GUÍA PARA LA IMPLEMENTACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

EN LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

DELEGATURA PARA LA PROTECCIÓN
DE DATOS PERSONALES
2019-2021

Industria y Comercio
SUPERINTENDENCIA

El futuro es de todos
Gobierno de Colombia

Industria y Comercio
SUPERINTENDENCIA

GUÍA PARA LA IMPLEMENTACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

EN LAS TRANSFERENCIAS INTERNACIOANLES DE DATOS PERSONALES

DELEGATURA PARA LA PROTECCIÓN
DE DATOS PERSONALES

CONTENIDO

PÁG.

CONTENIDO

INTRODUCCIÓN

Para efectos de la circulación transfronteriza de datos, la Superintendencia de Industria y Comercio (SIC) —autoridad colombiana de protección de datos personales— ha establecido que los siguientes países tienen nivel adecuado de protección de datos[1]:

Alemania, Australia, Austria, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, 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 el nivel adecuado de protección por la Comisión Europea (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda).

Al mismo tiempo, la SIC, mediante la Circular Externa 5 del 10 de agosto del 2017, ordenó lo siguiente en el parágrafo primero del numeral 3.2: ***"Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, Los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia[2]".***

Como se observa, para transferir datos a otros países no es suficiente que el país de destino esté catalogado por la SIC como un país con nivel adecuado de protección, sino que además es necesario que el responsable del tratamiento pueda demostrar que ha tomado medidas adecuadas, útiles y prácticas para lograr estos dos objetivos:

(1) Garantizar el adecuado tratamiento de los datos personales que se transfieren a otro país.
(2) Conferir la seguridad de "los registros al momento de efectuar dicha transferencia".

No obstante lo anterior, la guía de la SIC del 28 de mayo del 2015 sobre responsabilidad demostrada (accountability) no dice nada sobre las transferencias internacionales —sólo menciona las transmisiones que son sustancialmente diferentes—. En efecto, si bien los datos pueden salir del territorio de la República de Colombia porque han sido transferidos, transmitidos o recolectados internacionalmente, en el caso de las transmisiones internacionales el exportador de la información sigue siendo responsable del debido tratamiento de los datos que transmitió a un encargado ubicado o domiciliado en otro país.

Así las cosas, se hace necesario expedir una guía complementaria que desarrolle lo atinente a la responsabilidad demostrada en las transferencias internacionales de datos personales.

1 Cfr. SIC Circulares externas 5 y 8 de 2017 y 2 de 2018.
2 Cfr. el numeral 3.2 de la Circular 5 del 2017 de la SIC.

OBJETIVOS Y PRECISIONES

Esta guía[3] tiene como propósito presentar algunas sugerencias a quienes envían datos personales desde Colombia a otros países, con el fin de orientarlos para que implementen medidas de responsabilidad demostrada con miras a dar cumplimiento a la regulación colombiana.

Este documento no es un concepto legal, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucran las transferencias y las transmisiones internacionales de datos, pues ello es un asunto interno que define cada organización a la luz de las particularidades de cada exportación de datos personales.

Las orientaciones contenidas en este texto solo comprenden algunos de los temas más relevantes sobre transferencias. Por consiguiente, el lector debe tener claro que este documento no incluye todos los deberes legales sobre la materia y que la omisión de algunos de ellos en esta guía no lo exime de cumplir todos los requerimientos legales.

3. Para la elaboración de esta guía se siguió el formato y se usaron contenidos de: (i) Red Iberoamericana de Protección de Datos (2019) Recomendaciones generales para el tratamiento de datos personales en la inteligencia; y (ii) Universidad de los Andes, Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática -GECTI- (2018) Guía GECTI para la implementación del principio de responsabilidad demostrada —accountability— en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Existe pluralismo terminológico para referirse a las transferencias y a las transmisiones internacionales de datos. así, por ejemplo, en varios documentos internacionales se les denomina de la siguiente manera:

