

# Protección de Datos Personales Colombia

**Luz Helena Adarve**

Socia

T +57 3137800 ext. 232

[luz.adarve@dentons.com](mailto:luz.adarve@dentons.com)

**Juanita Acosta**

Socia

T +57 3137800 ext. 266

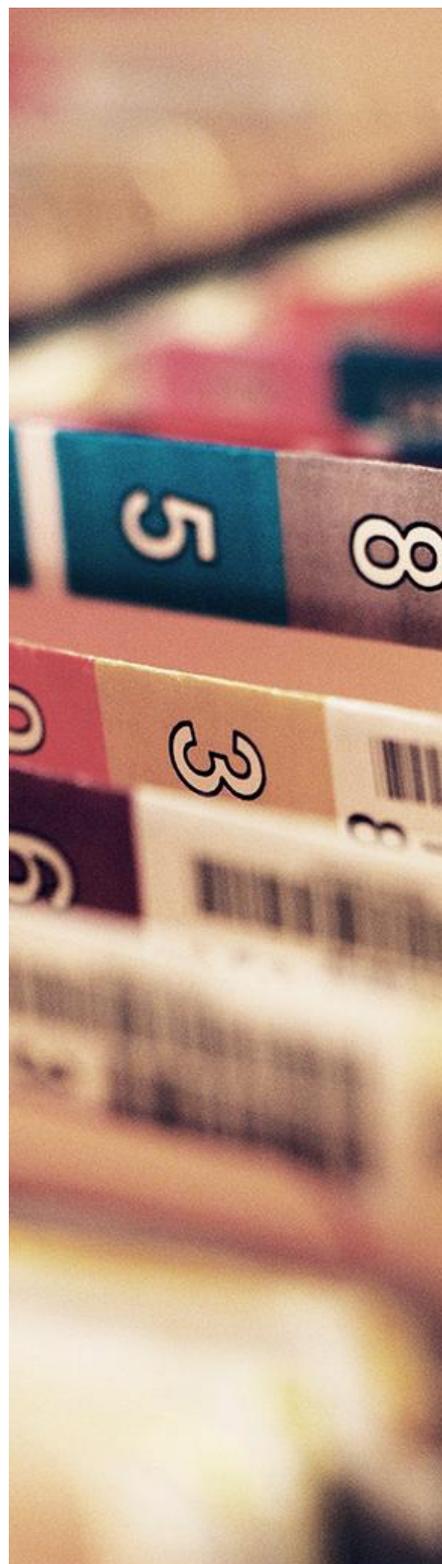
[juanita.acosta@dentons.com](mailto:juanita.acosta@dentons.com)

# Introducción

Siguiendo la experiencia adquirida por múltiples países en materia privacidad y protección de datos personales, en el año 2012 Colombia estableció un régimen general para la protección de la información personal que debe ser observado por todas las personas naturales o jurídicas que realicen el tratamiento de datos personales en Colombia. La normatividad general de protección de datos, instituida a través de la Ley 1581 de 2012, presenta un alcance verdaderamente amplio considerando que aplica a todo tratamiento de datos personales realizado en Colombia, que no se encuentre dentro de las precisas excepciones establecidas en la ley. Adicionalmente, la legislación colombiana no se limita al tratamiento de datos personales realizado en el sector privado, sino que es aplicable igualmente al tratamiento ejecutado por todas las entidades pertenecientes y adscritas al sector público.

Es importante destacar que el tratamiento de datos personales incluye cualquier operación que se realice sobre información que pueda ser vinculada a una persona natural, incluyendo la recolección, el almacenamiento, el uso, la supresión, la actualización, la transmisión y la transferencia de datos personales. Por lo tanto, la realización de cualquiera de las actividades indicadas anteriormente sobre información personal, que no se encuentre fundamentada en una excepción establecida por la ley, implica la aplicación del régimen general para la protección de datos personales.

A continuación, presentamos un panorama general sobre las obligaciones derivadas de la legislación colombiana de protección de datos personales, así como de un proyecto regulatorio en la materia que está siendo discutido actualmente.



# Definiciones y actores principales

Para comprender adecuadamente las obligaciones del régimen de protección de datos personales en Colombia, es preciso comprender el alcance y significado de términos transversales a la legislación, como lo son el dato personal, el tratamiento, el titular, el responsable y el encargado del tratamiento.

