mínimo, deberá contener la siguiente información:</i></p> <ol style="list-style-type: none"> <li>1. Nombre o razón social y datos de contacto del responsable del tratamiento.</li> <li>2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.</li> <li>3. Los derechos que le asisten al titular.</li> <li>4. Los mecanismos dispuestos por el responsable para que el titular conozca la</li> </ol>

previsto en el artículo 25 de la presente ley.

3. Cuando los datos personales no hubieran sido obtenidos del titular, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 de la presente ley facilitando a aquel la información básica señalada en el numeral anterior, indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también:
  - a) Las categorías de datos objeto de tratamiento.
  - b) Las fuentes de las que procedieron los datos.

**conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.**

**No obstante, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.**

**En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.**

3. Cuando los datos personales no hubieran sido obtenidos del titular, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 de la presente ley facilitando a aquel la información básica señalada en el numeral anterior, indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también:
  - a) Las categorías de datos objeto de tratamiento.
  - b) Las fuentes de las que procedieron los datos.

4. **Los Responsables deberán conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas.**

*política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.*

*No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.*

*En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.*

***Artículo 16. Deber de acreditar puesta a disposición del aviso de privacidad y las políticas de Tratamiento de la información. Los***

*Responsables deberán conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra*

	<p><u>mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.</u></p>	<p><i>tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.</i></p> <p>Igualmente se anota que este artículo es un claro ejemplo de que muchas disposiciones del proyecto se pueden manejar vía reglamentación administrativa y no necesariamente por una ley estatutaria.</p>
<p><b>ARTÍCULO 17. Disposiciones generales sobre ejercicio de los derechos.</b></p> <ol style="list-style-type: none"> <li>1. Los derechos reconocidos en la presente ley, podrán ejercerse directamente o con el acompañamiento de los apoyos señalados en la ley 1996 de 2019 y la ley 1306 de 2009 o cualquier norma que la adicione, modifique o sustituya, o por medio de representante legal.</li> <li>2. El responsable del tratamiento estará obligado a informar al titular sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el titular. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar por otro medio y deberá redireccionarse al área encargada de atender de fondo la solicitud presentada por el titular.</li> <li>3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los titulares de sus derechos si así se estableciera en el contrato o acto jurídico que les vincule. En ningún caso ello significa pérdida de la responsabilidad que recae en el responsable del tratamiento.</li> <li>4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio</li> </ol>	<p><b>ARTÍCULO 17. Disposiciones generales sobre ejercicio de los derechos.</b></p> <ol style="list-style-type: none"> <li>1. Los derechos reconocidos en la presente ley, podrán ejercerse directamente o con el acompañamiento de los apoyos señalados en la ley 1996 de 2019 y la ley 1306 de 2009 o cualquier norma que la adicione, modifique o sustituya, o por medio de representante legal.</li> <li>2. El responsable del tratamiento estará obligado a informar al titular sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el titular. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar por otro medio y deberá redireccionarse al área encargada de atender de fondo la solicitud presentada por el titular.</li> <li>3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los titulares de sus derechos si así se estableciera en el contrato o acto jurídico que les vincule. En ningún caso ello significa pérdida de la responsabilidad que recae en el responsable del tratamiento.</li> <li>4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulada por el titular recaerá sobre el responsable.</li> </ol>	<p>La creación de sub-derechos crea confusión e incertidumbre, se insiste en la necesidad de contar con una Ley que defina principios y reglas generales, estos derechos pueden ser superados o verse afectados por cambios sociales, económicos y tecnológicos que pueden generar obsolescencia normativa.</p> <p>Así mismo, no se entiende como se “hiper regula” disposiciones y procedimientos para sub derechos de un derecho, que al final resulta ser un mismo bien jurídico protegido. Lo dispuesto y vigente en la Ley 1581 de 2012 evidencia que este trato diferencial y conceptual detallado no es necesario.</p> <p>Lo dispuesto tan al detalle en estos ejercicios, tal como información a solicitar, mecanismos de solicitud, relacionamiento con responsables y encargados debe ser objeto de reglamentación e instrucción administrativa y no parte de una Ley Estatutaria. Es por esto que se sugiere la eliminación del artículo en su totalidad.</p>

<p>de sus derechos formulada por el titular recaerá sobre el responsable.</p> <p>5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en la presente ley, se aplicará lo dispuesto en aquellas.</p> <p>6. En cualquier caso, los titulares de la patria potestad o representante legal podrán ejercitar en nombre y representación de los menores de edad los derechos de acceso, rectificación, cancelación, oposición o cualquier otro que pudieran corresponderles en el contexto de la presente ley, respetando siempre el interés superior del menor y su derecho a ser escuchado o expresar su opinión en función de su edad y madurez.</p> <p>7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en la presente ley.</p> <p>8. El ejercicio de uno o varios de los derechos no afectará negativamente al titular para el ejercicio de los demás derechos y garantías contenidos en esta norma siempre que ello fuere posible.</p>	<p><del>5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en la presente ley, se aplicará lo dispuesto en aquellas.</del></p> <p><del>6. En cualquier caso, los titulares de la patria potestad o representante legal podrán ejercitar en nombre y representación de los menores de edad los derechos de acceso, rectificación, cancelación, oposición o cualquier otro que pudieran corresponderles en el contexto de la presente ley, respetando siempre el interés superior del menor y su derecho a ser escuchado o expresar su opinión en función de su edad y madurez.</del></p> <p><del>7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en la presente ley.</del></p> <p><del>8. El ejercicio de uno o varios de los derechos no afectará negativamente al titular para el ejercicio de los demás derechos y garantías contenidos en esta norma siempre que ello fuere posible.</del></p>	
<p><b>ARTÍCULO 18. Derecho de acceso.</b></p> <p>1. El titular tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, <b>el</b> derecho de acceso a <b>tales datos</b>, y entre otra, a la siguiente información:</p> <p>a) Los fines del tratamiento.</p> <p>b) Las categorías de datos personales de que se trate.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>c) Los destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales.</p> <p>d) El plazo previsto de conservación de los datos personales o, en su defecto, los criterios utilizados para determinar este plazo.</p> <p>e) La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al titular, u oponerse a dicho tratamiento.</p> <p>f) El derecho a presentar una queja ante la autoridad de protección de datos.</p> <p>g) Cuando los datos personales no se hayan obtenido del titular, cualquier información disponible sobre su origen.</p> <p>h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. Cuando se transfieran datos personales a tercer país u organización internacional, el titular tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia en virtud de la presente ley.</p> <p>3. El responsable del tratamiento facilitará al titular una copia de los datos personales objeto de tratamiento. Cuando el titular presente la solicitud</p>		
--	--	--

<p>por medios electrónicos, a menos que solicite expresamente otro método de entrega, la información se facilitará en un formato electrónico de uso común. La entrega de la información no afectará negativamente los derechos y garantías de otras personas naturales.</p>		
<p><b>ARTÍCULO 19. Derecho de rectificación.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a obtener del responsable del tratamiento, la rectificación en condiciones de equidad de los datos personales inexactos, parciales, incompletos, fraccionados o que induzcan a error que le concierne, teniendo en cuenta los fines del tratamiento.</li> <li>2. En el caso de solicitudes relacionadas con situaciones que tengan consecuencias jurídicas significativas, el responsable del tratamiento podrá requerir pruebas que respalden la inexactitud de los datos, sin que esto suponga una carga desproporcionada para el titular.</li> </ol>	<p>Sin modificación</p>	<p>Sin modificación</p>
<p><b>ARTÍCULO 20. Derecho de supresión.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las siguientes circunstancias:             <ol style="list-style-type: none"> <li>a) Los datos personales ya no serán necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.</li> <li>b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se</li> </ol> </li> </ol>	<p><b>ARTÍCULO 20. Derecho de supresión.</b></p> <ol style="list-style-type: none"> <li>4. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las siguientes circunstancias:             <ol style="list-style-type: none"> <li>h) Los datos personales ya no serán necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.</li> <li>i) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se fundamente en otra base legitimadora.</li> </ol> </li> </ol>	<p>Es necesario que se incluya la precisión de la conservación de los datos personales en el desarrollo del derecho a la seguridad social y a la obligación legal de conservación que tienen las entidades, en el marco del régimen de la seguridad social</p>

fundamente en otra base legitimadora.

- c) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.
  - d) Los datos personales hayan sido tratados ilícitamente.
  - e) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.
  - f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.
  - g) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o la presente ley.
2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
- a) Para ejercer el derecho a la libertad de expresión e información.

- j) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.
- k) Los datos personales hayan sido tratados ilícitamente.
- l) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.
- m) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.
- n) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o la presente ley.

5. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
6. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
- a) Para ejercer el derecho a la libertad de expresión e información.
  - b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una

<p>b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.</p> <p>c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.</p> <p>d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.</p> <p>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p>	<p>función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.</p> <p>c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.</p> <p>d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.</p> <p>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p> <p>f) <b><u>Para la conservación de los datos personales en el desarrollo del derecho a la seguridad social y a la obligación legal de conservación que tienen las entidades que hacen parte de este sistema.</u></b></p>	
<p><b>ARTÍCULO 21. Derecho a la limitación del tratamiento.</b></p> <p>1. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las <b>siguientes condiciones:</b></p> <p>a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.</p> <p>b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>solicite en su lugar la limitación de su uso.</p> <p>c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de <b>reclamos</b> administrativos o judiciales.</p> <p>d) El titular se haya opuesto al tratamiento en virtud de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.</p> <p>2. Cuando el tratamiento de datos personales se haya limitado en virtud del numeral 1, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular; o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales; o con miras a la protección de los derechos de otra persona natural o jurídica o por razones de interés público.</p> <p>3. Todo titular que haya obtenido la limitación del tratamiento con arreglo al numeral 1, será informado por el responsable antes del levantamiento de dicha limitación.</p>		
<p><b>ARTÍCULO 22. Obligación de notificar la rectificación o supresión de datos personales o la limitación del tratamiento.</b></p> <p>El responsable del tratamiento notificará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo a esta ley, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado y esté en condición de demostrarlo. El responsable informará al titular</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>acerca de dichos destinatarios, si éste así lo solicita.</p>		
<p><b>ARTÍCULO 23. Derecho a la portabilidad de los datos.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común, lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:             <ol style="list-style-type: none"> <li>a) El tratamiento esté basado en el consentimiento o en un contrato con arreglo a esta ley.</li> <li>b) El tratamiento se efectúe por medios automatizados.</li> </ol> </li> <li>2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.</li> <li>3. El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio de lo dispuesto en esta ley. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento.</li> <li>4. El derecho mencionado en el numeral 1 no afectará negativamente los derechos y garantías de otras personas naturales.</li> <li>5. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada,</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.</p>		
<p><b>ARTÍCULO 24. Derecho de oposición.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en lo dispuesto en esta ley, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las garantías del titular, o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</li> <li>2. Cuando el tratamiento de datos personales tenga por objeto marketing y publicidad directa, el titular tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles en la medida en que esté relacionada con marketing y publicidad. Cuando el titular se oponga al tratamiento con fines de marketing y publicidad directa, los datos personales dejarán de ser tratados para <b>tal fin</b>.</li> <li>3. A más tardar en el momento de la primera comunicación con el titular, el derecho indicado en los numerales 1 y 2 será mencionado explícitamente al titular y será presentado claramente y</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>al margen de cualquier otra información.</p> <p>4. En el contexto de la utilización de servicios de la sociedad de la información, el titular podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.</p> <p>5. Cuando los datos personales se traten con fines de investigación científica, histórica o estadística, el titular tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de sus datos personales, salvo que sea necesario, para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas.</p>		
<p><b>ARTÍCULO 25. Decisiones individuales automatizadas, incluida la elaboración de perfiles.</b></p> <p>1. Todo titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar.</p> <p>2. El numeral 1 no se aplicará, si la decisión:</p> <ol style="list-style-type: none"> <li>Es necesaria para la celebración o la ejecución de un contrato entre el titular y un responsable del tratamiento.</li> <li>Está autorizada por una ley que se aplique al responsable del tratamiento, siempre que se establezcan medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</li> <li>Se basa en el consentimiento explícito del titular.</li> </ol>		<p>Se recomienda que el proyecto determine con precisión qué se considera "efectos jurídicos significativos" y que se establezcan medidas de transparencia adicionales, como la obligación de informar a los titulares sobre la lógica y las consecuencias del perfilamiento. Luego, al ser una definición de la autora, no se considera pertinente sugerir una definición.</p>

<p>3. En los casos a que se refiere el numeral 2, literales a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista, recibir una explicación de la decisión e impugnar la decisión.</p> <p>4. Las decisiones a las que se refiere el numeral 2, no se basarán en datos sensibles contemplados en esta ley, salvo que se apliquen las excepciones previstas en la presente ley y se hayan tomado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</p>		
<p><b>ARTÍCULO 26. Derecho a presentar una queja ante la autoridad de protección de datos.</b></p> <p>1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley, tendrá derecho a presentar una queja ante la autoridad de protección de datos.</p> <p>2. El titular o quien represente sus intereses sólo podrá elevar queja ante la autoridad de protección de datos, una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta,</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>esta no satisfaga los intereses del titular.</p>		
<p><b>ARTÍCULO 27. Derecho a presentar una denuncia ante la Autoridad de protección de datos.</b></p> <ol style="list-style-type: none"> <li>1. Quien tenga conocimiento sobre hechos que deriven en el posible incumplimiento de las disposiciones establecidas en esta ley, tendrá derecho a presentar una denuncia ante la <b>autoridad de protección</b> de datos, persiguiendo la protección del interés colectivo y el derecho a la protección de los datos personales.</li> <li>2. La denuncia podrá presentarse a nombre propio o de forma anónima. Si quien presenta la denuncia solicita a la autoridad de protección de datos la reserva de su identidad, ésta deberá adoptar las medidas técnicas necesarias para evitar a terceros conocer los datos personales del denunciante.</li> <li>3. La <b>autoridad de protección de datos</b> tendrá la obligación de examinar integralmente las denuncias presentadas por los ciudadanos. Con base en los hechos presentados, los documentos aportados y las indagaciones preliminares que realice, determinará si existe mérito o no para iniciar una investigación administrativa y, como resultado de ellas, establecerá las medidas que sean necesarias para hacer efectivo el derecho a la protección de los datos personales conforme a lo establecido en la presente ley.</li> </ol>		
<p><b>ARTÍCULO 27. Deberes del responsable del tratamiento.</b></p> <p>Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de</p>	<p><b>ARTÍCULO 28. Deberes del responsable del tratamiento.</b></p> <p>Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de</p>	<p>Se modificación ordenada, de 27 a 28.</p>

las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.
2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6 de la presente ley.
3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.
4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.
5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.
6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.
7. Cumplir con el deber de información contenido en los artículos 14 y 15 de la presente ley
8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.
9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.

las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.
2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6 de la presente ley.
3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.
4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.
5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.
6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.
7. Cumplir con el deber de información contenido en los artículos 14 y 15 de la presente ley
8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.
9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.

10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.
11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.
12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.
13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.
14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.

Con carácter extraordinario deberá realizarse dicha revisión siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.

15. Cooperar con la autoridad de protección de datos cuando lo solicite.
16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.
17. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.
18. Demostrar el cumplimiento del código de conducta al que se haya adherido,

10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.
11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.
12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.
13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.
14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.

Con carácter extraordinario deberá realizarse dicha revisión siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.

15. Cooperar con la autoridad de protección de datos cuando lo solicite.
16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.
17. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.
18. Demostrar el cumplimiento del código de conducta al que se haya adherido, de

<p>de conformidad con el artículo 42 de la presente ley.</p> <p>19. Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.</p>	<p>conformidad con el artículo 42 de la presente ley.</p> <p>Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.</p>	
<p><b>ARTÍCULO 29. Deberes del encargado del tratamiento.</b></p> <p>Los encargados del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</li> <li>2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe alguno de los principios contemplados en la presente ley o cualquier otra disposición en materia de protección, informará inmediatamente al responsable.</li> <li>3. Utilizar los datos personales objeto de tratamiento, sólo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios.</li> <li>4. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, de conformidad con el artículo 33 de la presente ley.</li> <li>5. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento.</li> <li>6. No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con autorización expresa del responsable.</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

7. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo, incluso después de que finalice el mismo.
8. Garantizar que el personal, con acceso a datos personales objeto del encargo reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad. El encargado debe mantener a disposición del responsable y/o la autoridad competente, la documentación que demuestre el cumplimiento de estas obligaciones.
9. El encargado informará al responsable del tratamiento, sobre cualquier incidente de seguridad relacionado con los datos personales objeto del tratamiento, proporcionando toda la información pertinente necesaria para documentar y notificar el incidente a la autoridad de protección de datos.
10. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.
11. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.
12. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea el caso, de conformidad con el artículo 38 de la presente ley.
13. Poner a disposición del responsable o de la Autoridad de Protección de Datos, toda la información necesaria para demostrar el cumplimiento de sus obligaciones.
14. Implantar las medidas de seguridad acordadas con el responsable del tratamiento, así como aquellas que

<p>correspondan en función del riesgo asociado a la prestación del servicio.</p> <p>15. Eliminar o devolver al responsable del tratamiento los datos personales, así como los soportes en los que estén almacenados, una vez finalizada la prestación del servicio. La devolución debe incluir la eliminación completa de los datos almacenados en los equipos informáticos utilizados por el encargado, a menos que existan excepciones legales y/ o contractuales.</p> <p>16. Cooperar con la autoridad de protección de datos cuando lo solicite.</p>		
<p><b>ARTÍCULO 30. Protección de datos desde el diseño y por defecto.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y garantías de las personas naturales, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la presente ley y proteger los derechos de los titulares.</p> <p>2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles.</p> <p>Tendrá acceso únicamente el personal autorizado, salvo que se modifique en razón de las circunstancias del tratamiento.</p> <p>3. Para el cumplimiento de lo establecido en los numerales 1 y 2, el responsable del tratamiento tendrá en cuenta:</p> <ul style="list-style-type: none"> <li>a) La protección de los datos personales de forma proactiva y no reactiva.</li> <li>b) La protección de los datos personales preventiva y no correctiva.</li> <li>c) La privacidad como configuración predeterminada.</li> <li>d) La protección de los datos en el ciclo de vida completo de su tratamiento, es decir, desde la recolección hasta su posible supresión.</li> <li>e) La transparencia en el tratamiento de los datos.</li> <li>f) La prevalencia de la privacidad como interés del titular.</li> </ul> <p>4. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 60, como elemento que acredite el cumplimiento de las obligaciones establecidas en los numerales 1 y 2 del presente artículo.</p>		
<p><b>ARTÍCULO 31. Corresponsables del tratamiento.</b></p> <p>1. Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables</p>	Sin modificaciones	Sin modificaciones

