Versión 5/11/2021

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

GUÍA DE IMPLEMENTACIÓN DE CLÁUSULAS CONTRACTUALES MODELO PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

INDICE

1. Introducción

El uso de cláusulas contractuales es una alternativa para poder realizar transferencias internacionales de datos personales. En ese sentido, el literal c) del inciso 1 del artículo 36 de los Estándares de protección de datos personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos (RIPD) dispone que "*El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos: … c. El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados Iberoamericanos aplicable en la materia*".

En línea con lo anterior, la presente guía busca establecer los principales aspectos que deben tenerse en cuenta cuando se realizan transferencias internacionales de datos personales (TIDP) mediante el uso de CCM (en adelante cláusulas contractuales modelo o CCM). Como tal, esta guía presenta algunas orientaciones para que sean tenidas en cuenta por quienes deben realizar TIDP a jurisdicciones no adecuadas desde los países miembros de la Red Iberoamericana de Protección de Datos Personales (RIPD).

Asimismo, en América Latina no existen cláusulas contractuales modelo aprobadas conjuntamente a nivel regional. Por eso la RIPD presenta como anexo a esta Guía un modelo de contrato de transferencia internacional en dos versiones, uno para transferencias entre Responsables y otro para transferencias de Responsables a Encargados. Se considera que estos dos modelos son un primer paso y se espera mas adelante elaborar modelos adicionales para transferencias de Encargado a Encargado y de Encargado a Responsable.

El contenido sustancial de ambos modelos sigue los lineamientos de los Estándares de protección de datos personales para los Estados Iberoamericanos de la RIPD[1] ("Estándares").

Las CCM propuestas en el Anexo son además compatibles en su estructuración con las recientes cláusulas contractuales tipo para la transferencia de datos personales a terceros países aprobados en junio de 2021 por la Comisión de la Unión Europea ("UE")[2] ya que en su esencia contienen elementos y principios similares.

[1] Cfr. Red Iberoamericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Disponibles en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

[2] Cfr. DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

2. Precisiones y limitaciones

Esta Guía es complementaria de las recomendaciones, documentos y regulación vigente en cada país de Iberoamérica[3]. Algunas normas de países de Iberoamérica contienen disposiciones especiales de TIDP e incluso varias contienen una previsión normativa para el uso de cláusulas contractuales y hasta han desarrollado modelos de cláusulas contractuales (ver punto 3.3. de esta Guía).

Esta Guía no reemplaza a las leyes locales ni opiniones de las distintas autoridades de protección de datos de la región.

Cabe aclarar también que, en caso de contradicción manifiesta entre este documento y alguna recomendación o guía de la autoridad local, se sugiere seguir la recomendación de dicha autoridad en el entendimiento que corresponde a la entidad pública encargada de velar por la protección de datos en determinada jurisdicción el determinar las reglas para hacer efectiva una TIDP.

En cualquier caso, la aplicación de esta Guía y el uso de los dos modelos contractuales anexos a la presente Guía deberá hacerse en armonía con las recomendaciones, resoluciones y determinaciones de las autoridades de protección de datos locales y, sobre todo, con la legislación local aplicable.

Para la elaboración de este documento, así como las de las CCM se tomaron como referencia los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la RIPD[4] para establecer los principios, términos, definiciones, obligaciones del Responsable y del Encargado y derechos de los titulares de datos personales. La Guía y las CCM no transcriben textualmente todos los aspectos de los mismos, sino que se tomaron los principios contenidos en los Estándares como fuente de todos los principios legales que corresponde aplicar en caso de una TIDP. Por lo tanto, este documento debe leerse de manera conjunta e integral con los citados Estándares, sin perjuicio de la eventual adaptación que puede realizar alguna autoridad local de protección de datos personales.

La presente Guía no es un concepto legal, ni un artículo académico, ni constituye asesoría jurídica de ninguna clase. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas porque ello es un asunto interno que corresponde decidir a cada organización a la luz de los objetivos y la magnitud de cada proyecto que implique transferir datos personales a jurisdicciones no adecuadas.

[3] Por ejemplo, ver las mencionadas en la sección de Documentos consultados de esta Guía.
[4] Cfr. Red Iberoamericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Disponibles en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

3. Antecedentes de las TIDP

3.1. Antecedentes internacionales

La Directiva de Protección de Datos de la Unión Europea del año 1995[5] fue la primera norma que implementó a nivel de derecho comunitario europeo la prohibición de TIDP a países no adecuados. La citada Directiva fue reemplazada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante Reglamento General de protección de Datos, RGPD)[6].