## Dato personal

Por dato personal debe entenderse cualquier información vinculada o vinculable a una o varias personas naturales determinadas o determinables. Por consiguiente, en Colombia debe considerarse como información personal cualquier dato que identifique o pueda identificar de manera directa o indirecta a un individuo.

## Tratamiento

Como se estableció previamente, la ley colombiana entiende por tratamiento cualquier operación que se realice sobre datos personales. Lo anterior, incluye la recolección, almacenamiento, uso, circulación, transmisión, transferencia y supresión de la información, entre otros.

## Titular

Es la persona natural cuyo datos personales son objeto de tratamiento. El titular, en conjunto con el responsable y el encargado del tratamiento, constituyen los actores principales de la legislación colombiana de protección de datos personales.

## Autorización

Es el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de los datos personales. Bajo la ley colombiana, la autorización constituye uno de los pilares fundamentales así como la regla general para legitimar el tratamiento de los datos personales.



## Responsable del tratamiento

Es la persona natural o jurídica, independientemente de su naturaleza, que por sí misma o en conjunto con otros, decide sobre el tratamiento de los datos personales. En términos generales, las compañías son generalmente responsables de los datos personales de sus empleados, proveedores y clientes.

## Encargado del tratamiento

Es la persona natural o jurídica, independientemente de su naturaleza, que por sí misma o en conjunto con otros, realiza el tratamiento de los datos personales por cuenta y bajo instrucciones de un responsable. Por ejemplo, los asesores externos son generalmente encargados de la información personal que envían sus clientes para efectos de la asesoría.

# Principales obligaciones de los encargados y responsables del tratamiento

Las obligaciones que se derivan de la ley colombiana de protección de datos personales dependen de la calidad en la que actúe la entidad o individuo que realiza el tratamiento de la información, es decir, si son responsables o encargados. Si bien existen obligaciones similares o idénticas para ambos actores, los responsables del tratamiento deben asumir un mayor compromiso al ser ellos quienes deciden sobre las bases de datos y las finalidades del tratamiento.

Es común que en una misma persona natural o jurídica recaigan simultáneamente las calidades de encargado y responsable. En ese caso, deberán observarse las obligaciones definidas para cada uno.

A continuación, se comparan las obligaciones principales de los responsables y encargados del tratamiento establecidas en la ley.



TEMAS	OBLIGACIONES EN CABEZA DE LOS RESPONSABLES	OBLIGACIONES EN CABEZA DE LOS ENCARGADOS
<b>Derechos de los titulares</b>	Garantizar a los titulares, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data (conocer, actualizar, rectificar y suprimir sus datos personales).	Garantizar a los titulares, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data (conocer, actualizar, rectificar y suprimir sus datos personales).
<b>Legitimación del tratamiento de los datos personales</b>	Solicitar y conservar las autorizaciones otorgadas por los titulares para el tratamiento de sus datos personales.	Realizar el tratamiento a la información personal de conformidad con: (i) las instrucciones y políticas de privacidad establecidas por el responsable y (ii) las autorizaciones otorgadas por los titulares.
<b>Seguridad de la información personal</b>	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
<b>Políticas internas para el tratamiento de la información personal</b>	Adoptar una política para el tratamiento de datos personales y ponerla a disposición de los titulares, así como manuales y procedimientos para garantizar el adecuado cumplimiento de la ley, incluyendo la implementación de un oficial o comité de privacidad.	Adoptar una política para el tratamiento de datos personales y ponerla a disposición de los titulares, así como manuales y procedimientos para garantizar el adecuado cumplimiento de la ley, incluyendo la implementación de un oficial o comité de privacidad.
<b>Notificación de incidentes de seguridad</b>	Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio -SIC) cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.	Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio - SIC) cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
<b>Registro de bases de datos</b>	Registrar sus bases de datos en el Registro Nacional de Bases de Datos (RNBD), el cual es un directorio público administrado por la Superintendencia de Industria y Comercio.	N/A

# Transferencias y transmisiones internacionales de datos personales

La normatividad colombiana hace especial énfasis en el envío de información a otros países, y define lineamientos específicos con el objetivo de proteger la información que es enviada o accedida por terceros en el exterior. Para ello, distingue dos categorías.