<p>determinarán de modo transparente y de mutuo acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por la presente ley, en particular, en el ejercicio de los derechos de los titulares y sus obligaciones de suministro de información, a las cuales se refiere la presente ley.</p> <p>2. El acuerdo indicado en el numeral 1, reflejará adecuadamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.</p> <p>3. Independientemente de los términos del acuerdo a que se refiere el numeral 1, los titulares podrán ejercer los derechos que les reconoce la presente ley frente a cada uno de los responsables.</p>		
<p><b>ARTÍCULO 32. Encargado del tratamiento.</b></p> <p>1. El encargado del tratamiento no recurrirá a otro encargado sin la autorización, específica o general, del responsable ya sea por escrito o por mensajes de datos suficientes y verificables.</p> <p>Cuando la autorización para el subencargo del tratamiento sea general, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.</p> <p>2. El tratamiento debe regirse por un contrato u otro acto jurídico con arreglo a las leyes civiles o mercantiles, que vincule al encargado respecto del</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

responsable y establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de titulares, categorías de datos personales, las obligaciones y los derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:

- a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país u organización internacional, salvo que esté obligado a ello en virtud de un mandato legal que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que dicho mandato lo prohíba por razones importantes de interés público.
- b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza contractual.
- c) Tomará todas las medidas necesarias de conformidad a la presente ley.
- d) Respetará las condiciones indicadas en la presente ley para recurrir a un subencargado del tratamiento.
- e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su

obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares o podrá comprometerse a resolver, por cuenta del responsable y dentro de los plazos establecidos en esta ley, las solicitudes de ejercicio de derechos.

- f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en la presente ley, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.
- g) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud de una disposición legal o por motivos de responsabilidad derivada de su relación.
- h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

3. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe la presente ley u otras disposiciones en materia de protección de datos.

4. Cuando un encargado del tratamiento recurra a un subencargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este subencargado, las mismas obligaciones de protección de datos que las estipuladas en el contrato entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones de la presente ley. Si el subencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro.
5. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como lo indica esta ley, podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a **las** que se refiere el presente artículo.
6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato que menciona los numerales 2 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales modelo, las cuales hacen alusión a los numerales 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con esta ley.
7. La autoridad de protección de datos podrá fijar cláusulas contractuales modelo, para los contratos a los que

hacen mención los numerales 2 y 4 del presente artículo.

8. El contrato al cual se refieren los numerales 2 y 4 deberá constar por escrito, inclusive en formato electrónico.
9. Sin perjuicio de lo dispuesto en esta ley, si un encargado o subencargado del tratamiento infringe la presente ley, al determinar los fines y medios del tratamiento, será considerado responsable con respecto a dicho tratamiento.
10. El responsable del tratamiento podrá exigir a los encargados que sean proveedores de servicios tecnológicos, aplicaciones e infraestructura tecnológica, con los que esté adherido o se vaya a adherir a través de condiciones generales de contratación, que demuestre el cumplimiento de la presente ley. En caso de que el proveedor ignore las solicitudes realizadas por los responsables o incumpla con la presente ley, los responsables podrán denunciar dicha situación ante la autoridad de protección de datos, de conformidad con lo establecido en el artículo 27 de la presente ley.

Lo anterior no exonera al responsable del tratamiento del cumplimiento de las obligaciones establecidas en el artículo 28 de la presente ley.

*Parágrafo primero.* Las obligaciones establecidas en esta ley para los encargados del tratamiento serán de aplicación directa para quienes, en atención a lo dispuesto en los numerales 2 y 4 del presente artículo, adquieran la calidad de subencargados.

*Parágrafo segundo.* El encargado del tratamiento y cualquier persona que actúe bajo el control del responsable o del encargado y

<p>tenga acceso a datos personales, sólo podrán tratar dichos datos siguiendo instrucciones del responsable, a menos que no estén obligados a ello en virtud de una disposición legal.</p>		
<p><b>ARTÍCULO 33. Registro de las actividades de tratamiento.</b></p> <p>1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su control. Dicho registro deberá contener toda la información indicada a continuación:</p> <ul style="list-style-type: none"> <li>a) El nombre y los datos de contacto del responsable y, cuando sea el caso, del corresponsable, y del oficial de protección de datos o área encargada.</li> <li>b) Los fines del tratamiento.</li> <li>c) Una descripción de los tipos de titulares y de las categorías de datos personales.</li> <li>d) Los destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en otros países u organizaciones internacionales.</li> <li>e) Los encargados que intervienen en el tratamiento.</li> <li>f) De ser procedente, las transferencias de datos personales a otro país o una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de las transferencias indicadas en el artículo 33 de la presente esta ley relativa a la documentación de garantías adecuadas.</li> <li>g) Cuando sea posible, los plazos previstos para la supresión de</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

las diferentes categorías de datos.

h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.

i) Los responsables del tratamiento, deben inscribir sus registros de actividades ante el Registro Nacional de las Actividades, administrado por la autoridad de protección de datos y de libre consulta para los ciudadanos.

2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos o área encargada.

b) Las categorías de tratamientos efectuados por cuenta de cada responsable.

c) Los subencargados autorizados por el responsable, que intervienen en el tratamiento.

d) De ser procedente, las transferencias de datos personales a otro país u organización internacional, incluida la identificación de dicho país u organización internacional y en el caso de las transferencias indicadas en esta ley, relativo a la documentación de garantías adecuadas.

<p>e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.</p> <p>3. Los registros a los que se refieren los numerales 1 y 2 constarán por escrito, inclusive en formato electrónico.</p> <p>4. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de protección de datos, cuando lo requiera.</p> <p>Los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, harán público el registro de sus actividades de tratamiento accesible por medios electrónicos, en el que constará la información establecida en el presente artículo.</p>		
<p><b>ARTÍCULO 34. Bloqueo de los datos.</b></p> <p>1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.</p> <p>2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, Fiscalía General de la Nación o las Administraciones Públicas competentes, en particular de la autoridad de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>mismas. Transcurrido ese plazo, se procederá a la destrucción de los datos.</p> <p>3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.</p> <p>4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información, de manera que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.</p> <p>La autoridad de protección de datos, dentro del ámbito de sus competencias, podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de titulares afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los titulares, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.</p>		
<p><b>ARTÍCULO 35. Seguridad del tratamiento.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>seguridad adecuado al riesgo, que en su caso incluya, entre otros:</p> <ul style="list-style-type: none"> <li>a) La seudonimización y el cifrado de datos personales.</li> <li>b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.</li> <li>c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.</li> <li>d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.</li> </ul> <p>2. Al evaluar la adecuación del nivel de seguridad, se tendrá en cuenta los riesgos que presente el tratamiento de datos, en particular, la destrucción, pérdida, alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales.</p> <p>3. La adhesión a un código de conducta aprobado de conformidad con el artículo 42 o a un mecanismo de certificación aprobado de conformidad con el artículo 45, así como, la adopción de directrices dadas por la autoridad de protección de datos o indicaciones proporcionadas por un oficial de protección de datos podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el numeral 1 del presente artículo.</p>		
---	--	--

<p>4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, sólo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello por la ley.</p>		
<p><b>ARTÍCULO 36. Notificación de un Incidente de seguridad de los datos personales a la autoridad de protección de datos.</b></p> <p>1. En caso de incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de protección de datos de conformidad con esta ley, sin demora injustificada y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la autoridad de protección de datos no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación.</p> <p>2. El encargado del tratamiento notificará, sin demora injustificada, al responsable del tratamiento, los incidentes de seguridad de los datos personales de los que tenga conocimiento.</p> <p>3. La notificación contemplada en el numeral 1 deberá, como mínimo:</p> <p>a) Describir la naturaleza del Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado, tipo de titulares afectados, las categorías de datos y el número aproximado de registros de datos personales afectados.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto, en el que pueda obtenerse más información.</p> <p>c) Describir las posibles consecuencias del incidente de seguridad de los datos personales.</p> <p>d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento, para poner remedio al incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.</p> <p>4. Si no fuera posible facilitar la información descrita en el numeral 3 del presente artículo, simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin demora injustificada.</p> <p>5. El responsable del tratamiento documentará cualquier incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de protección de datos, verificar el cumplimiento de lo dispuesto en el presente artículo.</p> <p>Los datos personales contenidos en la notificación de un incidente de seguridad y que fueron comunicados a la autoridad de protección de datos, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante el incidente,</p>		
---	--	--

adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.		
<p><b>ARTÍCULO 37. Comunicación de un Incidente de seguridad de los datos personales al titular.</b></p> <ol style="list-style-type: none"> <li>1. Cuando sea probable que el incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin demora injustificada.</li> <li>2. La comunicación al titular contemplada en el numeral 1 del presente artículo, deberá describir en un lenguaje claro y sencillo la naturaleza del incidente de seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 36, numeral 3, literales b), c) y d).</li> <li>3. La comunicación al titular a la que se refiere el numeral 1, no será necesaria si se cumple alguna de las siguientes condiciones:                         <ol style="list-style-type: none"> <li>a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.</li> <li>b) El responsable del tratamiento ha tomado medidas ulteriores que garantizan que ya no exista la probabilidad de que se materialice el alto riesgo para</li> </ol> </li> </ol>	Sin modificaciones	Sin modificaciones

<p>los derechos y garantías del titular.</p> <p>4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, <b>éste</b> podrá optar por una comunicación pública o una medida de difusión semejante, de manera que se informe efectivamente a los titulares.</p> <p>5. Cuando el responsable no haya comunicado al titular el incidente de seguridad de los datos personales, la autoridad de protección de datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.</p>		
<p><b>ARTÍCULO 38. Evaluación de impacto relativa a la protección de datos y consulta previa.</b></p> <p>1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.</p> <p>2. El responsable del tratamiento solicitará asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.</p>	Sin modificaciones	Sin modificaciones

3. La evaluación de impacto relativa a la protección de los datos, a los que se refiere el numeral, 1 se requerirá en especial cuando:

- a) Se realice evaluación sistemática y exhaustiva de aspectos personales de personas naturales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de forma similar.
- b) Tratamiento a gran escala de datos sensibles o de los datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.
- c) Observación sistemática a gran escala de una zona de acceso público.
- d) Se efectúen tratamientos sobre neurodatos.