"Circulación transfronteriza de datos personales" (OCDE, 1980),"Flujos transfronterizos de datos de carácter personal" (Convenio 108 de 1981), *"Transferencia de datos personales a países terceros"* (Directiva 95/46), *"Transferencia de datos a destinatarios no sometidos a las partes del Convenio"* (Protocolo adicional del 2001 al convenio 108), *"Flujo de datos a través de las fronteras"* (Resolución 45/95 de 1990 de la ONU), "Transferencia a otra persona u organización internacional" (APEC, 2004), "Transferencia internacional de datos" (APEC, 2013), "Transferencias internacionales" (Resolución de Madrid del 2009), *Transferencias de datos personales a terceros países u organizaciones internacionales"* (Reglamento UE 2016/679),"*Transferencias internacionales de datos personales"* (Red Iberoamericana de Protección de Datos, 2017) y "Flujo transfronterizo de datos" (OEA, 2021).

Al margen de su denominación, las transferencias internacionales se refieren al envío de datos personales desde un país por un responsable a otro responsable ubicado en otro u otros países. En últimas, los datos personales son remitidos o exportados desde un país a empresas y organizaciones ubicadas en un territorio diferente al del país de envío. Se trata de un proceso de exportación de datos personales.

No obstante, según la regulación colombiana, las expresiones para referirse a este fenómeno difieren cuando se exporta de un responsable a otro responsable (caso en el cual se denomina *transferencia*) o cuando se envían datos de un responsable a un encargado (situación que se denomina *transmisión*). A continuación nos referiremos brevemente a este último.

TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES

La transmisión de datos consiste en la entrega o el envío de datos personales por un responsable al encargado del tratamiento de ellos. El artículo 24 del Decreto 1377 del 2013 —incorporado en el Decreto 1074 del 2015— establece que las transmisiones internacionales *"no requerirán ser informadas al titular ni contar con su consentimiento cuando exista un contrato"* de transmisión entre el responsable y el encargado. Dicho contrato de transmisión internacional de datos personales está regulado en el artículo 25 de dicho decreto, del cual se deriva lo siguiente:

En primer lugar, se recalca que el encargado realizará el tratamiento bajo la responsabilidad y el control del responsable del tratamiento. Por eso, en el contrato se debe definir el alcance del tratamiento, sus finalidades y las obligaciones del encargado respecto del titular del dato y el responsable. En segundo lugar, se precisa que las obligaciones fijadas en la Política de Tratamiento de Información (PTI) del responsable deben ser cumplidas por el encargado observando la mencionada PTI. En otras palabras, la PTI del responsable hace parte del contrato y debe ser observada por el encargado.

En tercer lugar, la finalidad del tratamiento debe ser la autorizada por el titular del dato o por la ley.

El responsable debe asegurarse de estar legitimado para tratar los datos y de encomendar al encargado realizar actividades autorizadas por el titular o permitidas por la ley. Se recalca que el uso de la información no es ilimitado sino que depende de los supuestos mencionados (autorización o ley). Finalmente, y en adición a lo anterior, en el contrato es obligatorio incluir, por lo menos, estas obligaciones a cargo del encargado, de acuerdo con lo dispuesto por el citado artículo 25:

OBLIGACIONES LEGALES DEL ENCARGADO QUE SE DEBEN INCLUIR EN EL CONTRATO:

01 Dar aplicación a las obligaciones del Responsable bajo la Política de Tratamiento de Información

02 Realizar el Tratamiento de acuerdo con la finalidad autorizada por los Titulares y con las leyes

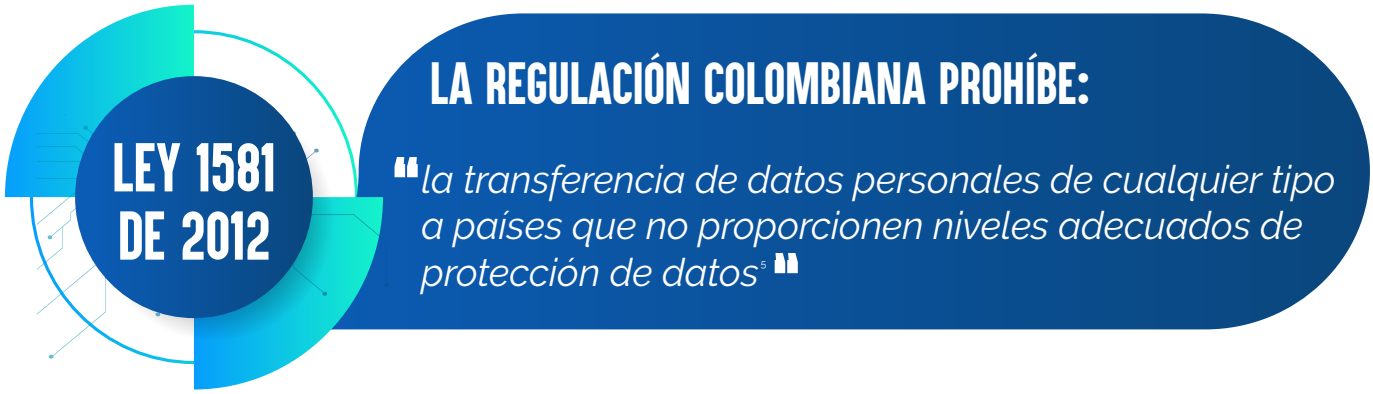
03 Tratar los datos, a nombre del Responsable, conforme a los principios que los tutelan.

04 Salvaguardar la seguridad de las bases de datos

05 Guardar la confidencialidad respecto del tratamiento de los datos personales

OBJETIVOS DE LAS REGLAS SOBRE TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Las regulaciones sobre transferencia internacional de datos o *"flujo transfronterizo de datos"* procuran garantizar que el nivel de protección de los datos personales de los ciudadanos de un país no disminuya o desaparezca cuando esa información es exportada a otro u otros países. Esta regla se conoce como el principio de continuidad de la protección de datos, el cual se fundamenta en que *"la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales"*[4].



La regulación colombiana es enfática en señalar con absoluta claridad que los estándares fijados para establecer si un país tiene dicho nivel "en ningún caso podrán ser inferiores"[5] a los que contempla la Ley 1581 de 2012. Como se observa, para el caso colombiano no se puede enviar datos a un país que tenga un grado de protección inferior al previsto en la precitada norma.

La exportación de información personal no pueden convertirse en un escenario reductor del nivel de protección que se le confiere al titular del dato en el país desde donde se exportan datos personales. Dichas actividades no deben facilitar, permitir ni tolerar la vulneración de los derechos de las personas ni la disminución de las garantías con que cuentan en el país exportador.

5 Cfr. República de Colombia. Ley 1581 de 2012, artículo 26

4 De Frutos, José Manuel. 2008. Globalización de la privacidad: hacia unos estándares comunes. Conferencia realizada en el VI Encuentro Iberoamericano de Protección de Datos, 27-30 de mayo del 2008, Cartagena, Colombia.

RECOMENDACIONES

I. EFECTUAR ESTUDIOS DE IMPACTO DE PRIVACIDAD ANTES DE ENVIAR LOS DATOS A OTRO PAÍS

Previo a la exportación de los datos, y en la medida en que sea probable que el mismo entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, se sugiere efectuar una evaluación de impacto en la privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.

Dicha evaluación debería incluir, como mínimo, lo siguiente:

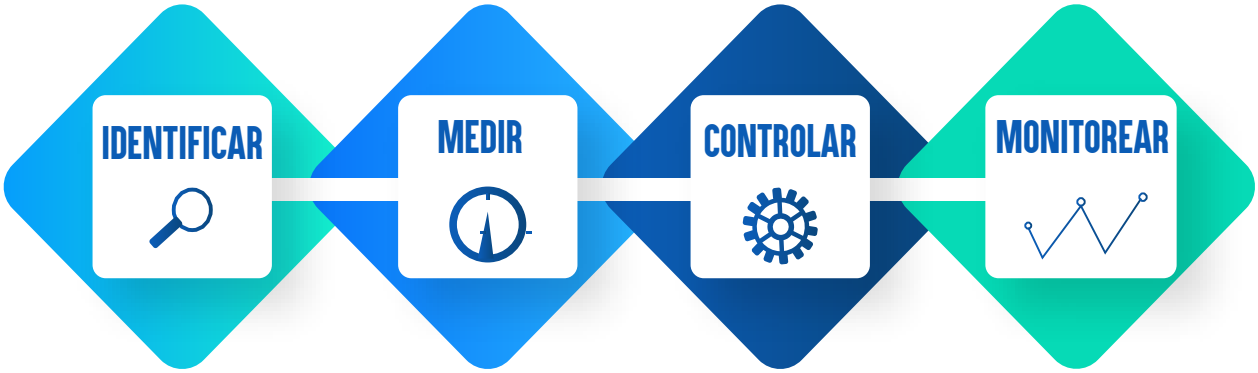
- Una descripción detallada de las operaciones de Tratamiento de datos personales que involucra la transferencia internacional de los datos.
- Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales.
- La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del Principio de Responsabilidad Demostrada.

Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales*"[6] que les permita "*identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales*"[7].

Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de *software*, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

SISTEMA DE ADMINISTRACIÓN DE RIESGOS



6 Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)". Págs 16-18.
7 Ibid. Pág. 16

II. INCORPORAR LA PRIVACIDAD, LA ÉTICA Y LA SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

La privacidad desde el diseño y por defecto (Privacy by Design and by Default**),** es considerada una medida proactiva para cumplir con el Principio de Responsabilidad Demostrada. Al introducir la privacidad desde el diseño, se está buscando garantizar el correcto Tratamiento de los datos objeto de transferencia internacional.

La Privacidad por Diseño *"promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo [sic] por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización"*[8]. Por eso, desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos Tratamientos de datos personales.

La ética desde el diseño y por defecto debe irradiar los procesos de exportación de datos, teniendo que ser parte del ADN de cualquier aspecto relacionado con esa actividad.

Lo anterior también debe predicarse de la seguridad en el Tratamiento de datos personales. Sin seguridad no habrá debido Tratamiento de los mismos.
Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que eviten:

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el estado de la técnica, y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad deben ser objeto de revisión, evaluación y mejora permanente.

8. Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

III. VERIFICAR QUE ESTÁ FACULTADO PARA TRANSFERIR O TRANSMITIR LOS DATOS PERSONALES A OTRO PAÍS

Si va a exportar datos personales a otros países es necesario que establezca si usted está facultado para enviar la información fuera territorio de la República de Colombia.

Si no está facultado, tenga presente que se expone a investigaciones administrativas o de naturaleza penal. Sobre este último aspecto, recuerde que la Ley 1273 del 2009 creó algunos tipos penales que sancionan, entre otros, ciertos aspectos relacionados con el tratamiento de datos personales como el acceso no autorizado a sistemas de información, la destrucción o manipulación de datos, la suplantación de sitios virtuales para capturar datos personales y la violación de datos personales. Este último delito sanciona con prisión de cuatro a ocho años y multa de 100 a 1000 salarios mínimos legales mensuales a quien *"sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda,* ***intercambie, envíe****, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes"* (destacamos).

Como se observa, son diversas las conductas que generan responsabilidad penal en el tratamiento de datos personales. Esto hace que tanto los responsables como los encargados del tratamiento tengan que realizar una gestión muy cuidadosa y diligente para no incurrir en un delito. Lo anterior es aún más grave si se tiene en cuenta que la pena señalada se aumenta de la mitad a las tres cuartas partes si la conducta la cometiere "[…] el responsable de la administración, manejo o control de dicha información". Además, dicha persona se expone a que se le imponga *"hasta por tres años la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales".*

IV. ESTABLECER CÓMO SE PROBARÁN LAS MEDIDAS DE *ACCOUNTABILITY* PARA TRANSFERIR LOS DATOS PERSONALES

Desde el inicio, su organización debe establecer la manera como probará que ha adoptado medidas útiles para cumplir las reglas sobre transferencias internacionales de datos. Es necesario tener presente que, "los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"9 y en el Decreto 1377 de 2013. (Incorporada en el decreto 1074 de 2015)

Medidas *"apropiadas"* son aquellas ajustadas a las necesidades del Tratamiento de datos. Y *"efectivas"*, son las que permiten lograr el resultado o efecto que se desea o espera. En otras palabras, no se deben adoptar medidas inoperantes, inservibles, inanes o infructuosas. Solo se deben instaurar aquellas adecuadas, correctas, útiles, oportunas y eficientes con el propósito de cumplir los requerimientos legales para realizar tratamiento de datos personales.