## Transmisión internacional

Implica el envío de información personal a una persona natural o jurídica ubicada en el exterior, quién realizará el tratamiento de datos personales bajo las instrucciones de un responsable. Como ejemplos de transmisiones internacionales de datos personales se encuentran

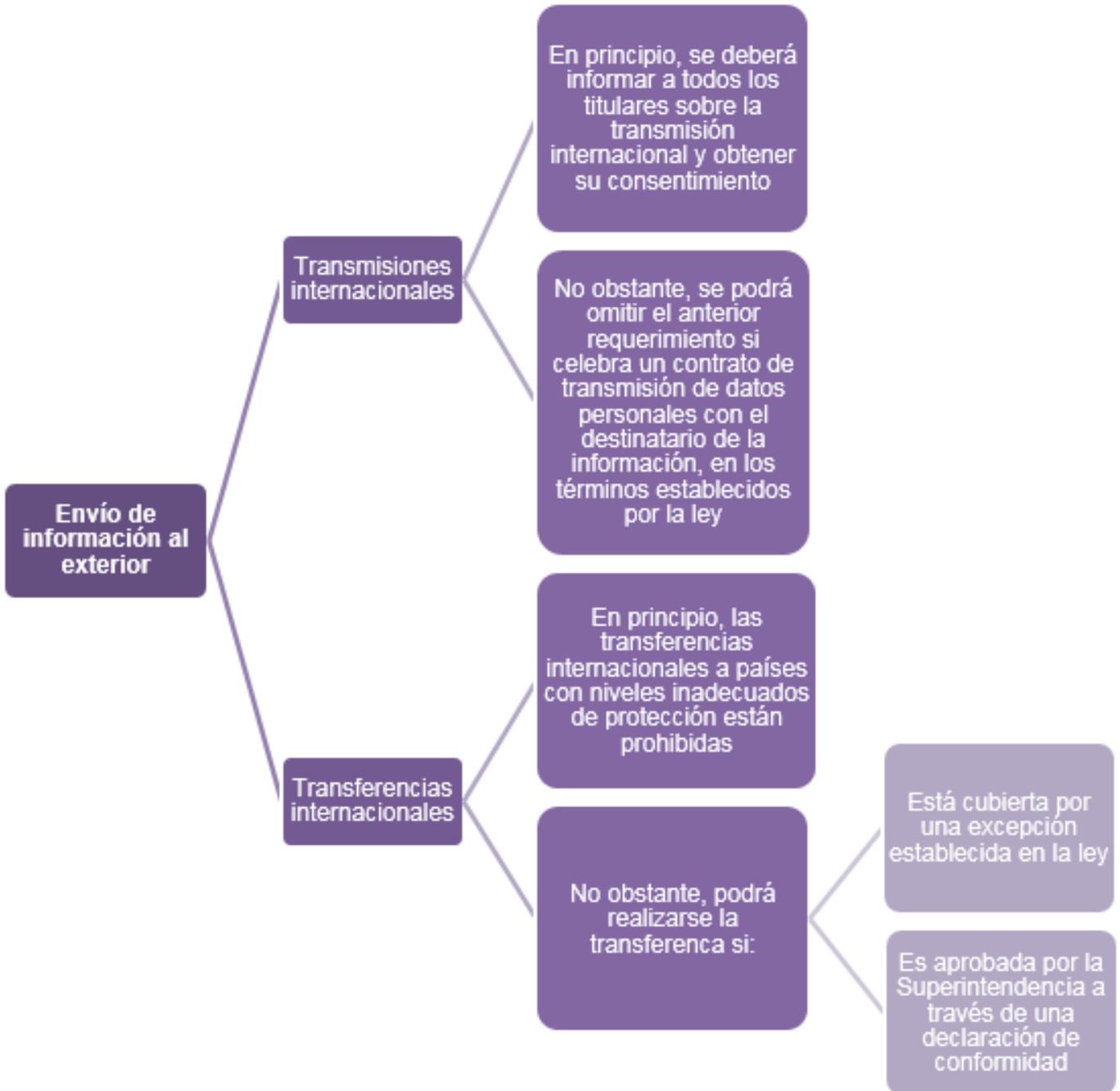
- (i) la contratación de servicios de tercerización (outsourcing) con entidades ubicadas en el exterior, que impliquen el envío de bases de datos o información personal (Ej. Procesos de gestión de nómina, servicios de salud en el exterior, etc.); o
- (ii) la contratación de servicios en la nube, cuando el proveedor almacena información en un servidor ubicado fuera del país.