4. La autoridad de protección de datos establecerá y publicará una lista de los tipos de operaciones de tratamiento, que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el numeral 1.

5. La evaluación a la que se refiere el numeral 1 del presente artículo, deberá incluir como mínimo:

- a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.
- b) Una evaluación de la necesidad y la

proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

- c) Una evaluación de los riesgos para los derechos y garantías de los titulares a los que se refiere el numeral 1.
  - d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos y garantías de los titulares y de otras personas afectadas.
6. El cumplimiento de los códigos de conducta aprobados, a los que se refiere el artículo 38, por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.
7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.
8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la

<p>evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.</p> <p>9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La autoridad de protección de datos deberá emitir un concepto en el menor tiempo posible.</p> <p><i>Parágrafo:</i> La zona de acceso público a la que se refiere el numeral 3 literal c) del presente artículo, hace referencia a cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas naturales, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.</p>		
<p><b>ARTÍCULO 39. Designación del Oficial de protección de datos.</b></p> <p>1. El responsable y el encargado del tratamiento designarán un oficial de protección de datos siempre que:</p> <p>a) El tratamiento lo lleve a cabo los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa,</p>	Sin modificaciones	Sin modificaciones

los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas.

b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares a gran escala.

c) Las actividades principales del responsable o del encargado, consistan en el tratamiento a gran escala de datos sensibles y de datos relativos a antecedentes penales, anotaciones judiciales o contravencionales, y/o sanciones administrativas.

d) La autoridad de protección de datos podrá definir nuevas indicaciones en las que se deba designar un Oficial de protección de datos y estipulará las condiciones y particularidades para dicha designación.

2. Un grupo empresarial podrá nombrar un único oficial de protección de datos, siempre que sea fácilmente accesible desde cada una de las empresas que pertenecen al grupo.

3. Cuando el responsable o el encargado del tratamiento sea una entidad u organismo público, se podrá designar un único oficial de protección de datos para varias de estas entidades u organismos, teniendo en cuenta su estructura administrativa y tamaño.

4. En casos distintos de los contemplados en el numeral 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a sectores a los que pertenezcan los responsables o encargados, podrán designar de forma voluntaria un oficial de protección de datos.
5. El oficial de protección de datos será designado siempre que cuente con un perfil legal o un perfil interdisciplinario con conocimientos legales y experiencia en protección de datos. Además, se verificará su capacidad para desempeñar las funciones indicadas en esta ley.
6. El oficial de protección de datos podrá vincularse con el responsable o el encargado del tratamiento por medio de un contrato de prestación de servicios o un contrato laboral.
7. El responsable o el encargado del tratamiento publicará los datos de contacto del oficial de protección de datos y los comunicará a la autoridad de protección de datos en un plazo de quince (15) días hábiles.  
  
Las designaciones, nombramientos y ceses de los oficiales de protección de datos, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria, también deberán ser notificadas en el mismo término.
8. La autoridad de protección de datos, mantendrá en el ámbito de sus competencias, una lista actualizada de oficiales de protección de datos que será accesible **a través de** medios electrónicos.
9. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento, podrán

<p>establecer la dedicación completa o a tiempo parcial del oficial, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos y garantías de los titulares.</p>		
<p><b>ARTÍCULO 40. Posición del oficial de protección de datos.</b></p> <ol style="list-style-type: none"> <li>1. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relacionadas con la protección de datos personales.</li> <li>2. El responsable y el encargado del tratamiento respaldarán al oficial de protección de datos en el desempeño de las funciones estipuladas en la presente ley, facilitando los recursos necesarios para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento.</li> <li>3. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurrieren en dolo o negligencia grave en su ejercicio. El oficial de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.</li> <li>4. Los titulares podrán ponerse en contacto con el oficial de protección de datos, en relación a todas las cuestiones correspondientes al tratamiento de sus datos personales y al ejercicio de sus derechos y garantías al amparo de la presente ley.</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>5. El oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el artículo 74 de la Constitución Política.</p> <p>6. El oficial de protección de datos podrá desempeñar otras funciones y el responsable o encargado del tratamiento garantizará que estas no den lugar a conflicto de intereses.</p> <p>7. El oficial de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la autoridad de protección de datos. El oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.</p>		
<p><b>ARTÍCULO 41. Funciones del oficial de protección de datos.</b></p> <p>1. El oficial de protección de datos tendrá como mínimo las siguientes funciones:</p> <ul style="list-style-type: none"> <li>a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les competen en virtud de la ley y otras disposiciones referentes a la protección de datos.</li> <li>b) Supervisar el cumplimiento de lo dispuesto en la presente ley.</li> <li>c) Supervisar la implementación y aplicación de un manual interno de políticas y procedimiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y</li> </ul>	Sin modificaciones	Sin modificaciones

<p>las auditorías correspondientes.</p> <p>d) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos y supervisar su aplicación de conformidad con la presente ley.</p> <p>e) Cooperar con la autoridad de protección de datos.</p> <p>f) Actuar como punto de contacto de la autoridad de protección de datos, sobre cuestiones relativas al tratamiento, incluida la consulta previa a la que se refiere el artículo 38, numeral 9, así como solicitar instrucciones, en su caso, sobre cualquier otro asunto.</p> <p>g) Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.</p> <p>2. El oficial de protección de datos, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.</p>		
<p><b>ARTÍCULO 44. Códigos de conducta.</b></p> <p>1. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y</p>	<p><b>ARTÍCULO 44. Códigos de conducta.</b></p> <p><del>8. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y las necesidades</del></p>	<p>En la numeración del articulado, salta del artículo 41 al artículo 44.</p> <p>El capítulo V, es a todas luces inconveniente, la autorregulación es una medida excepcional que nace de un mismo mercado para propender por la protección y</p>

las necesidades específicas de las microempresas, las pequeñas y medianas empresas.

2. Las asociaciones y otras entidades representativas de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:

- a) El tratamiento leal y transparente.
- b) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.
- c) La recogida de datos personales.
- d) La seudonimización de datos personales.
- e) La información proporcionada al público y a los titulares.
- f) El ejercicio de los derechos de los titulares.
- g) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.
- h) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.
- i) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.
- j) La transferencia de datos personales a terceros países u organizaciones internacionales.

~~específicas de las microempresas, las pequeñas y medianas empresas.~~

~~9. Las asociaciones y otras entidades representativas de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:~~

- ~~l) El tratamiento leal y transparente.~~
- ~~m) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.~~
- ~~n) La recogida de datos personales.~~
- ~~e) La seudonimización de datos personales.~~
- ~~p) La información proporcionada al público y a los titulares.~~
- ~~q) El ejercicio de los derechos de los titulares.~~
- ~~r) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.~~
- ~~s) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.~~
- ~~t) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.~~
- ~~u) La transferencia de datos personales a terceros países u organizaciones internacionales.~~
- ~~v) Los procedimientos extrajudiciales y otros~~

desarrollo del sector, tal y como ocurre con la autorregulación del mercado de valores y la de anunciantes publicitarios. En esa medida, establecer mecanismos de autorregulación transversales para tantos sectores que pueden adelantar tratamiento de datos es un error y puede generar profundos malentendidos. Por ejemplo, no es lo mismo tratar datos en el sector financiero, que en el sector salud. Si se requirieran medidas de autorregulación razonables debería existir una medida de autorregulación de tratamiento de datos para cada sector, lo que es un sinsentido en la práctica.

Así mismo, crear otras autoridades institucionales privadas aumentaría la carga de cumplimiento y resulta desproporcionado. Los criterios de interpretación y aplicación de normativa de tratamiento de datos, al considerar un derecho fundamente, no deben quedar en manos de entes privados.

Por lo anterior, se propone la eliminación total del artículo.