En suma, quienes exporten datos deben establecer medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas deben ser objeto de revisión y evaluación permanente a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los datos personales.

El reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas.

Se trata de una actividad constante que exige demostrar un cumplimiento real y efectivo en la práctica de sus labores.

En este aspecto es esencial realizar entrenamientos periódicos y especializados al equipo humano de la organización para proveerles la experticia, guía y herramientas que requieren para el correcto desarrollo de las tareas que involucren cualquier Tratamiento de datos personales.

9 Cfr. Artículo 26 del Decreto 1377 de 2013.

V. ASEGURAR EL CUMPLIMIENTO DE LAS FINALIDADES QUE SE DEBEN ALCANZAR CON LAS MEDIDAS DE ACCOUNTABILITY.

Debe recordarse que las medidas de accountability, por lo menos deben ser adecuadas y pertinentes para garantizar los siguientes objetivos establecidos en la circular 5 de 2017 de la SIC:

(I) Garantizar el adecuado tratamiento de los datos personales que se transfieren a otros países.
(II) Conferir seguridad a "los registros al momento de efectuar dicha transferencia"

El adecuado tratamiento de los datos personales supone, por lo menos, que en el país de destino de la exportación se respeten los derechos del titular del dato y que el tratamiento de datos en ese país garantice el cumplimiento de los principios de tratamiento de datos que exige la regulación del país desde donde se exporta la mencionada información.

VI. PREVER LAS TRANSFERENCIAS ULTERIORES DE DATOS PERSONALES

Se deben establecer reglas para el reenvío de los datos del territorio de destino inicial (país A) de la exportación de los datos a otros (países B, C, D, etc). Tenga presente que si esto se deja sin control, al final del día los datos pueden terminar en países o empresas que en el práctica no garantizan un nivel adecuado de protección de datos.

VII. REPLICAR MEDIDAS PROACTIVAS DEL TRATAMIENTO DE DATOS PERSONALES A LAS TRANSFERENCIAS INTERNACIONALES DE DICHA INFORMACIÓN

Internacionalmente se ha recomendado la implementación de medidas proactivas de protección de datos con miras a mejorar el cumplimiento de las normas respectivas, así como consolidar y fortalecer el debido tratamiento de datos personales en las organizaciones. Dentro de dichas herramientas se encuentran, entre otras, las siguientes:

DESIGNACIÓN DE UN DELEGADO DE PROTECCIÓN DE DATOS

Esta persona podría ser, entre otras, la encargada de verificar que en la organización se cumplan todos los requerimientos legales y las exigencias de la autoridad de protección de datos para transferir datos a otros países. Además, sería la que se responsabilizaría de realizar planes de monitoreo y evaluación respecto del tratamiento de los datos exportados.

EVALUACIÓN DE IMPACTO DE PRIVACIDAD O DE PROTECCIÓN DE DATOS.

Según el caso, estos estudios son útiles en proyectos de gran impacto o de alto riesgo que involucren, por ejemplo, el tratamiento de datos personales sensibles o de menores de edad.

CAPACITACIÓN Y ENTRENAMIENTOS ESPECIALIZADOS.

Realizar periódicamente actividades de educación y entrenamientos específicos a las personas a cargo de enviar datos personales a otros países con el fin de verificar si cuentan con la preparación suficiente y especializada para realizar transferencias o transmisiones internacionales de datos personales.

IMPLEMENTACIÓN DE PLANES DE MONITOREO, EVALUACIÓN Y CONTINGENCIA

Según el caso, resulta pertinente que el responsable (exportador de los datos) pueda realizar monitoreo o auditorías al responsable o encargado ubicado en el país destinatario de los datos para que verifique si éste está cumplimiento adecuadamente con sus obligaciones respecto de, entre otras, seguridad, uso debido de los datos y confidencialidad.

