Bogotá D.C.,

10

Respetado(a) Señor (a):

[Datos personales eliminados en virtud de la Ley 1581 de 2012]

Asunto: Radicación: 17-364624- -1
Trámite: 113
Evento: 0
Actuación: 440
Folios: 1

Estimado(a) Señor :

De conformidad con lo previsto en el artículo 28 de la Ley 1755 de 2015, "*por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo",* fundamento jurídico sobre el cual se funda la consulta objeto de la solicitud, procede la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** a emitir un pronunciamiento, en los términos que a continuación se pasan a exponer:

1. CUESTIÓN PREVIA

Reviste de gran importancia precisar en primer lugar que la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** a través de su Oficina Asesora Jurídica no le asiste la facultad de dirimir situaciones de carácter particular, debido a que, una lectura en tal sentido, implicaría la flagrante vulneración del debido proceso como garantía constitucional.

Al respecto, la Corte Constitucional ha establecido en la Sentencia C-542 de 2005:

> *"Los conceptos emitidos por las entidades en respuesta a un derecho de petición de consulta no constituyen interpretaciones autorizadas de la ley o de un acto administrativo. No pueden reemplazar un acto administrativo. Dada la naturaleza*

misma de los conceptos, ellos se equiparan a opiniones, a consejos, a pautas de acción, a puntos de vista, a recomendaciones que emite la administración pero que dejan al administrado en libertad para seguirlos o no".

Ahora bien, una vez realizadas las anteriores precisiones, se suministrarán las herramientas de información y elementos conceptuales necesarios que le permitan absolver las inquietudes por usted manifestadas, como sigue:

2. FACULTADES DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La Ley 1581 de 2012, en su artículo 21 señala las siguientes funciones para esta Superintendencia:

"a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementara campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley.

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

k) Las demás que le sean asignadas por ley.

A continuación, resolveremos los interrogantes de su consulta radicado con fecha 28 de marzo de 2017 en los siguientes términos:

Primer interrogante

Los políticos o personas que son elegidas popularmente a corporaciones públicas y tienen páginas web personales (por ejemplo, concejales, senadores, diputados, etc.) y cuentan con la opción de que se registren datos de simpatizantes, militantes u otros, ¿qué normas deben cumplir para la captura u obtención de esta información?

Respuesta: El artículo 5 de la Ley 1581 de 2012 señala lo siguiente:

> *"Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos".*

La Corte Constitucional mediante sentencia C-748 de 2011 señaló lo siguiente:

> "*La Sala encuentra que esta definición se ajusta a la jurisprudencia Constitucional y su delimitación, además de proteger el habeas data, es una garantía del derecho a la intimidad, razón por la cual la Sala la encuentra compatible con la Carta Política.*
>
> *En efecto, como explicó la Corte en la sentencia C-1011 de 2008, la información sensible es aquella "(…) relacionada, entre otros aspectos,*

con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella 'esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico.
"

Conforme a esta explicación, la definición del artículo 5 es compatible con el texto constitucional, siempre y cuando no se entienda como una lista taxativa, sino meramente enunciativa de datos sensibles, pues los datos que pertenecen a la esfera intima son determinados por los cambios y el desarrollo histórico."

Respecto al derecho a la intimidad, la Corte Constitucional en sentencia C- 640 de 2010 ha manifestado lo siguiente:

"[D]esde 1992, la Corte Constitucional reconoció el derecho a la intimidad como un derecho fundamental que permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores. Se dijo en ese entonces que se trataba de un derecho "general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada.

(...)

Se afirmó también que la intimidad es "el espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto." En 1995, se reiteró esta visión del derecho a la intimidad, cuando se afirmó que ".este derecho, que se deduce de la dignidad humana y de la natural tendencia de toda persona a la libertad, a la autonomía y a la autoconservación, protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo. Uno y otra están en posición de reclamar una mínima consideración particular y pública a su interioridad, actitud que se traduce en abstención de conocimiento e injerencia en la esfera reservada que les corresponde y que está compuesta por asuntos, problemas, situaciones y circunstancias de su exclusivo interés. Esta no hace parte del dominio público y, por tanto, no debe ser materia de

información suministrada a terceros, ni de la intervención o análisis de grupos humanos ajenos, ni de divulgaciones o publicaciones (…)

(...)