<p>k) Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los titulares relativos al tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.</p> <p>3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.</p> <p>Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p> <p>4. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.</p> <p>5. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la</p>	<p><del>procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los titulares relativos al tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.</del></p> <p><del>10. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.</del></p> <p><del>Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.</del></p> <p><del>11. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.</del></p> <p><del>12. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la modificación o ampliación a la autoridad de protección de datos.</del></p>	
---	--	--

<p>modificación o ampliación a la autoridad de protección de datos.</p> <p>La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.</p> <p>6. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.</p> <p>7. La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.</p>	<p><del>La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.</del></p> <p><del>13. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.</del></p> <p><del>La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.</del></p>	
<p><b>ARTÍCULO 43. Supervisión de códigos de conducta aprobados.</b></p> <p>1. Podrá supervisar el cumplimiento de un código de conducta, una entidad que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditada para tal fin por la autoridad de protección de datos, sin perjuicio de las funciones y facultades de esta.</p> <p>2. La autoridad de protección de datos fijará los criterios de acreditación de las entidades a las que se refiere el presente artículo.</p> <p>3. Sin perjuicio de las funciones y las facultades de la autoridad de protección de datos, en virtud del numeral 1 del presente artículo, la entidad acreditada deberá, con sujeción a las garantías del debido proceso, tomar las medidas oportunas en caso de infracción del código por un</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>responsable o encargado del tratamiento, incluida la suspensión o exclusión de este.</p> <p>Informará de dichas medidas y sus razones, a la autoridad de protección de datos.</p> <p>4. La autoridad de protección de datos podrá revocar la acreditación de una entidad de conformidad con el numeral 1, si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicha entidad infringe la presente ley.</p> <p>5. El presente artículo no se aplicará al tratamiento realizado por autoridades y entidades públicas.</p>		
<p><b>ARTÍCULO 44. Deberes de las entidades supervisoras de códigos de conducta.</b></p> <p>Las entidades supervisoras de códigos de conducta deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>1. Demostrar, a satisfacción de la autoridad de protección de datos, su independencia y pericia en relación con el objeto del código.</li> <li>2. Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.</li> <li>3. Establecer procedimientos y estructuras para tratar los reclamos relativos a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>tratamiento, para hacer que estos sean transparentes para los titulares y el público en general.</p> <p>4. Demostrar, a satisfacción de la autoridad de protección de datos, que sus funciones y objetivos no dan lugar a conflicto de intereses.</p>		
<p><b>ARTÍCULO 45. Certificación.</b></p> <p>1. La Autoridad de protección de datos promoverá, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en la presente ley, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados conforme al numeral 5 del presente artículo, con el objetivo de demostrar que los responsables o encargados no sujetos a la presente ley, según lo establecido en el artículo 3, ofrecen garantías adecuadas en el contexto de transferencias internacionales de datos personales a terceros países u organizaciones internacionales, según lo dispuesto en el artículo 49, numeral 2, literal e).</p> <p>Los responsables o encargados mencionados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas aquellas relativas a los derechos de los titulares.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.
4. La certificación a la que se refiere el presente artículo, no limitará las obligaciones del responsable o encargado del tratamiento en cuanto al cumplimiento de la presente ley y se entenderá sin perjuicio de las funciones y las facultades de la autoridad de protección de datos.
5. La certificación en virtud del presente artículo será expedida por las entidades de certificación o por la autoridad de protección de datos, sobre la base de los criterios aprobados por ésta.
6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación, darán a la entidad de certificación o en su caso a la autoridad de protección de datos, toda la información y acceso a sus actividades de tratamiento que requieran para llevar a cabo el procedimiento de certificación.
7. La certificación se expedirá a un responsable o encargado del tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.  
  
La certificación será retirada, cuando proceda, por las entidades de certificación, o en su caso por la autoridad de protección de datos, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la misma.
8. La autoridad de protección de datos llevará en un registro todos los mecanismos de certificación, sellos y marcas de protección de datos y los

<p>pondrá a disposición pública por cualquier medio apropiado.</p> <p><i>Parágrafo primero:</i> Serán entidades certificadoras aquellas que hayan sido acreditadas por un organismo del subsistema nacional de calidad, el cual tenga la pericia necesaria para evaluar si los aspirantes a entidades certificadoras cuentan con un nivel adecuado de competencia en materia de protección de datos.</p> <p><i>Parágrafo segundo:</i> La autoridad de protección de datos hará públicos los requisitos y los criterios a los que se refiere el numeral 5 del presente artículo, en una forma fácilmente accesible.</p>		
<p><b>ARTÍCULO 46. Deberes de las entidades certificadoras.</b></p> <p>Las entidades certificadoras deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>1. Demostrar ante la autoridad de protección de datos y/o los sujetos interesados en la certificación que se encuentran acreditadas por un organismo del subsistema nacional de calidad.</li> <li>2. Respetar y cumplir los criterios de certificación aprobados por la autoridad de protección de datos.</li> <li>3. Establecer procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas de protección de datos en los términos descritos en el numeral 7 del artículo 45.</li> <li>4. Establecer procedimientos y estructuras para tratar los reclamos relativos al retiro de la certificación por</li> </ol>	Sin modificaciones	Sin modificaciones

<p>el incumplimiento de los requisitos por parte de un responsable o encargado del tratamiento.</p> <p>5. Informar a la autoridad de protección de datos sobre las razones para la retirada de una certificación a un responsable o encargado del tratamiento.</p>		
<p><b>ARTÍCULO 47. Regla general de las transferencias.</b></p> <p>Solo se realizarán transferencias de datos personales si, a reserva de las demás disposiciones de la presente ley, el responsable o el encargado del tratamiento cumplen las condiciones establecidas en el presente título, incluidas las relativas a las transferencias ulteriores de datos personales. Todas las disposiciones del presente título se aplicarán, a fin de asegurar un nivel adecuado en materia de protección de datos personales.</p> <p><i>Parágrafo:</i> Se considera transferencia la salida de datos fuera del territorio nacional, bien sea por cesión o comunicación de datos, o por un tratamiento de datos personales por parte del encargado del tratamiento.</p>	Sin modificaciones	Sin modificaciones
<p><b>ARTÍCULO 48. Transferencias basadas en un nivel adecuado de protección.</b></p> <p>1. Se podrán realizar transferencias de datos personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos.</p> <p>2. Se entiende que un tercer país, un territorio, uno o varios sectores específicos del tercer país, o una organización internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a los</p>	Sin modificaciones	Sin modificaciones

sujetos obligados. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos deberá tener en cuenta los siguientes elementos:

- a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales;
- b) La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;
- c) La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales;
- d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Protección de Datos.

3. La declaración de nivel adecuado establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Cuando la información disponible, muestre que un tercer país, un territorio o un sector específico de ese tercer

<p>país, o una organización internacional ya no garantiza un nivel de protección adecuado de conformidad con lo dispuesto por el presente artículo, la Autoridad de Protección de Datos, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión adecuación.</p> <p><i>Parágrafo primero:</i> La autoridad de protección de datos habilitará canales de contacto para que el tercer país u organización internacional, pueda subsanar la situación que dé lugar a la decisión adoptada, de conformidad con el numeral 3.</p>		
<p><b>ARTÍCULO 49. Transferencias mediante garantías adecuadas.</b></p> <ol style="list-style-type: none"> <li>1. A falta de declaración de nivel adecuado de protección, en los términos del artículo 48, el responsable o el encargado del tratamiento sólo podrá transferir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los titulares cuenten con derechos exigibles y acciones legales efectivas.</li> <li>2. Las garantías adecuadas con arreglo al numeral 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de la autoridad de protección de datos, por:             <ol style="list-style-type: none"> <li>a) Un instrumento jurídicamente vinculante y exigible, bilateral o multilateral, entre Colombia y otros países u organizaciones internacionales, que habilite las transferencias desde entidades u organismos públicos establecidas en Colombia hacia entidades u organismos públicos establecidas en otros países.</li> </ol> </li> </ol>	Sin modificaciones	Sin modificaciones

<p>b) Normas corporativas vinculantes de conformidad con el artículo 50 de la presente ley.</p> <p>c) Cláusulas contractuales modelo. La autoridad de protección de datos, establecerá los criterios bajo los cuales se deben elaborar las cláusulas.</p> <p>d) Un código de conducta aprobado con arreglo a la presente ley, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p> <p>e) Un mecanismo de certificación aprobado con arreglo al artículo 45, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p> <p>3. Siempre que exista declaración de nivel adecuado de protección, expedida por la autoridad de protección de datos, las garantías adecuadas contempladas en el numeral 1 podrán igualmente ser aportadas, en particular, mediante:</p> <p>a) Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.</p> <p>b) Disposiciones que se incorporen en acuerdos administrativos entre las</p>		
---	--	--

<p>entidades u organismos públicos, que incluyan derechos efectivos y exigibles para los titulares.</p>		
<p><b>ARTÍCULO 50. Normas corporativas vinculantes.</b></p> <p>1. La autoridad de protección de datos aprobará normas corporativas vinculantes, siempre que estas:</p> <ul style="list-style-type: none"> <li>a) Sean jurídicamente vinculantes y se apliquen a todos los miembros que hacen parte del mismo grupo de empresas o de la unión de empresas dedicadas a una actividad económica conjunta.</li> <li>b) Confieran expresamente a los titulares derechos exigibles previstos en los artículos 18 al 27 de la presente ley.</li> <li>c) Cumplan los requisitos establecidos en el numeral 2 del presente artículo.</li> </ul> <p>2. Las normas corporativas vinculantes mencionadas en el numeral 1 especificarán, como mínimo, los siguientes elementos:</p> <ul style="list-style-type: none"> <li>a) La estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.</li> <li>b) Las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamiento y sus fines, el tipo de titulares afectados y el nombre de los países en cuestión.</li> <li>c) Su carácter jurídicamente vinculante, tanto a nivel interno como externo.</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

- d) La aplicación de los principios generales en materia de protección de datos establecidos en la presente ley.
- e) Los derechos de los titulares en relación con el tratamiento y los medios para ejercerlos.
- f) La forma en que se facilita a los titulares la información, sobre las normas corporativas vinculantes.
- g) Las funciones del o los oficiales de protección de datos, designados de conformidad con el artículo 39, de cualquier otra persona o entidad encargada de la supervisión y del cumplimiento de las normas corporativas vinculantes, así como de la supervisión de la formación y de la tramitación de las reclamaciones.
- h) Los procedimientos de reclamaciones.
- i) Los mecanismos establecidos, para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas con el fin de proteger los derechos del titular.
- j) Los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de protección de datos.
- k) Los mecanismos para informar a la autoridad de protección de

datos de cualquier requisito jurídico de aplicación en un tercer país a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes.

l) La formación en protección de datos pertinente, para el personal que tenga acceso permanente o habitual a datos personales.