Se deben fijar las pautas o acciones que seguirá frente a situaciones graves o inesperadas respecto de los datos enviados a otro estado. Por ejemplo: ¿qué haría en caso de que se presente un ataque informático que comprometa la seguridad y confidencialidad de los datos transferidos o transmitidos a otro país?

VIII. ARTICULAR LAS HERRAMIENTAS DE ACCOUNTABILITY EN UN CONTRATO AJUSTADO A LAS PARTICULARIDADES DE CADA TRANSFERENCIA.

Los contratos representan una alternativa jurídica para demostrar la implementación de medidas de accountability en las transferencias internacionales de datos. Aunque existen cláusulas tipo[10] en esta materia, es crucial que el contrato sea consistente con las peculiaridades y necesidades de cada organización. Así mismo, es relevante que el exportador de los datos trate de establecer si el receptor de los mismos en otro país es una empresa u organización confiable que cumplirá las obligaciones .

Para la redacción del contrato tenga presente varios aspectos:

- La naturaleza jurídica de los datos que se exportarán a otro país. Dependiendo de la misma (sensibles, de menores de edad, privados, semiprivados, públicos) pacte medidas especiales de protección. Recuerde, por ejemplo, que para el tratamiento de datos sensibles se exige una responsabilidad reforzada, es decir, mayores medidas de seguridad, mayores restricciones de acceso, uso y circulación.

- Las medidas de seguridad que debe cumplir el destinatario de los datos exportados a otro país.

- La cantidad de datos que se exportarán.

- ¿Cuáles son los derechos que el destinatario de la información debe garantizar al titular del dato?

- ¿Cuáles son los principios del tratamiento de datos personales que el destinatario de los datos debe observar o garantizar?

- ¿Quiénes podrán tener acceso a la información exportada?

- Los mecanismos para que el titular del dato pueda ejercer sus derechos de manera sencilla y expedita ante el destinatario de los datos exportados.

- Las finalidades para las cuales se transfiere.la información. Es muy importante dejar claro qué puede y qué no puede hacer el destinatario de los datos transferidos.

- ¿Cuál será el límite de tiempo durante el cual el destinatario de los datos transferidos podrá tratarlos?

10 La Comisión Europea, por el ejemplo, el 4de junio de 2021 adoptó la Decisión de Ejecución (UE) 2021/914relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679. En: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=es

- La ley de protección de datos que regirá el contrato: ¿será la ley del país del exportador de los datos o la del importador de los mismos? Si se quiere garantizar el principio de "continuidad de protección de datos" a que nos referimos en este documento, lo recomendable es que el contrato se rija por la ley de protección de datos del país desde donde se exportarán.

- La posibilidad o no de realizar transferencias ulteriores a otros países. Deje claro si los datos inicialmente transferidos a un país **(A)**, pueden ser posteriormente transferidos desde ese país **(A)** a otro país **(B).** En caso positivo, establezca las condiciones que se deben observar para dicho efecto.

- ¿Qué hacer para recuperar los datos transferidos y garantizar los derechos de los titulares de los mismos cuando el destinatario de la exportación incumpla el contrato?

- ¿Quién (es) responderá (n) ante las autoridades y los titulares de los datos por los eventuales indebidos tratamientos de la información exportada y los daños y perjuicios causados?

- ¿Cuál será la responsabilidad (conjunta o solidaria) del exportador y del importador de los datos frente al titular de los mismos por las eventuales vulneraciones de sus derechos o los daños y perjuicios causados?

- Defina quién gestionará los incidentes de seguridad que afecten datos personales, así como el responsable de informar a las autoridades y a los titulares de los datos.

- ¿Qué se hará con los datos una vez termine el contrato?

- Establezca los responsables de cada parte junto con sus datos y canales de contacto para efectos del cumplimiento del contrato.

IX. INCREMENTAR LA CONFIANZA Y LA TRANSPARENCIA CON SUS CLIENTES Y TERCEROS TITULARES DE DATOS PERSONALES

Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que se realice a través del uso de las tecnologías[11]. Lo cual ha sido reiterado al establecer que, "las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización"[12].

La confianza se entiende como la expectativa de que *"se puede contar con la palabra del otro"* y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y lleva a cabo las acciones prometidas[13].