El derecho a la intimidad, junto con otros derechos como el del libre desarrollo de la personalidad y la libertad de conciencia, están concebidos para permitir a las personas fortalecer y desarrollar su condición de seres libres y autónomos, que es el presupuesto esencial del estado democrático.

(...)

De conformidad con la definición los datos sensibles, son aquellos que afectan la intimidad de las personas el uso indebido de los mismos puede generar su discriminación, pues esta relacionada, entre otros aspectos, con la salud, la orientación sexual, los hábitos del individuo y el credo religioso y político.

Los datos sensibles tienen un tratamiento especial consagrado en el artículo 6 de la Ley 1581 de 2012 así:

"Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento,salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El Tratamiento sea necesario para salvaguardar el interés vital delTitular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El Tratamiento sea efectuado en el curso de las actividades legítimas ycon las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

d) El Tratamiento se refiera a datos que sean necesarios para elreconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

> *e) El Tratamiento tenga una finalidad histórica, estadística o científica. Eneste evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares."*

Al respecto, la Corte Constitucional mediante la Sentencia C-748 de 2011 señaló lo siguiente:

> *"[C]omo se indicó en apartes previos, la prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios –como la atención médica y la educación- o para la realización de derechos ligados precisamente a la esfera íntima de las personas –como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios(…)"*

Por lo anterior, la Ley 1581 de 2012 señala los eventos en los que se puede realizar tratamiento de los datos sensibles, esto es, la recolección, el almacenamiento, el uso, la circulación o supresión de los mismos, entre ellos, cuando el titular haya dado **su autorización explícita o cuando el mismo sea efectuado en el curso de actividades legítimas cuya finalidad sea política, filosófica, religiosa o sindical.**

En consecuencia y con el fin de dar trámite a su primer interrogante, tenga en cuenta que **los datos personales sobre el origen político o la afinidad política ostentan la calidad de dato sensible**. Así las cosas y a efectos de realizar tratamiento de los referidos datos -como la captura u obtención de los mismos - se deberá observar para el efecto lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios frente al tratamiento de datos sensibles.

Segundo interrogante:

2. Si las personas acceden voluntariamente a este tipo de páginas web, plataformas o aplicaciones, y deciden registrase en formularios de contacto automáticamente están consintiendo con el hecho de suministrar sus datos personales?

Respuesta: Respecto a la autorización para el tratamiento de los datos personales entendido este como la recolección, almacenamiento, uso, circulación o supresión de los mismos debe tenerse en cuenta el principio de libertad definido en el literal c) del artículo 4 de la mencionada ley así:

> *"c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento*"

Al respecto, la Corte Constitucional mediante Sentencia C-748 de 2011 señaló lo siguiente:

> *"[P]rincipio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.*
>
> *Este principio, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.*
>
> *El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su "imagen informática".*
>
> *(...)*
>
> *En materia de manejo de información personal, el consentimiento exigido es además, calificado, por cuanto debe ser* ***previo, expreso e informado.*** *Sobre el particular, en la Sentencia C-1011 de 2008 se sostuvo que tales características concretan la libertad del individuo frente al poder informático*
>
> *(…)*
>
> *En relación con* ***el carácter previo****, la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. (…)*
>
> *En relación con el* ***carácter expreso****, la autorización debe ser inequívoca, razón por la cual, al contrario de lo sostenido por algunos intervinientes, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito. (…)*

> *En relación con el **carácter informado**, el titular no sólo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. (…)"*

Por lo anterior, el tratamiento de los datos personales sólo puede realizarse cuando exista la autorización previa, expresa e informada del titular, con el fin de permitir al titular que se garantice que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación.