3. La autoridad de protección de datos podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y la autoridad de control en relación con las normas corporativas vinculantes según lo dispuesto en el presente artículo.

*Parágrafo primero.* Las Normas Corporativas Vinculantes sólo podrán ser sometidas a la aprobación de la autoridad de protección de datos una vez hayan sido aprobadas por el órgano correspondiente según los estatutos de la sociedad o los acuerdos del grupo empresarial. Las normas que sean formalmente presentadas ante la autoridad de protección de datos sólo estarán vigentes a partir de la fecha en que ésta emita su certificación y a partir de ese momento, se podrán aplicar.

*Parágrafo segundo.* En los casos en que las normas no sean aprobadas, los ajustes requeridos por la autoridad de protección de datos, una vez realizados, deben contar con la aprobación del órgano social o contractual correspondiente, antes de ser sometidas, nuevamente, a aprobación.

<p><b>ARTÍCULO 51. Excepciones para situaciones específicas.</b></p> <p>1. En ausencia de una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, una transferencia o conjunto de transferencias de datos personales a terceros países u organizaciones internacionales sólo podrá realizarse si se cumplen alguna de las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>a) El titular haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias debido a la ausencia de una declaración de nivel adecuado de protección y de garantías adecuadas.</li> <li>b) La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.</li> <li>c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular, entre el responsable del tratamiento y otra persona natural o jurídica.</li> <li>d) La transferencia sea necesaria por razones importantes de interés público.</li> <li>e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones judiciales o administrativas.</li> <li>f) La transferencia sea necesaria para proteger los intereses</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
--	---------------------------	---------------------------

vitales del titular o de otras personas, cuando el titular esté física o jurídicamente incapacitado para dar su consentimiento.

g) La transferencia se realice desde un registro público destinado a facilitar información y esté accesible para consulta por el público en general o cualquier persona con un interés legítimo, siempre que se cumplan las condiciones establecidas por la ley para dicha consulta en cada caso particular. En tal situación, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro público. Si la finalidad del registro es la consulta por parte de personas con un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

2. Cuando una transferencia no pueda basarse en una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, y no se aplique ninguna de las excepciones para situaciones específicas mencionadas en el numeral primero del presente artículo, sólo podrá llevarse a cabo si se cumplen las siguientes condiciones:

- a) No es repetitiva.
- b) Afecta sólo a un número limitado de titulares.
- c) Es necesaria para fines e intereses legítimos imperiosos perseguidos por el responsable del tratamiento, sobre los cuales no prevalecen

los intereses, derechos y garantías del titular. El responsable del tratamiento informará al titular, de la transferencia y de los intereses legítimos imperiosos perseguidos.

d) El responsable del tratamiento ha evaluado los riesgos y basándose en esta evaluación ha ofrecido garantías apropiadas con respecto a la protección de datos personales.

Adicionalmente, el responsable del tratamiento informará a la autoridad de protección de datos sobre la transferencia y a los titulares de los intereses legítimos imperiosos perseguidos con dicha transferencia.

3. El numeral 1, literales a), b) y c), y el numeral 2 no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus funciones.
4. En ausencia de una declaración de nivel adecuado de protección, una normativa con rango de ley, podrá por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional.
5. El responsable o el encargado del tratamiento documentará en los registros de las actividades del tratamiento, la evaluación y las garantías apropiadas a las que se refiere el numeral 2 del presente artículo.

<p><b>ARTÍCULO 52. Cooperación internacional en el ámbito de la protección de datos personales.</b></p> <p>En relación con terceros países y organizaciones internacionales, la autoridad de protección de datos tomará medidas apropiadas para:</p> <ul style="list-style-type: none"> <li>a) Crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales.</li> <li>b) Prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y garantías fundamentales.</li> <li>c) Asociar a partes interesadas en la materia, a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales.</li> <li>d) Promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
<p><b>ARTÍCULO 53. Autoridad de Protección de Datos.</b></p> <ul style="list-style-type: none"> <li>1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de protección de datos personales, garantizando el efectivo cumplimiento de los principios, derechos, garantías y los</li> </ul>	<p><b>ARTÍCULO 53. Autoridad de Protección de Datos.</b></p> <ul style="list-style-type: none"> <li>1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de protección de datos personales, garantizando el efectivo cumplimiento de los principios, derechos, garantías y los procedimientos</li> </ul>	<p>Para efectos de evitar colisión y conflictos de competencias, este artículo debe establecer un parámetro claro de coordinación entre las entidades nacionales que tienen la función de vigilancia en temas de protección de datos personales. Es decir, que haya una coordinación</p>

<p>procedimientos establecidos en la presente ley en aras de facilitar la libre circulación de datos.</p> <ol style="list-style-type: none"> <li>2. Sin perjuicio de lo mencionado, cuando el tratamiento de datos personales dé lugar a un comportamiento delictivo, la Fiscalía General de la Nación será la encargada de la persecución penal de dichas conductas.</li> <li>3. La autoridad de protección de datos, tendrá a su cargo las funciones de inspección, vigilancia y control, las cuales se desarrollarán en cumplimiento de las facultades otorgadas en la presente ley.</li> <li>4. Para el ejercicio de sus funciones, deberán tenerse en cuenta las garantías constitucionales y principios generales que regulan el actuar de la autoridad de protección de datos, garantizando en todo momento el derecho al debido proceso y demás garantías procesales.</li> </ol>	<p>establecidos en la presente ley en aras de facilitar la libre circulación de datos.</p> <ol style="list-style-type: none"> <li>2. Sin perjuicio de lo mencionado, cuando el tratamiento de datos personales dé lugar a un comportamiento delictivo, la Fiscalía General de la Nación será la encargada de la persecución penal de dichas conductas.</li> <li>3. La autoridad de protección de datos, tendrá a su cargo las funciones de inspección, vigilancia y control, las cuales se desarrollarán en cumplimiento de las facultades otorgadas en la presente ley.</li> <li>4. Para el ejercicio de sus funciones, deberán tenerse en cuenta las garantías constitucionales y principios generales que regulan el actuar de la autoridad de protección de datos, garantizando en todo momento el derecho al debido proceso y demás garantías procesales.</li> </ol> <p><b><u>Parágrafo: Para efectos de este artículo, las autoridades gubernamentales que ejercen funciones de control y vigilancia sobre el tratamiento de datos personales, definirán sus criterios de coordinación para el ejercicio de sus funciones.</u></b></p>	<p>liderada por la SIC para que expidan solicitudes y regulaciones afines en lo que corresponda y que no sean contradictorias, con la SFC (autoridad de protección de datos personales de las entidades financieras en los términos del objeto de la Ley Estatutaria 1266 de 2008.).</p> <p><i>Art. 17 de la Ley Estatutaria 1266 de 2008. FUNCIÓN DE VIGILANCIA. La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.</i></p> <p><i>En los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con las facultades que le son propias, según lo establecido en el Estatuto Orgánico del Sistema Financiero y las demás normas pertinentes y las establecidas en la presente ley. ...”</i></p> <p>Este es un elemento que ha sido desarrollado en el Decreto 2399 de 2019 - Por el cual se modifica parcialmente la estructura de la Superintendencia Financiera de Colombia -, y que se presta para conflictos de competencias, ya que el</p>
--	--	---

		<p>Despacho del Superintendente Delegado para el Consumidor Financiero tiene dentro de sus funciones, entre otras: "... 2. <i>Dirigir la supervisión de las entidades vigiladas respecto del cumplimiento del Régimen de Protección al Consumidor Financiero y las obligaciones legales en materia de Habeas Data ...</i>".</p> <p>Sobre lo anterior, es de nuestro entendimiento que dicha facultad solamente se circunscribe a la Ley 1266 de 2008 en lo de su resorte, pero que se ha prestado desde dicha autoridad de una manera más extensa.</p> <p>Por lo anterior, resulta relevante que exista una coordinación entre autoridades gubernamentales que vigilan los temas de datos personales (ya que adicionalmente a nivel de tutela, los jueces de la República también tienen dicha competencia en virtud del Art. 15 de la C.P).</p>
<p><b>ARTÍCULO 54. Funciones de la Autoridad de Protección de Datos.</b></p> <p>La autoridad de protección de datos, ejercerá las siguientes funciones:</p> <ul style="list-style-type: none"> <li>a) Responder a las consultas previas realizadas por los responsables del tratamiento de conformidad con lo establecido en el artículo 38.</li> <li>b) Emitir, por iniciativa propia o previa solicitud, instrucciones, guías y demás instrumentos que considere necesarios sobre cualquier asunto relacionado con la protección de los datos personales.</li> <li>c) Emitir un dictamen y aprobar proyectos de códigos de conducta de</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>conformidad con lo dispuesto en el artículo 44 de la presente ley.</p> <p>d) Aprobar criterios de certificación.</p> <p>e) Aprobar las Cláusulas contractuales modelo contempladas en el artículo 49, numeral 2, literal c).</p> <p>f) Aprobar normas corporativas vinculantes de conformidad con el artículo 50.</p> <p>g) Autorizar las cláusulas contractuales de las que trata el artículo 49, numeral 3, literal a).</p> <p>h) Autorizar los acuerdos administrativos entre las entidades u organismos públicos de conformidad con el artículo 49, numeral 3, literal b).</p> <p>i) Impartir instrucciones a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.</p> <p>j) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte.</p> <p>k) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 45 de la presente ley.</p> <p>l) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley.</p> <p>m) Obtener de los responsables y encargados del tratamiento el acceso a toda la información necesaria para el ejercicio de sus funciones, así como el acceso a todas las instalaciones, incluidos equipos y medios de tratamiento de datos, respetando el debido proceso y la confidencialidad que ello requiere de acuerdo con la normativa vigente.</p> <p>n) Impartir instrucciones a los responsables y encargados del tratamiento cuando las operaciones de tratamiento infrinjan lo dispuesto en la presente ley.</p>		
--	--	--

- o) Imponer multas de carácter personal o institucional a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley.
- p) Imponer una limitación temporal o definitiva del tratamiento, como resultado de una sanción o de una orden administrativa a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido la presente ley.
- q) Impartir instrucciones a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de los artículos 18 al 27 de la presente ley.
- r) Impartir instrucciones al responsable del tratamiento para que comunique a los titulares, los incidentes de seguridad de los datos personales.
- s) Impartir instrucciones para garantizar el pleno y efectivo ejercicio de los derechos de rectificación, supresión o limitación del tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.
- t) Impartir instrucciones al organismo de certificación para que retire o que no emita una certificación con arreglo al artículo 45, si no se cumplen o dejan de cumplirse los requisitos para ello.