Una organización transparente puede generar mayor confianza en sus clientes y en los Titulares de los datos. Para lograrlo se sugiere lo siguiente:

a. Mantener canales abiertos de comunicación y divulgación del uso de los datos personales en los procesos de transferencias internacionales de datos. Es importante que esto se haga en términos muy claros y completos, utilizando un lenguaje sencillo que pueda ser entendido por cualquier persona.

b. Implementar un sistema efectivo de debida y oportuna atención de quejas y reclamos.

c. Cumplir en la práctica lo que se dice o promete en las Políticas de Tratamiento de Información.

Finalmente, es importante recalcar que todas las sugerencias anteriores sólo están enfocadas para implementar el principio de accountability en la circulación transfronteriza de datos personales, ya sea a través de transferencias o mediante transmisiones internacionales de datos. Como tal, esta guía es de carácter especial y complementario a la Guía para implementación del principio de responsabilidad demostrada (accountability) expedida por la SIC el 28 de mayo del 2015.

11 Cfr. Reichel & Shefter. Harvard Business Review. Jul-Ago, 2000.
12 Cfr. Edelman Trust Barometrer de 2019.https://www.edelman.com/trust-barometer
13 Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

GLOSARIO

Para mayor comprensión de algunos términos utilizados en esta guía, a continuación, transcribimos la denominación exacta de cada uno y su definición legal:

AUTORIZACIÓN:

"Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales"[14].

BASE DE DATOS:

"Conjunto organizado de datos personales que sea objeto de Tratamiento"[15].

ENCARGADO DEL TRATAMIENTO:

"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"[16].

RESPONSABLE DEL TRATAMIENTO:

"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos"[17].

TITULAR:

"Persona natural cuyos datos personales sean objeto de Tratamiento"[18].

TRATAMIENTO:

"Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"[19].

DATO PERSONAL:

"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"[20].

DATO PRIVADO:

"Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular"[21].

DATO PÚBLICO:

"Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva"[22].

14 Literal a) del artículo 3 de la Ley 1581 de 2012.
15 Literal b) del artículo 3 de la Ley 1581 de 2012.
16 Literal d) del artículo 3 de la Ley 1581 de 2012.
17 Literal e) del artículo 3 de la Ley 1581 de 2012.
18 Literal f) del artículo 3 de la Ley 1581 de 2012.
19 Literal g) del artículo 3 de la Ley 1581 de 2012.
20 Literal c) del artículo 3 de la Ley 1581 de 2012.
21 Literal h) del artículo 3 de la Ley 1266 de 2008.
22 Numeral 2 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.

DATO SEMIPRIVADO:

"Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley"[23].

DATOS SENSIBLES:

"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"[24].

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"[25].

TRANSMISIÓN:

"Tratamiento de datos personales que implica la comunicación de los mismos 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"[26].

23 Literal g) del artículo 3 de la Ley 1266 de 2008.
24 Artículo 5 de la Ley 1581 de 2012 y numeral 3 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario 1074 de 2015.
25 Numeral 4 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.
26 Numeral 5 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.

DOCUMENTOS CONSULTADOS

Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B10.pdf

Comisión Europea (2021) Decisión de Ejecución (UE)2021/914 relativa a las cláusulas contractuales tipo para latransferencia de datos personales a terceros países deconformidad con el Reglamento (UE) 2016/679.

Global Privacy Assemby (2020) Resolution on accountabilityin the development and use of artificial intelligence.

Red Iberoamericana de Protección de Datos (2019) Recomendaciones generales para el tratamiento de datos personales en la Inteligencia Artificial.

Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)".

Universidad de los Andes, Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática -GECTI- (2018) Guía GECTI para la implementación del principio de responsabilidad demostrada —accountability—en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.

Industria y Comercio

SUPERINTENDENCIA

www.sic.gov.co

@sicsuper

Superintendencia de Industria y Comercio de Colombia

Superintendencia de Industria y Comercio

Conmutador: **(571) 5 870 000** - Contact Center: **(571) 5 920 400**
Línea gratuita nacional desde teléfonos fijos: **01 8000 910 165**

El futuro es de todos

Gobierno de Colombia