Respecto a la autorización el artículo 2.2.2.25.2.2., del Decreto 1074 de 2015 señala lo siguiente:

> *"Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento."*

Para el tratamiento de los datos sensibles el artículo 2.2.2.25.2.3. del precitado Decreto señala lo siguiente:

> *"De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5 de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la citada ley.*
>
> *En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:*
>
> *1. Informar al Titular que por tratarse de datos sensibles no está obligado aautorizar su Tratamiento.*
>
> *2. Informar al Titular de forma explícita y previa, además de los requisitosgenerales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.*
>
> *Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles."*

En concordancia con lo anterior, el artículo 2.2.2.25.2.4., del precitado decreto dispone:

> *"Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 2.2.2.25.4.1., del presente Decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada.*
>
> *Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca."*

En consecuencia, los responsables del tratamiento de los datos personales deben obtener la autorización por parte del titular a más tardar al momento de su recolección informándole la finalidad específica del tratamiento de los mismos, y debe utilizar mecanismos que garanticen su consulta posterior.

Se entiende que el titular de la información ha dado su autorización para el tratamiento de los datos personales cuando: (i) sea por escrito; (ii) sea oral o (iii) mediante conductas inequívocas, es decir, aquellas que no admiten duda o equivocación, del titular que permitan concluir de forma razonable que otorgó la autorización. El silencio no puede asimilarse a una conducta inequívoca.

No obstante lo anterior y en aras de dar solución a su interrogante, para el caso donde se lleve a cabo algún tratamiento de datos sensibles, **la autorización debe ser explícita, es decir, admite únicamente el otorgamiento del consentimiento de forma escrita u oral y en consecuencia, no es factible la obtención de la referida autorización mediante conductas inequívocas.**

Así las cosas y en relación al tratamiento de datos sensibles, el diligenciamiento por parte del titular de un formulario donde se le solicite información personal, no es prueba legal suficiente que permita inferir que el titular otorgó su consentimiento para su tratamiento y en todo caso deberá obtener, ya sea de forma escrita u oral, la autorización explícita frente al mismo.

Tercer interrogante

3. Qué datos se pueden solicitar y/o suministrar?

Respuesta: El literal b) del artículo 4 de la mencionada Ley 1581 de 2012 define el principio de finalidad así: "***b) Principio de finalidad:*** *el tratamiento debe obedecer a una*

finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular".

Al respecto, la Corte Constitucional mediante Sentencia C-748 de 2011 señaló lo siguiente:

> ***"Principio de finalidad:*** *En virtud de tal principio, el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.*
>
> *La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.*
>
> *Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad* ***no sólo debe ser legítima,*** *sino que la referida información se destinará a realizar los* ***fines exclusivos*** *para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa,* ***deberá ser autorizada en forma expresa por el Titular.***
>
> *Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está haciendo usado para la finalidad por él autorizada. Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato.*
>
> *Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.*
>
> *Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también:* ***(i) un ámbito temporal****, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y* ***(ii) un ámbito material****, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.*
>
> *En razón de lo anterior****,*** *el literal b) debe ser entendido en dos aspectos.*

Primero, *bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado.*

En la Sentencia ***C-1011 de 2008****, la Corporación reiteró la importancia de la existencia de unos criterios razonables sobre la permanencia de datos personales en fuentes de información. Además, sostuvo que este periodo se encuentra en una estrecha relación con la finalidad que pretende cumplir. Así, a partir del estudio de la jurisprudencia, construyó una doctrina constitucional comprehensiva sobre la caducidad del dato negativo en materia financiera y concluyó que dentro de las prerrogativas mismas del derecho al habeas data, se encuentra esta garantía, como una consecuencia del derecho al olvido. Sobre el particular observó la providencia:*

"De acuerdo con lo señalado en el artículo 15 Superior, la Corte identifica como facultades que conforman el contenido del derecho al hábeas data, las de (i) conocer la información personal contenida en las bases de datos, (ii) solicitar la actualización de dicha información a través de la inclusión de nuevos datos y (iii) requerir la rectificación de la información no ajustada a la realidad. Junto con las prerrogativas expuestas, la Corte, habida cuenta los precedentes jurisprudenciales anteriores que señalaban la necesidad de establecer un límite al reporte financiero negativo, estableció un nuevo componente del derecho al hábeas data, la de la caducidad del dato negativo."