El RGPD contiene una detallada regulación de las transferencias internacionales de datos personales (arts. 44 a 50, RGPD). El art. 44 inc. 2 del RGPD permite las TIDP cuando se adoptan garantías adecuadas, entre las que se enumeran las cláusulas tipo de protección de datos aprobadas por la Comisión Europea o por alguna autoridad de control.

Hace dos décadas la Comisión de la Unión Europea -mediante la Decisión 2001/497/CE de la Comisión[7] y luego mediante la Decisión 2010/87/UE de la Comisión[8]-, aprobó sendos modelos que contienen cláusulas contractuales tipo para facilitar la transferencia de datos personales por parte de un Responsable establecido en la UE a otro Responsable o Encargado establecido en un tercer país que no ofreciera un nivel de protección adecuado.

Las cláusulas contractuales tipo de las Decisiones mencionadas fueron actualizadas en junio de 2021 para adaptarlas al RGPD luego de su discusión pública[9]. La nueva decisión[10] aprueba un modelo más completo dado el tiempo transcurrido.

---

[5] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DO L 119 de 4.5.2016, p. 1. DIsponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

[7] Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2001%3A181%3ATOC

[8] Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

[9] Estas nuevas cláusulas contractuales recibieron comentarios, aportes y sugerencias de toda la comunidad internacional y constituyen un texto que refleja los estándares más importantes a nivel internacionales incluidos los últimos desarrollos jurisprudenciales en la materia.

[10] DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Es del caso mencionar también el "Acuerdo sobre comercio electrónico del MERCOSUR"[11] (vinculante para la República Argentina, la República Federativa del Brasil, la República del Paraguay y la República Oriental del Uruguay) firmado el 28 de enero de 2021.

El art. 6.2 del citado Acuerdo dispone que las partes deberán adoptar o mantener leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico. A tales efectos tomarán en consideración los estándares internacionales que existen en esta materia.

Asimismo, por el art. 6.7 del Acuerdo se dispone que las partes se comprometen a aplicar a los datos personales que reciban de otra Parte un nivel de protección adecuado mediante una norma general o regulación específica autónoma o por acuerdos mutuos, generales o específicos, o en marcos internacionales más amplios, admitiéndose para el sector privado **la implementación de contratos** o autorregulación.

El art. 7 de la normativa del Mercosur establece el principio de no discriminación en materia de transferencias internacionales de datos personales.

El 9 de abril de 2021, el CJI de la OEA aprobó los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales[12].

El Principio n. 11 se refiere al Flujo Transfronterizo de Datos y dispone así: "Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios".

Por otra parte el Convenio n. 108 del Consejo de Europa con las modificaciones del Protocolo del 2001[13] dispone en su art. 2 titulado "Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio" dispone que "Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección".

[11] Ver MERCOSUR/CMC/DEC. Nº 15/20, Disponible en https://normas.mercosur.int/public/normativas/4018 y https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf

[12] OEA, Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con Anotaciones (CJI/RES. 266 (XCVIII-O/21)). http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Trabajos_Actuales_CJI.asp

[13] Disponible en https://rm.coe.int/1680080626

Por su parte el art. 2.2 dispone que "No será de aplicación el párrafo 1 del Artículo 2 del presente Protocolo, pudiendo las Partes autorizar la transferencia de datos personales: … b) si se prevén las suficientes garantías, que pueden resultar, en particular, **de cláusulas contractuales**, por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno".

3.2. Red Iberoamericana de Protección de Datos

La RIPD se ha preocupado por la regulación legal de las TIDP desde sus orígenes. Así, en el marco del III Encuentro Iberoamericano de Protección de Datos celebrado en Cartagena de Indias (Colombia) en el año 2004[14] los miembros de la RIPD emitieron diversas conclusiones donde se evidenciaba su preocupación por las TIPD.

En ese encuentro los miembros de la RIPD concluyeron que "*La transferencia internacional de datos personales debe estar sometida a un régimen de garantías para impedir que los principios que rigen el derecho fundamental a la protección de datos se vean vulnerados por el mero traslado de dichos datos a otro país. La Directiva de Protección de Datos de la Unión Europea ha consagrado este principio y ha otorgado a la Comisión Europea competencias para decidir que un país que ha establecido una legislación de protección de datos acorde con los estándares europeos y ha creado una autoridad de control independiente es un destino seguro para los datos personales provenientes de Estados miembros de la UE*".