## Transferencia internacional

Implica el envío de información personal a una persona natural o jurídica ubicada en el exterior, quien decidirá autónomamente sobre las finalidades y el tratamiento de la información personal. Como un ejemplo de esta figura, se encuentra el envío de información de una compañía filial a su casa matriz, cuando ésta última utiliza la información según sus propios parámetros.

Las transmisiones y transferencias internacionales constituyen regímenes distintos con obligaciones diversas. Por lo tanto, si se realizan transmisiones o transferencias internacionales de datos personales se deberá tener en cuenta lo siguiente:







## Notificación de incidentes de seguridad

La ley colombiana impone la obligación de notificar a la autoridad de protección de datos (Superintendencia de Industria y Comercio) cuando se presenten incidentes de seguridad que generen riesgos en la administración de la información personal. Esta obligación recae tanto en los responsables como en los encargados que realicen cualquier tipo de tratamiento de información personal en territorio colombiano.

Si bien no existe una definición única de incidente de seguridad, la ley colombiana se refiere a ellos en los siguientes términos:

a) La Ley 1581 de 2012 establece que tanto en los responsables como en los encargados recae la obligación de “informar a la autoridad de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares”.

b) El capítulo segundo de la Circular Única de la Superintendencia de Industria y Comercio define los incidentes de seguridad como la violación de códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable o su encargado.

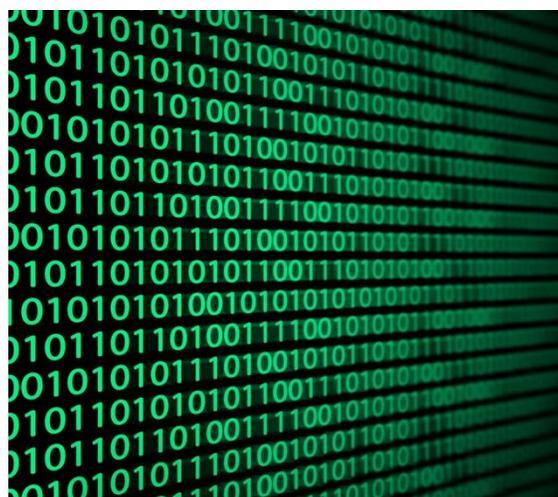
De manera adicional, la Superintendencia de Industria y Comercio estableció una definición a través de su Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*). Si bien dicho documento no es vinculante, establece los parámetros y definiciones que la autoridad de datos considera adecuados para la gestión integral de la información personal. En relación a los incidentes de seguridad, la Guía establece que “se refieren a cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que atente contra la seguridad de los datos personales en ellos almacenados”. En otras palabras, y considerando las definiciones anteriores es posible formular que un incidente de seguridad es una violación a la infraestructura de información física o tecnológica de un responsable o encargado del tratamiento, que compromete la disponibilidad, integridad o confidencialidad de la información personal contenida en ella.

Por otro lado, la Superintendencia de Industria y Comercio ha delimitado la información que debe aportarse al momento de notificar un incidente de seguridad. Por lo tanto, el reporte debe contener, como mínimo, la siguiente información:

- Tipo de incidente
- Fecha del incidente
- Fecha de conocimiento del incidente
- Causal
- Tipo de información comprometida
- Cantidad de titulares afectados

Al día de hoy, la legislación no ha definido un procedimiento específico para la notificación de los incidentes de seguridad. Sin embargo, la Superintendencia de Industria y Comercio permite a los responsables del tratamiento realizar la notificación a través del Registro Nacional de Bases de Datos (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.

Finalmente, es importante tener en cuenta que los responsables y encargados del tratamiento no están obligados a informar a los titulares de los datos personales sobre la ocurrencia incidentes de seguridad. A pesar de lo anterior, en la Guía para la Implementación del Principio de Responsabilidad Demostrada se recomienda implementar mecanismos eficientes para informar a los titulares sobre la ocurrencia de incidentes de seguridad y sus posibles consecuencias, así como proporcionar herramientas para minimizar el daño potencial o causado. Por lo anterior, aún si la notificación a titulares no es obligatoria, puede ser valorada por la autoridad como un ejercicio de transparencia.