(…)

La Corte reitera que los procesos de administración de datos personales de contenido crediticio cumplen un propósito específico: ofrecer a las entidades que ejercen actividades de intermediación financiera y, en general, a los sujetos que concurren al mercado, información relacionada con el grado de cumplimiento de las obligaciones suscritas por el sujeto concernido, en tanto herramienta importante para adoptar decisiones sobre la suscripción de contratos comerciales y de crédito con clientes potenciales. Esta actividad es compatible con los postulados superiores, pues cumple con propósitos legítimos desde la perspectiva constitucional, como son la estabilidad financiera, la confianza en el sistema de crédito y la protección del ahorro público administrado por los establecimientos bancarios y de crédito.

Es precisamente la comprobación acerca de la finalidad específica que tienen los operadores de información financiera y crediticia la que, a su vez, permite

determinar los límites al ejercicio de las actividades de acopio, tratamiento y divulgación de datos."

***Segundo**, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: **(i)**adecuados, **(ii)** pertinentes y **(iii)** acordes con las finalidades para las cuales fueron previstos."*

Por lo anterior, el tratamiento de los datos personales de un titular sólo puede hacerse para los casos autorizados de manera previa y expresa por éste cumpliendo con una finalidad legítima y destinada a realizar los fines exclusivos para los cuales fue entregada por el titular a cada uno de los responsables del tratamiento.

En consecuencia, cada responsable que pretenda realizar el tratamiento de datos personales de un titular debe contar con su autorización previa y expresa, de acuerdo a la finalidad específica que se requiera.

Frente al principio de finalidad, es necesario hacer referencia al principio de necesidad, el cual no se encuentra dentro de los enunciados en el artículo 4 de la Ley 1581 de 2011, sin embargo, la Corte Constitucional en la sentencia de examen de constitucionalidad C-748 de 2012 hace referencia a la aplicación del mismo en los siguientes términos:

"En relación con el principio de necesidad, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. Sobre el particular, la Sentencia T-307 de 1999, afirmó: "la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer"(subraya fuera del texto)

En conclusión y con el fin de dar solución a su inquietud, le indicamos que los datos que se podrán solicitar al titular serán aquellos que **guarden estrecha relación con la finalidad legítima del tratamiento que se pretende efectuar y cumpla con los objetivos específicos y explícitos perseguidos por el responsable de la información**, siempre y cuando, se reitera, la finalidad sea comunicada previa y expresamente al titular de la información.

Cuarto Interrogante

¿Qué debe hacer el propietario o el administrador de esa página para garantizar estándares legales de cumplimiento?

Respuesta: El artículo 4 de la Ley 1581 de 2012 establece como uno de los principios del tratamiento de datos personales el de seguridad, en los siguientes términos:

> "***Principios para el Tratamiento de datos personales.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios: (…)*
>
> *g)* ***Principio de seguridad:*** *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"*

En relación con dicho principio la Corte Constitucional mediante Sentencia C-748 de 2011 consideró:

> *"2.3.1.1.1. Principio de seguridad: Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
>
> *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.*

> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos".*
>
> *Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria."*

Con el fin de materializar el principio en mención, el artículo 17 de la Ley 1581 de 2012 ha establecido, entre otros, los siguientes deberes a cargo de los responsables del tratamiento de datos personales:

> ***"Deberes de los Responsables del Tratamiento.*** *Los Responsables 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: (…)*
>
> *d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *(…)*
>
> *i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;*
>
> *(…)*
>
> *n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares."*

Así mismo, respecto de los encargados del tratamiento de datos personales el artículo 18 de la mencionada ley ha señalado los siguientes deberes en relación con la seguridad:

> *"**Deberes de los Encargados del Tratamiento.** 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:*
>
> *(…)*
>
> *b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *(…)*
>
> *k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;*
>
> (…)"

De acuerdo con lo anterior, es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas **con el fin de garantizar la seguridad de las bases de datos, y en especial que: (i) no sea adulterada la información contenida en las bases de datos, (ii) no se pierda la información de las bases de datos, (iii) no se pueda hacer uso, consultar o acceder sin autorización o de manera fraudulenta a las bases de datos.**

Finalmente, es necesario aclarar que la normativa no determina de manera específica qué medidas se deben adoptar para garantizar el principio de seguridad en el tratamiento de las bases de datos, y hasta tanto no se instruya sobre la materia, corresponde a los responsables y encargados del tratamiento implementar las medidas técnicas, humanas y administrativas que resulten idóneas para la obtención de tal fin.