En el mismo documento los miembros de la RIPD aclararon que "*En el caso que no exista este reconocimiento, es posible, entre otras opciones, **la utilización de las cláusulas contractuales tipo** […] Su utilización permite establecer las garantías necesarias que suplan la carencia de una legislación adecuada en el país de destino al otorgar a los titulares cuyos datos se transfieren la posibilidad de exigir el cumplimiento de las cláusulas del contrato que les afectan así como una reparación en el caso de que se les causen perjuicios por no respetarse*".

La Declaración de Cartagena de Indias concluye señalando que "*Por lo tanto, los participantes en el III Encuentro Iberoamericano de Protección de Datos hacen votos para que en los países iberoamericanos se promulguen regulaciones sobre protección de datos y se establezcan mecanismos de control independientes que promuevan una efectiva implantación del derecho fundamental a la protección de datos personales que, al mismo tiempo, faciliten el libre flujo de datos personales entre los países*".

[14] RIPD, Declaración de Cartagena de Indias, mayo de 2004, punto III - "Las transferencias internacionales de datos. Perspectivas europeas e iberoamericanas" en https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

En el marco del XVIII Encuentro Iberoamericano de Protección de Datos[15] celebrado en modalidad en línea el 4 de diciembre de 2020 en Montevideo (Uruguay), los miembros de la RIPD establecieron en su Declaración Final (conclusión punto 7) que: "*[…] el tratamiento de datos personales como impulsor de la economía mundial requiere* ***reglas claras y transparentes que permitan flujos internacionales de datos seguros****, basados en la consideración del nivel de protección que brindan los países u organizaciones destinatarias de dichos flujos, en tratados internacionales, o en normas contractuales entre emisor y receptor que garanticen la vigencia de los principios en protección de datos, el ejercicio de los derechos por parte de los titulares, y el cumplimiento de las obligaciones correspondientes a responsables, encargados de tratamiento y otros terceros*".

En conclusión, resulta natural que en el desarrollo de documentos adicionales a los Estándares y a la Declaraciones de la RIPD se busque elaborar guías y modelos que faciliten el libre flujo de datos, pero manteniendo una protección adecuada de los datos personales de los titulares tales como las cláusulas contractuales modelo o los códigos corporativos vinculantes.

En el año 2017 los miembros de la RIPD aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Los Estándares Iberoamericanos buscan establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región. Por otra parte, los Estándares Iberoamericanos incluyen las mejores prácticas nacionales e internacionales en la materia al momento de su dictado. Entre los objetivos de los Estándares Iberoamericanos se encuentran los siguientes que de alguna forma justifican adoptar cláusulas contractuales modelo para la región: (i) *facilitar el flujo* de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región y (ii) favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

El art. 36 inc. 1, letra "c" de los Estándares dispone que "*El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos: … c. El exportador y destinatario* ***suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes*** *y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados Iberoamericanos aplicable en la materia*".

De los Estándares Iberoamericanos surge lo siguiente:

- El Exportador y el Importador pueden suscribir cláusulas contractuales.

[15] RIPD, XVIII Encuentro Iberoamericano de Protección de Datos, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

- Estas cláusulas contractuales deben ofrecer garantías suficientes, que permitan demostrar: (i) el alcance del tratamiento de los datos personales, (ii) las obligaciones y responsabilidades asumidas por las partes y (iii) los derechos de los Titulares.
- La autoridad de control respectiva podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados Iberoamericanos aplicable en la materia.

3.3. Normativa Iberoamericana sobre TIDP

En consonancia con la normativa internacional antes citada y con los Estándares, gran parte de los países iberoamericanos regulan la transferencia internacional de datos personales, en ausencia de una continuidad en el nivel de protección.

Este es el caso de los siguientes países:

- Argentina (art. 12 ley n. 25.326 de protección de datos personales, art. 12 del decreto reglamentario n. 1558/2001 y Disposición 60).
- Brasil (arts. 33 a 35 de la LGPD).
- Cabo Verde (art. 20, Ley nº 41/VIII/2013, de 17 de septiembre, de Protección de Datos Personales de las Personas Físicas).
- Colombia (Art. 26 de la Ley 1581 de 2012).
- Ecuador (arts. 55 a 61 de la Ley Orgánica de Protección de Datos Personales).
- México (arts. artículos 65-70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).
- Nicaragua (art.14 de la Ley nº 787, Ley de Protección de Datos Personales).
- Panamá (arts. 5 y 33, Ley nº 81, de 26 de marzo de 2019, sobre Protección de Datos Personales).
- Perú (art. 15 de la ley 29.733).
- República Democrática de Santo Tomé y Príncipe (arts. 19 y 20, Ley 3/2016, de 2 de mayo de Protección de Datos Personales de las Personas Físicas).
- República Dominicana (art. 80 de la Ley Nº 172-13, de 13 de diciembre de 2013, sobre Protección de Datos de Carácter Personal).
- Uruguay (art. 23 de la Ley N° 18.331 de Protección de Datos Personales, Resolución N° 4/019, de 12 de marzo de 2019 y Resolución N° 41/021, de 8 de setiembre de 2021).