## Vigilancia y sanciones

La entidad designada para la vigilancia del régimen de protección de datos personales es la Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales. Tenga en cuenta que el incumplimiento de cualquiera de las disposiciones establecidas en la ley puede desencadenar las siguientes sanciones:

- a) Multas hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes (aproximadamente COP\$1.475.000.000 o USD \$500.000)
- b) Suspensión o cierre temporal de las actividades relacionadas con el tratamiento de datos personales
- c) Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

En la actualidad, La mayoría de las sanciones impuestas por la autoridad hacen referencia a la violación del régimen de Habeas Data en el sector Financiero (Ley 1266 de 2008). No obstante, respecto al régimen general de protección de datos personales, las violaciones más recurrentes se derivan de:

Ley 1581 de 2012	
<b>Responsables del tratamiento</b>	No solicitar y/o conservar la autorización de los titulares para el tratamiento de sus datos personales.  No implementar medidas de seguridad adecuadas para la protección de la información
<b>Encargados del tratamiento</b>	Permitir el acceso a la información a personas no autorizadas.



# Proyectos regulatorios

En la actualidad, el tema que ha generado mayor discusión y controversia en materia de protección de datos personales es la transferencia de información al exterior. Por lo anterior, 17 de julio de 2017, la Superintendencia de Industria y Comercio presentó un nuevo proyecto de circular con el objetivo de desarrollar la regulación existente en materia de transferencias internacionales de datos personales. En concreto, el proyecto de circular establece de manera explícita los estándares que deben considerarse para determinar si un país cuenta con un nivel adecuado de protección de datos personales, así como una lista de países que cuenta con dicho nivel. De igual manera, se determinan parámetros específicos en relación al procedimiento para solicitar una declaración de conformidad ante la Superintendencia de Industria y Comercio.

Conforme lo anterior, el proyecto de circular contiene las siguientes disposiciones:

## Estándares de un nivel adecuado de protección

Para determinar si un país ofrece un nivel adecuado de protección de datos personales, deberán considerarse los siguientes estándares:

- (i) la existencia de normas aplicables al tratamiento de datos personales;
- (ii) la consagración normativa de principios aplicables al tratamiento de datos personales, derechos en cabeza de los titulares y deberes de responsables y encargados del tratamiento;
- (iii) la existencia de medios y vías judiciales y administrativas para garantizar la aplicación efectiva de la ley y los derechos de los titulares; y
- (iv) la existencia de autoridades competentes encargadas de la supervisión del tratamiento de los datos personales y el cumplimiento de la legislación aplicable. Conforme a lo anterior, corresponde a los responsables del tratamiento verificar que el país receptor de la información cumple con los estándares anteriormente mencionados, en aras de legitimar la transferencia internacional de los datos personales.

## Países que ofrecen niveles adecuados de protección

Según el proyecto de circular se consideran países con un nivel adecuado de protección los siguientes: Alemania, Austria, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia, y los países que han sido declarados con nivel adecuado de protección por la Comisión Europea. Las transferencias internacionales hacia Estados Unidos podrán realizarse siempre y cuando la empresa receptora se haya adherido al marco del “Privacy Shield”, establecido en la Unión Europea en el año 2016.

## Procedimientos relativos a las declaraciones de conformidad

Si los responsables del tratamiento no logran justificar la transferencia internacional a través de las excepciones de la ley, los estándares de un nivel adecuado de protección o el listado de países que ofrecen dicho nivel, deberán solicitar una declaración de conformidad ante la Superintendencia de Industria y Comercio. Para ello, se deberá radicar una petición ante el Grupo de Gestión Documental y Recursos Físicos o enviar

una solicitud al correo electrónico [contactenos@sic.gov.co](mailto:contactenos@sic.gov.co), aportando la información descrita en la “Guía para solicitar la declaración de conformidad”, en idioma español. El trámite para la solicitud de una declaración de conformidad se regirá por lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) en relación al procedimiento administrativo general.