Quinto interrogante

¿La información recabada es considerada una base de datos y debe ser registrada?

Respuesta: El artículo 25 de la Ley 1581 de 2012 señala lo siguiente:

> *"Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.*
>
> *El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.*

> *Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.*
>
> ***Parágrafo.*** *El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente Ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en éste los Responsables del Tratamiento."*

Dicho artículo fue reglamentado mediante el artículo 2.2.2.26.1.2., del Decreto 1074 de 2015, que incorpora el Decreto 886 de 2014 y en el que se determina qué bases de datos deben ser inscritas en el Registro Nacional de Bases de datos:

> "*Ámbito de aplicación. Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2 de la Ley 1581 de 2012*."

De acuerdo con lo cual, todas las bases que sean reguladas por la Ley 1581 de 2012 deben ser inscritas en el Registro Nacional de Bases de Datos, sin importar si el Responsable del Tratamiento es una entidad de naturaleza pública o privada y personas naturales o jurídicas.

Por su parte, el artículo 2.2.2.26.1.3., del Decreto 1074 de 2015 dispone lo siguiente:

> ***"2.2.2.26.1.3. Deber de inscribir las bases de datos****. El Responsable del Tratamiento debe inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento".*

En consecuencia, la obligación de realizar la inscripción de las bases de datos en el Registro Nacional le corresponde al responsable del tratamiento entendido como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos *ylo* el Tratamiento de los datos, esto es, la recolección, el uso, el almacenamiento, la circulación y la supresión de los mismos.

Por otra parte, respecto de la información mínima que debe contener el Registro Nacional de Bases de Datos el artículo 2.2.2.26.2.1., del Decreto 1074 de 2015 establece:

> "*Información mínima del Registro Nacional de Bases de Datos. La información*
>
> *mínima que debe contener el Registro Nacional de Bases de Datos es la siguiente:*
>
> 1. *Datos de identificación, ubicación y contacto del Responsable del Tratamientode la base de datos;*
> 2. *Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos;*
> 3. *Canales para que los titulares ejerzan sus derechos;*
> 4. *Nombre y finalidad de la base de datos;*
> 5. *Forma de Tratamiento de la base de datos (manual y/o automatizada), y*
> 6. *Política de Tratamiento de la información.*
>
> *La Superintendencia de Industria y Comercio, como autoridad de protección de datos personales, podrá establecer dentro del Registro Nacional de Bases de Datos información adicional a la mínima prevista en este artículo, acorde con las facultades que le atribuyó la Ley 1581 de 2012 en el literal h) del artículo 21."*

En concordancia con lo anterior, en el Capítulo Segundo del Título V de la Circular Única de esta Superintendencia, que incorpora la Circular Externa 01 de 2016, se imparten instrucciones sobre el Registro Nacional de Bases de Datos para personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio, entre ellas, la información adicional a la señalada en el artículo 2.2.2.26.2.1. del Decreto 1074 de 2015, que debe inscribirse en los siguientes términos:

> *"a) Información almacenada en la base de datos. Es la clasificación de los datos personales almacenados en cada base de datos, agrupados por categorías y subcategorías, de acuerdo con la naturaleza de los mismos.*
>
> *b) Medidas de seguridad de la información. Corresponde a los controlesimplementados por el Responsable del Tratamiento para garantizar la seguridad de las bases de datos que está registrando, teniendo en cuenta las preguntas dispuestas para el efecto en el RNBD. Tales preguntas no constituyen de ninguna manera instrucciones acerca de las medidas de seguridad que deben implementar los Responsables del Tratamiento de datos personales.*
>
> *c) Procedencia de los datos personales. La procedencia de los datos se refiere a siestos son recolectados del Titular de la información o suministrados por terceros*

y si se cuenta con la autorización para el tratamiento o existe una causal de exoneración, de acuerdo con lo establecido en el artículo 10 de la Ley 1581 de 2012.