*Parágrafo Primero.* La Sala Administrativa del Consejo Superior de la Judicatura cumplirá funciones de promoción y difusión de la normativa en protección de datos personales en la Rama Judicial, y la Sala Disciplinaria será la encargada de investigar y sancionar la

<p>conducta de los funcionarios judiciales por el incumplimiento de la misma.</p> <p><i>Parágrafo Segundo.</i> El Departamento Administrativo de la Función Pública en articulación con la Autoridad de protección de datos realizará la promoción y difusión de la normativa en protección de datos personales que debe ser cumplida por cada una de las entidades públicas.</p>		
<p><b>ARTÍCULO 55. Tratamiento de los documentos de identificación.</b></p> <p>1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía, como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:</p> <ul style="list-style-type: none"> <li>a) Implementarán procedimientos de trazabilidad al interior de la organización, para evitar que se realicen copias no autorizadas de la cédula de ciudadanía entregada por los titulares. El titular podrá hacer uso de sellos, leyendas o firmas que determinen las condiciones de tiempo, modo, lugar y la finalidad con la que entrega la copia de su cédula de ciudadanía.</li> <li>b) Si no existe una base jurídica que legitime el tratamiento de los datos sensibles contenidos en la cédula de ciudadanía, deberá evitarse su captura o implementar técnicas de anonimización sobre los datos sensibles.</li> </ul>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>c) Exclusivamente el personal autorizado podrá tener acceso a los lugares y/o activos de información donde se archiven las copias de la cédula de ciudadanía.</p> <p>d) Aquellas copias de cédulas de ciudadanía que se hubiesen recabado exclusivamente para la realización de trabajos temporales deberán cumplir, entre otras, las medidas de seguridad de conformidad con el artículo 35 y ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su tratamiento.</p> <p>e) Mientras la cédula de ciudadanía no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser tratada por terceros no autorizados.</p> <p>2. Si para efectos de identificación, el titular no facilitó su cédula de ciudadanía para las operaciones de tratamiento llevadas a cabo por el responsable, en caso de ejercicio de los derechos contemplados en esta ley, utilizará el método de identificación previsto al momento de la recolección de los datos personales del titular, y sólo en caso excepcional y motivado, podrá requerirles para que el titular se identifique.</p> <p>3. Cuando sea necesaria la publicación de un acto administrativo que contenga datos personales del titular, incluyendo</p>		
---	--	--

<p>su cédula de ciudadanía, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de la cédula de ciudadanía, cédula de extranjería, pasaporte o documento equivalente o cualquier otro mecanismo de seudonimización.</p> <p><i>Parágrafo.</i> Lo contemplado en el presente artículo aplicará en igual medida para cédula de extranjería, pasaporte o documento de identificación equivalente presentado por el titular.</p>		
<p><b>ARTÍCULO 56. Tratamiento de neurodatos.</b></p> <p>El responsable, o en su caso el encargado que traten neurodatos, deberán garantizar la protección de los derechos y garantías fundamentales relacionadas con la protección de los datos personales y la intimidad de las personas, por lo que se establecen las siguientes obligaciones:</p> <ol style="list-style-type: none"> <li>1. Se prohíbe la obtención de neurodatos mediante técnicas de manipulación o coerción que comprometa la integridad cerebral o afecte negativamente la salud mental. Todo tratamiento efectuado a neurodatos respetará la dignidad y la integridad física y psíquica de las personas.</li> <li>2. El deber de información, además de cumplir los requisitos del artículo 14 , podrá contener los riesgos y beneficios para el titular.</li> <li>3. Queda prohibido cualquier tratamiento de neurodatos que pueda ocasionar la pérdida de identidad personal.</li> </ol>	Sin modificaciones	Sin modificaciones
<p><b>ARTÍCULO 57. Tecnologías de rastreo.</b></p> <ol style="list-style-type: none"> <li>1. Es necesario obtener el consentimiento del titular para utilizar tecnologías de rastreo. Las opciones de aceptar o</li> </ol>	Sin modificaciones	Sin modificaciones

<p>rechazar deben presentarse de manera destacada y equitativa, sin que rechazar sea más complicado que aceptar. No se considerará acción afirmativa utilizar los servicios sin manifestar la aceptación o el rechazo de las tecnologías de rastreo.</p> <p>2. Las tecnologías de rastreo técnicamente necesarias o esenciales, que son indispensables para el funcionamiento adecuado y para proporcionar los servicios solicitados por el titular, están exentas del requisito de obtener el consentimiento.</p> <p>3. Las tecnologías consideradas técnicamente necesarias cumplen con los siguientes criterios:</p> <ul style="list-style-type: none"> <li>a) Son temporales y se eliminan al finalizar la sesión. Se utilizan para mantener la sesión del titular, establecer parámetros libremente elegidos por éste y permitir el acceso a ciertas funcionalidades.</li> <li>b) Se utilizan para recordar los artículos agregados al carrito de compras, durante una sesión de compra en línea.</li> <li>c) Se utilizan para mantener la sesión activa y autenticar al titular mientras navega por la plataforma.</li> <li>d) Se utilizan para garantizar la seguridad de las interacciones detectando actividades potencialmente maliciosas o no autorizadas.</li> <li>e) No podrán ser usadas para otras finalidades ni para elaborar perfiles de los titulares. En caso de que no cumplan esta función, se deberá informar al usuario y darle la opción de rechazarlas.</li> </ul> <p>4. Las tecnologías de rastreo técnicamente necesarias no deben</p>		
--	--	--

<p>recopilar información personal más allá de lo estrictamente necesario para el funcionamiento del servicio y deben usarse exclusivamente con fines técnicos.</p>		
<p><b>ARTÍCULO 58. Derecho a indemnización y responsabilidad.</b></p> <ol style="list-style-type: none"> <li>1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidos en la presente ley, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.</li> <li>2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones del responsable.</li> <li>3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2, si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.</li> <li>4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado</li> </ol>	<p><b>ARTÍCULO 58. Derecho a indemnización y responsabilidad.</b></p> <ol style="list-style-type: none"> <li>1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidos en la presente ley, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.</li> <li>2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones del responsable.</li> <li>3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2, si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.</li> <li>4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado</li> </ol>	<p>La acción de responsabilidad por indebido tratamiento de datos personales que propone el proyecto es una acción que se debería dejar para el conocimiento de los jueces de la república, incluso para un conocimiento de la Delegatura para Asuntos Jurisdiccionales de la SIC. No es viable que en un proceso administrativo se imponga en concurrencia una sanción administrativa y una indemnización particular, cuando esta última debe proceder de un juicio de responsabilidad tramitado en sede jurisdiccional.</p> <p>Es altamente inconveniente, e incluso inconstitucional, dejar dentro de las facultades administrativas de la SIC la de establecer indemnizaciones por juicios de responsabilidad, esto es un tema jurisprudencial. Por ello, se propone la eliminación total de este artículo.</p>

<p>responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.</p> <p>5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2.</p> <p>6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.</p>	<p>responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.</p> <p>5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2.</p> <p>6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.</p>	
<p><b>ARTÍCULO 59. Sujetos Responsables.</b></p> <p>Están sujetos al régimen sancionador establecido en la presente ley:</p> <ol style="list-style-type: none"> <li>1. Los responsables del tratamiento, así como los corresponsables en la medida que su participación en la operación de tratamiento fuera determinante en la infracción.</li> <li>2. Los encargados del tratamiento.</li> <li>3. Las entidades de certificación.</li> <li>4. Las entidades acreditadas de supervisión de los códigos de conducta.</li> </ol> <p><i>Parágrafo:</i> No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este título.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

**ARTÍCULO 60. Condiciones generales para la imposición de sanciones.**

1. La autoridad de protección de datos, garantizará que la imposición de las sanciones con arreglo al presente título por las infracciones a los deberes y obligaciones contemplados en la presente ley, sean en cada caso individual efectivas, proporcionadas y correctivas. En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Administrativo y de lo Contencioso Administrativo.
2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 54. Al decidir la imposición de la sanción y su cuantía se graduarán atendiendo los siguientes criterios que resulten aplicables:
  - a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el alcance o propósito de la operación de tratamiento de que se trate, así como, el número de titulares afectados y el daño o peligro generado a los intereses jurídicos tutelados en la presente ley.
  - b) El alcance continuado de la infracción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
  - c) Si existió dolo o negligencia en la comisión de la infracción.
  - d) Los beneficios obtenidos por el infractor o terceros, en virtud de la comisión de la infracción.