## Declaración de conformidad tácita

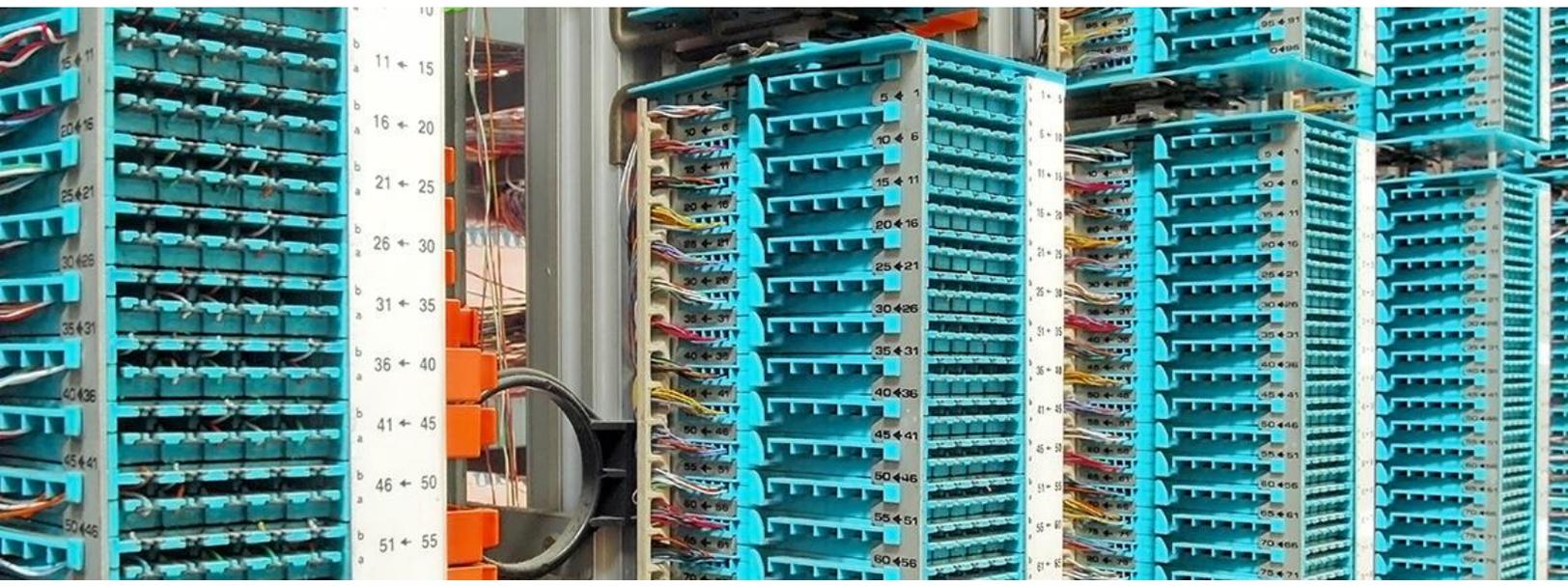
Los responsables del tratamiento podrán suscribir un contrato de transferencia u otro instrumento jurídico que garantice la protección de los datos objeto de la transferencia internacional, el cumplimiento de los principios que rigen el tratamiento y establezca las obligaciones de cada una de las partes. Si el instrumento jurídico consta con todos los elementos anteriormente mencionados y el responsable declara previamente la operación a realizar y la existencia del documento ante la Superintendencia de Industria y Comercio, se presumirá que la operación es viable y que cuenta con una declaración de conformidad. Sin perjuicio de lo anterior, la Superintendencia de Industria y Comercio podrá verificar las condiciones de la transferencia internacional, en cualquier momento, y podrá investigar y sancionar el incumplimiento de la legislación colombiana de protección de datos personales.

En resumen, si el nuevo proyecto de circular fuese aprobado, las opciones para legalizar la transferencia internacional de datos personales son:

1. Realizar la transferencia conforme una de las excepciones establecidas en la Ley 1581 de 2012; o
2. Verificar que el país receptor de la información personal esté incluido en el listado de países que cuentan con un nivel adecuado de protección; o
3. Verificar que el país receptor de la información personal cumpla con los estándares de un nivel adecuado de protección; o
4. Solicitar una declaración de conformidad ante la Superintendencia de Industria y Comercio a través de un procedimiento administrativo general; o
5. Suscribir un contrato de transferencia u otro instrumento jurídico según los requisitos establecidos por el proyecto de circular, e informar previamente a la Superintendencia de Industria y Comercio sobre la transferencia que se realizará y la existencia del instrumento legal.