d) Transferencia internacional de datos personales. La información relacionada conla Transferencia internacional de datos personales comprende la identificación del destinatario como Responsable del Tratamiento, el país en el que este se encuentra ubicado y si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio o por una causal de excepción en los términos señalados en el artículo 26 de la Ley 1581 de 2012.

e) Transmisión internacional de datos personales. La información relacionada conla Transmisión internacional de datos comprende la identificación del destinatario como Encargado del Tratamiento, el país en el que este se encuentra ubicado, si se tiene un contrato de transmisión de datos en los términos señalados en el artículo 2.2.2.25.5.2 de la Sección 5 del Capítulo 25 del Decreto Único 1074 de 2015 o si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio.

f)Cesión o transferencia nacional de la base de datos. La información relacionada con la cesión o transferencia nacional de datos incluye la identificación del cesionario, quien se considerará Responsable del Tratamiento de la base de datos cedida a partir del momento en que se perfeccione la cesión. No es obligatorio para el cedente registrar la cesión de la base de datos. Sin embargo, el cesionario, como Responsable del Tratamiento, debe cumplir con el registro de la base de datos que le ha sido cedida.

g) Reporte de novedades. Una vez finalizada la inscripción de la base de datos en el RNBD, se reportarán como novedades los reclamos presentados por los Titulares y los incidentes de seguridad que afecten la base de datos, de acuerdo con las siguientes reglas:

(i)Reclamos presentados por los Titulares. Corresponde a la información de los reclamos presentados por los Titulares ante el Responsable y/o el Encargado del Tratamiento, según sea el caso, dentro de un semestre calendario (enero – junio y julio – diciembre). Esta información se reportará teniendo en cuenta lo manifestado por los Titulares y los tipos de reclamos prestablecidos en el registro. El reporte deberá ser el resultado de consolidar los reclamos presentados por los Titulares ante el Responsable y el (los) Encargado (s) del Tratamiento.

(ii) Incidentes de seguridad. Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, que deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en

que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos".

Así mismo, señala el procedimiento para realizar el Registro Nacional de Bases de Datos, el cual deberá hacerse de acuerdo a las instrucciones contenidas en el "Manual del Usuario del Registro Nacional de Bases de Datos - RNBD" publicado en el sitio Web de la Superintendencia de Industria y Comercio, www.sic.gov.co.

La inscripción se realizará en línea en el portal Web de esta entidad www.sic.gov.co ingresa por el micrositio de "Protección de datos personales" ubicado en la barra horizontal superior, luego "Sobre la Protección de Datos Personales" y, finalmente, "Registro Bases de Datos", en el menú vertical que se encuentra al lado izquierdo.

Ahora bien, el artículo 2.2.2.26.3.1. del Decreto 1074 de 2015, modificado por el Decreto 1115 de 2017, establece lo siguiente:

"*La inscripción de las bases de datos en el Registro Nacional de Bases de Datos se llevará a cabo en los siguientes plazos:*

a) Los Responsables del Tratamiento, personas jurídicas de naturaleza privada ysociedades de economía mixta inscritas en las cámaras de comercio del país, deberán realizar la referida inscripción a más tardar el treinta y uno (31) de enero de 2018, de acuerdo con las instrucciones que para el efecto imparta la Superintendencia de Industria y Comercio.

b) Los Responsables del Tratamiento, personas naturales, entidades de naturalezapública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio, deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos a más tardar el treinta y uno (31) de enero de 2019, conforme con las instrucciones impartidas para tales efectos por la Superintendencia de Industria y Comercio.

Las bases de datos que se creen con posterioridad al vencimiento de los plazos referidos en los literales a) y b) del presente artículo, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación. ".