La redacción de los siguientes literales: A, B, C, F, L, R. es incoherente.

Se debe considerar: (i) ¿cuáles serían atenuantes y cuáles agravantes?; (ii) las condiciones generales de imposición de sanción, así como las conductas típicas deberían estar en un punto intermedio entre el gran detalle (que genera dificultad probatoria y sancionatoria) y la generalidad (que no cumple el principio de tipicidad). Así mismo, es necesario considerar que la SIC solo podrá sancionar por aquello que en los artículos se establezca, y la redacción propuesta no es clara.

La sugerencia es dejar el sistema sancionatorio como está hoy en día. Es decir, atar las sanciones a los deberes establecidos para los Responsables y Encargados del Tratamiento. De ahí que, se sugiere incluir dos artículos encaminados a establecer claramente cada uno de los deberes en cabeza de los Responsables y Encargados del Tratamiento. **En virtud de ello, se sugiere que esto se discuta a profundidad con la autora o el coordinador ponente para concertar ideas.**

- e) El grado de responsabilidad del infractor, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud del artículo 35.
- f) La reincidencia en la comisión de la infracción.
- g) La resistencia, negativa u obstrucción a las labores de inspección o de vigilancia de la Autoridad de protección de datos.
- h) La afectación a los derechos de los niñas, niños y adolescentes.
- i) El incumplimiento de las instrucciones impartidas en virtud del artículo 54, cuando hayan sido ordenadas previamente contra el infractor en relación con el mismo asunto.
- j) La renuencia o desacato a cumplir las instrucciones impartidas por la autoridad de protección de datos.
- k) Si las infracciones fueron realizadas con el propósito de cometer alguna conducta tipificada como delito por la ley.
- l) Cualquier medida tomada por el infractor para contener y mitigar los daños y perjuicios sufridos por los titulares.
- m) El grado de cooperación con la autoridad de protección de datos, con el fin de contener y mitigar los posibles efectos adversos de la infracción.
- n) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción.
- o) La existencia de un proceso de fusión por absorción posterior

a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

- p) La forma en que la autoridad de protección de datos tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.
- q) La adhesión a códigos de conducta en virtud del artículo 42 o a mecanismos de certificación aprobados de conformidad con el artículo 45.
- r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos.
- s) El reconocimiento o aceptación expresas que haga el infractor sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.
- t) El sometimiento por parte del infractor, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier titular o interesado.
- u) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.

3. Si la autoridad de protección de datos detecta un posible incumplimiento de las disposiciones de la presente ley por parte de una entidad pública, remitirá la actuación a la Procuraduría General de la Nación para que la procuraduría delegada competente realice la investigación correspondiente.

4. El ejercicio por la autoridad de protección de datos de sus funciones en virtud del presente artículo estará

sujeto a las garantías del debido proceso.		
<p><b>ARTÍCULO 61. Infracciones.</b></p> <p>Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley.</p>	Sin modificaciones	Sin modificaciones
<p><b>ARTÍCULO 62. Sanciones.</b></p> <p>La autoridad de protección de datos podrá imponer a los infractores las siguientes sanciones:</p> <ol style="list-style-type: none"> <li>1. Multas de carácter personal e institucional hasta por el equivalente de cuatro mil (4.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción; o, hasta el cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal inmediatamente anterior al de la imposición de la sanción.</li> <li>2. Sanciones operativas y medidas correctivas.                         <ol style="list-style-type: none"> <li>a) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las medidas correctivas que se deberán adoptar.</li> <li>b) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de protección de datos.</li> <li>c) Cierre inmediato y definitivo de las operaciones relacionadas</li> </ol> </li> </ol>	Sin modificaciones	Sin modificaciones

con el tratamiento ilícito de Datos Sensibles.

- d) Las medidas correctivas serán establecidas por la autoridad de protección de datos, de acuerdo a las facultades otorgadas por el artículo 54, dependiendo de cada caso individual y serán independientes de la imposición de multas.

**ARTÍCULO 63. Condiciones del consentimiento.**

La autorización entregada por los titulares de datos recabados antes de la entrada en vigencia de esta ley seguirá siendo válida por un período de un año contados desde la entrada en vigencia. Durante este plazo, el responsable deberá legitimar el tratamiento de datos de conformidad con el artículo 6.

*Parágrafo.* La autorización para el tratamiento de datos personales otorgada con fines de investigación en salud y biomédica recogidos con anterioridad a la entrada en vigencia de esta ley no perderá su legitimidad cuando concurra alguna de las circunstancias siguientes:

- a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.
- b) Que, habiéndolo obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

**ARTÍCULO 63. Condiciones del consentimiento.**

La autorización entregada por los titulares de datos recabados antes de la entrada en vigencia de esta ley seguirá siendo válida por un período de **dos años** contados desde la entrada en vigencia. Durante este plazo, el responsable deberá legitimar el tratamiento de datos de conformidad con el artículo 6.

*Parágrafo.* La autorización para el tratamiento de datos personales otorgada con fines de investigación en salud y biomédica recogidos con anterioridad a la entrada en vigencia de esta ley no perderá su legitimidad cuando concurra alguna de las circunstancias siguientes:

- a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.
- b) Que, habiéndolo obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Aunque se insiste en no derogar la totalidad de la 1581 de 2012, armonizar esta Ley con la 1266 de 2008 y simplemente realizar los ajustes que en verdad ameriten una modificación, lo cierto es que, un año de implementación para cambios tan significativos es un tiempo incipiente para dar cumplimiento a la normatividad.

<p><b>ARTÍCULO 64. Plazos para la implantación de las medidas de seguridad.</b></p> <p>La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas:</p> <ol style="list-style-type: none"> <li>1. Respecto de los tratamientos que existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera:             <ol style="list-style-type: none"> <li>a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en los tratamientos automatizados.</li> <li>b) Respecto de los tratamientos no automatizados que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.</li> </ol> </li> <li>2. Los tratamientos, tanto automatizadas como no automatizadas, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.</li> </ol> <p><i>Parágrafo.</i> A requerimiento de la autoridad de protección de datos, el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en los tratamientos existentes en el momento de la entrada en vigencia de la presente ley.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
<p><b>ARTÍCULO 65. Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.</b></p> <p>Las solicitudes para el ejercicio de los derechos que hayan sido efectuadas con anterioridad a la</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p>entrada en vigencia de la presente ley, su contestación se registrará por la Ley 1581 de 2012.</p>		
<p><b>ARTÍCULO 66. Contratos de encargados del tratamiento.</b></p> <p>Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos. Los responsables y encargados tendrán hasta dieciocho meses para modificar aquellos contratos que no resulten conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p>Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p><i>Parágrafo.</i> Los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 32.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
<p><b>ARTÍCULO 67. Transferencias Internacionales.</b></p> <ol style="list-style-type: none"> <li>1. Dentro de los primeros dos años posteriores a la entrada en vigencia de la presente ley, la Autoridad de Protección de Datos deberá revisar lo establecido en la Circular Única de la Superintendencia de Industria y Comercio relativo a las transferencias de datos personales, a la luz de los criterios establecidos en el artículo 48.</li> <li>2. Una vez revisada la Circular Única de la Superintendencia de Industria y Comercio, los reconocimientos a países con nivel adecuado por parte de la autoridad de protección de datos a través su Circular tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley.</li> </ol>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p><b>ARTÍCULO 68. Régimen Sancionatorio.</b></p> <p>1. El Régimen Sancionatorio contemplado en el Título VII entrará en aplicación a los 2 años de entrada en vigencia de la presente ley. La autoridad de protección de datos impondrá a los responsables y Encargados del Tratamiento las sanciones descritas en la Ley 1581 de 2012, señalando de forma paralela el equivalente de la infracción y su respectiva sanción en el Régimen Sancionatorio aprobado por la presente ley.</p> <p>2. De conformidad con las facultades constitucionales que le han sido otorgadas a la Procuraduría General de la Nación, esta deberá asignar en el término de 18 meses con posterioridad a la entrada en vigencia de la presente ley, las funciones y competencias a una procuraduría delegada que será seleccionada o creada atendiendo a los criterios de especialidad por el incumplimiento a las disposiciones establecidas en la presente ley.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
<p><b>ARTÍCULO 69. Registro Nacional de Bases de Datos – RNBD.</b></p> <p>El Directorio Público de Bases de Datos, actualmente gestionado por la autoridad de protección de datos, experimentará una transformación tanto en su denominación como en su estructura, convirtiéndose en el "Registro de las Actividades del Tratamiento", en un plazo máximo de dos años a partir de la entrada en vigencia de la presente ley.</p> <p>El Gobierno Nacional reglamentará las categorías de sujetos obligados, así como los términos y condiciones bajo los cuales deben inscribirse en el Registro señalado.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>

<p><b>ARTÍCULO 70. Entidades Certificadoras</b></p> <p>Los organismos del subsistema de calidad tendrán un año desde la entrada en vigencia de la presente ley para regular la forma de acreditar las entidades descritas en el artículo 45.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>
<p><b>ARTÍCULO 71. Vigencia y Derogatorias</b></p> <p>La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria un año después, salvaguarda los derechos adquiridos y deroga todas las disposiciones que le sean contrarias. También deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones de la presente ley.</p>	<p>Sin modificaciones</p>	<p>Sin modificaciones</p>