Según el proyecto de circular, los responsables del tratamiento siempre deberán ser capaces de demostrar la implementación de medidas adecuadas y efectivas para garantizar la seguridad y el adecuado tratamiento de los datos personales que se transfieren al exterior, aún si dicha operación se realiza a países que tienen un nivel adecuado de protección. Adicionalmente, el proyecto considera que el simple tránsito transfronterizo o redirección de los datos no equivale a una transferencia de datos a terceros países.

Actualmente, el proyecto de circular se encuentra en etapa de discusión, y en consecuencia, las transferencias internacionales que se lleven a cabo por el momento deberán ceñirse a las condiciones establecidas por la Ley 1581 de 2012.



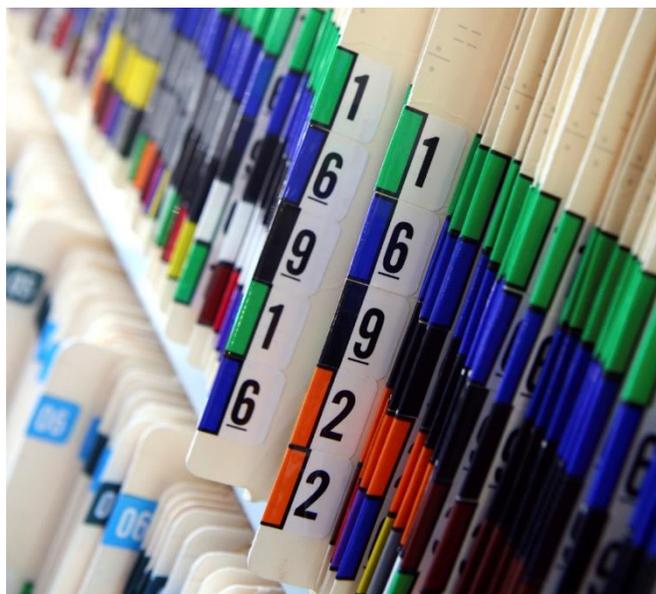
# Conclusiones

Si bien la protección de datos personales es un tema relativamente nuevo en Colombia, es cada día más relevante para las compañías que operan en el país. Por un lado, las empresas son más conscientes de su responsabilidad en el manejo de la información, debido al papel activo de la Superintendencia a través de las investigaciones y la imposición de sanciones.

Por otro lado, los ciudadanos son más conscientes de la importancia de la protección de su información personal, así como de los mecanismos dispuestos para ejercerlos.

El papel de la Superintendencia de Industria y Comercio ha sido de vital importancia al momento de hacer cumplir la regulación colombiana en la materia, al ser el motor que ha impulsado a las empresas a implementar políticas internas para la gestión de la información que aseguren la protección de la información de carácter personal. Si bien la cultura de protección de datos personales es aún incipiente en Colombia, es posible afirmar que, aunque quede trabajo por hacer, se está en una dirección adecuada.

No obstante lo anterior, es imposible desconocer la creciente importancia de la privacidad y la protección de datos personales en un mundo altamente digitalizado y globalizado, Por lo tanto, el cumplimiento de la normatividad debe realizarse como parte de una cultura que valora y entiende la importancia de la privacidad en nuestro entorno y no como un mero requisito para evitar sanciones.



©2017 Dentons. Dentons una firma legal global que presta servicios a sus clientes en todo el mundo a través de sus firmas miembro y afiliadas. Este documento no fue diseñado para prestar asesoría legal o de otro tipo y usted no debe tomar o abstenerse de tomar ninguna acción basado en su contenido. Estamos suministrando información en el entendido que usted acuerda mantenerla confidencial. Si usted no proporciona información confidencial, pero no nos da instrucciones ni nos contrata, podremos actuar a nombre de otro cliente o para cualquier asunto en el que dicha información confidencial sea relevante. Publicidad de Abogado. Favor visite [dentons.com](http://dentons.com) para las Notificaciones Legales.