De acuerdo con lo cual, existen tres plazos para la inscripción de bases de datos personales así: (i) hasta el treinta y uno (31) de enero de 2018 para las personas jurídicas de naturaleza privada y sociedades de economía mixta inscritas en las cámaras de comercio; (ii) hasta el treinta y uno (31) de enero de 2019 para las personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de

comercio, y (iii) para las bases de datos que se creen con posterioridad al vencimiento de los plazos referidos enteriormente, dentro de los dos (2) meses siguientes contados a partir de su creación.

No obstante lo anterior, tenga en cuenta que **el régimen general de protección de datos personales es aplicable a todas las personas naturales o jurídicas que realicen el tratamiento de datos personales, es decir, que recolecten, almacenen, usen o circulen datos de personas naturales**. La ley no establece ninguna excepción que excluya su aplicación por el tamaño de la empresa, el tipo de persona jurídica o sociedad, el número de empleados que tenga o la cantidad o tipo de datos personales que administre.

Así mismo y con el fin de dar solución a su inquietud, **todas las personas naturales o**

jurídicas que tengan la calidad de responsable del tratamiento de datos personales deben registrar las bases de datos en el Registro Nacional de bases de Datos, conforme al procedimiento señalado por esta Superintendencia en las Circulares Externas 002 de 2015, 001 de 2016 y 001 de 2017.

Sexto Interrogante:

Qué tratamiento se debe dar a esa información?

Respuesta: Nos remitimos a la respuesta brindada en relación al tercer interrogante de su solicitud frente al principio de finalidad, reiterando en todo caso que el tratamiento que se le debe dar a la información personal deberá corresponder a la finalidad previa, expresa e informada que establezca el responsable de la misma.

Al respecto tenga en cuenta que el artículo 12 de la Ley 1581 de 2012 establece frente al deber de información lo siguiente:

> ***Artículo 12. Deber de informar al Titular.*** *El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:*
> *a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad delmismo;*
> *b) El carácter facultativo de la respuesta a las preguntas que le sean hechas,cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;*
> *c) Los derechos que le asisten como Titular;*

d) La identificación, dirección física o electrónica y teléfono del Responsable delTratamiento.

Parágrafo. *El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.*

Séptimo interrogante:

A esas personas que libre y voluntariamente acceden a llenar formularios en línea, registrase como voluntarios, etc. Se les puede enviar información a sus correos electrónicos o direcciones físicas?

Respuesta: Nos remitimos al desarrollo dispuesto en torno a su segunda y tercera inquietud, reiterando en todo caso que el responsable debe suministrarle previamente al titular la finalidad del tratamiento. Una vez suministrada la misma, el titular deberá autorizar el tratamiento previa y expresamente.

En consecuencia, si desea efectuar tratamiento de información entendido este como la recolección, el almacenamiento, el uso, la circulación o supresión de los mismos, deberá contar con la autorización expresa, previa e informada del titular.

Sin embargo y en relación al tema de su inquietud, tenga en cuenta que frente al tratamiento de datos sensibles, la autorización mediante conductas inequívocas no es permitida y en tal sentido, el solo diligenciamiento de un formulario, no es prueba legal frente al otorgamiento del consentimiento, caso en cual, deberá contar con autorización **expresa** por parte del titular, la cual, se reitera podrá ser extendida de forma verbal o escrita.

Octavo interrogante:

Si a este tipo de páginas web se puede ingresar con el registro de otra, por ejemplo el perfil Facebook, Twitter, esa información queda a disposición de la página del tercero, que precauciones se deben tomar?

Respuesta: Nos remitimos a la respuesta brindada frente a su cuarta pregunta, reiterando en todo caso que es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas con el fin de garantizar la seguridad de las bases de datos, y en especial que: (i) no sea adulterada la información contenida en las bases de datos, (ii) no se pierda la información de las bases de datos, (iii) no se pueda hacer uso, consultar o acceder sin autorización o de manera fraudulenta a las bases de datos.

Cabe así mismo reiterar que ni la Ley 1581 de 2012 ni sus decretos reglamentarios determinan de manera específica qué medidas se deben adoptar para garantizar el principio de seguridad en el tratamiento de las bases de datos, y hasta tanto no se instruya sobre la materia, corresponde a los responsables y encargados del tratamiento implementar las medidas técnicas, humanas y administrativas que resulten idóneas para la obtención de tal fin.

Igualmente, la responsabilidad demostrada le corresponde al responsable del tratamiento, para demostrar, a petición de la Superintendencia de Industria y Comercio, que se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios. Para ello, pueden implementar un Programa Integral de Gestión de Datos Personales que permitan asegurar las políticas adoptadas por el responsable del tratamiento y su implementación al interior de cada organización, en el que se incluya un sistema de administración de riesgos asociados al tratamiento de datos personales.

Así mismo, dentro de la información adicional que los responsables del tratamiento deben incluir en el Registro Nacional de bases de datos se encuentran las medidas de seguridad de la información, entendidas como, los controles implementados por el Responsable del Tratamiento para garantizar la seguridad de las bases de datos que está registrando, teniendo en cuenta las preguntas dispuestas para el efecto en el RNBD. Así mismo, deberán reportar como novedad los incidentes de seguridad dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

Ahora bien y frente a su inquietud, cabe resaltar que **los datos suministrados por redes sociales a efectos de completar campos dentro de un formulario de datos son obtenidos como un mero mecanismo de autenticación autorizado por el titular**, quien inicia sesión en las referidas redes y acepta que la información sea exportada para culminar con los registros en otra plataforma digital.

En consecuencia y **una vez la información haya sido incluida en los mencionados formularios a través de inicio de sesión en redes sociales y con la aceptación del titular, el propietario de la referida plataforma adquiere la calidad de responsable de la información** y deberá observar para todos los efectos el Régimen de Protección de Datos Personales establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

Noveno interrogante

"*Cualquier otra información que estimen pertinente y relevante para páginas web de políticos, candidatos y otros similares.*"

Respuesta: El literal h) del artículo 4 de la Ley 1581 de 2012, prevé el principio de confidencialidad, así:

> *"h) Principio de confidencialidad: todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."*

En relación con dicho principio la Corte Constitucional consideró:

> *"Esta norma no ofrece ningún reparo, y por el contrario, busca que los operadores de los datos sigan guardando el secreto de ciertos datos, aún cuando haya finalizado la relación con la fuente de información"*
>
> *"En aras del principio de acceso y circulación restringida, seguridad y confidencialidad, el Titular tiene derecho a exigir que su información sea tratada de conformidad con los límites impuestos por la Ley y la Constitución y que en caso de incumplimiento existe un recurso efectivo para lograr el restablecimiento de sus derechos."*

La Doctrina por su parte se ha encargado de desarrollar este principio y en tal sentido ha manifestado que "*Este principio da un mensaje muy claro a las personas involucradas en el tratamiento de datos personales: salvo los datos públicos, deben mantener reserva o en secreto los datos personales que conocen con ocasión de su trabajo o gestión. No pueden hacer de conocimiento público los datos privados, a menos que lo autorice el titular, la ley o exista orden judicial legítima*"[1]

En consecuencia, las personas que intervengan en el Tratamiento de datos personales, esto es, en la recolección, el uso, el almacenamiento, la circulación o la supresión de los mismos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento y sólo pueden realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley 1581 de 2012 y sus decretos reglamentarios.

Finalmente le informamos que algunos conceptos de interés general emitidos por la

---

[1] REMOLINA, Nelson: "*Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012".* Editorial LEGIS. Bogotá. 2013. p 221.

Oficina Jurídica, así como las resoluciones y circulares proferidas por ésta Superintendencia, las puede consultar en nuestra página web **http://www.sic.gov.co/Doctrina**

En ese orden de ideas, esperamos haber atendido satisfactoriamente su consulta, reiterándole que la misma se expone bajo los parámetros del artículo 28 de la Ley 1437 de 2011, esto es, bajo el entendido que la misma no compromete la responsabilidad de esta Superintendencia ni resulta de obligatorio cumplimiento ni ejecución.

Atentamente,

JAZMÍN ROCÍO SOACHA PEDRAZA
JEFE OFICINA ASESORA JURÍDICA

Elaboró: Gabriel Turbay
Revisó: Rocío Soacha
Aprobó: Rocío Soacha