Además de estas limitaciones a transferencia internacional a destinos que no garanticen una protección adecuada, la mayor parte de las legislaciones también establecen ciertas excepciones para permitir las TIDP a esos destinos (cuando existen por ejemplo tratados internacionales). Por otra parte, es también posible recurrir a otras herramientas para la transferencia internacional.

Por ejemplo, Argentina, Colombia[16], México[17], Panamá, Perú y Uruguay contemplan o recomiendan la posibilidad de usar CCM.

Por su parte algunas autoridades de protección de datos como es el caso de Uruguay y de Argentina, han emitido normas donde aprueban directrices o modelos de CCM[18].

4. Principales actores en las TIDP

A continuación, se presentan los principales actores involucrados en las TIDP. Esto ayuda a comprender el interés de cada parte en una TIDP.

Las TIDP tienen lugar en una gran cantidad de situaciones como: transferencias bancarias, reservas de pasajes aéreos y de hoteles, servicios de computación en la nube, centralización de recursos humanos, operaciones de comercio exterior tradicionales y de comercio electrónico, captación de datos mediante aplicaciones, recolección internacional de datos, entre muchos otros casos.

En el escenario típico de una TIDP (cualquier sea el motivo de la misma) tenemos los siguientes elementos y actores:

- Una entidad que desea enviar datos al exterior denominada **Exportador de datos**.
- Una entidad que desea recibir esos datos denominada **Importador de datos**, localizada en otra jurisdicción.
- El Importador recibe los datos para tratarlos con una determinada finalidad. Pero la TIDP es por sí un procesamiento de datos: se parte de la base de que toda transferencia internacional de datos personales implica un tratamiento de datos según la definición dada por los Estándares[19].

[16] Colombia: En su nueva versión del año 2021 la Guía emitida por la autoridad colombiana de protección de datos personales se dan lineamientos sobre la TIDP y el uso de CCM. Ver Colombia, SIC, Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales, pág. 17 donde se recomienda el uso de cláusulas contractuales para las TIDP como forma de demostrar accountability por parte del Encargado del tratamiento de datos personales. Disponible en https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf

[17] México, Artículo 75 del Reglamento de la LFPDPPP, sugiere las cláusulas contractuales, al disponer “A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales”.

[18] Uruguay: Resolución N° 41/021, de 8 de setiembre de 2021. Disponible en https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay y Argentina: Disposición 60/2016 de la Dirección Nacional de Protección de Datos Personales. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

[19] Cfr. literal i del art. 2 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017).

- Los datos personales transferidos pertenecen al **Titular del dato personal** que es la "persona física a quien le conciernen los datos personales"[20] cuya información debe ser tratada debidamente. Todos los derechos del Titular deben garantizarse cuando el tratamiento se efectúe mediante una transferencia internacional de datos personales a una jurisdicción caracterizada como no adecuada. En el caso de los Estándares Iberoamericanos los derechos a garantizar se encuentran mencionados en los artículos 24 a 32. Una forma de garantizar estos derechos es a través del uso de CCM.
- A su vez el Titular es un **Tercero Beneficiario** en las CCM. Esto significa que el Titular tiene derechos que derivan no sólo de la ley de protección de datos personales de la jurisdicción del Exportador, sino también del propio contrato de transferencia internacional firmado entre las partes (ver punto 7 de esta Guía).
- Una **jurisdicción no adecuada** donde está localizado el Importador de datos. Esta jurisdicción es caracterizada como no adecuada a los fines de la TIDP según la normativa del país del Exportador de datos o la interpretación de la Autoridad competente. La falta de adecuación de la jurisdicción de destino obliga a las partes a adoptar resguardos para proteger los datos objeto de la TIDP, por ejemplo, a través de la firma de CCM.
- **Autoridad de protección de datos**. La Autoridad de protección de datos (Autoridad de Control)[21] debe vigilar que quienes realizan transferencias internacionales de datos personales realicen dicha actividad observando lo que dispone la regulación sobre dicho tema.
- **Ley aplicable**: 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 estos deben ser exportados o transferidos a otro u otros países[22]. Como consecuencia de la necesidad de tutelar los datos personales transferidos a una jurisdicción no adecuada, es necesario que los mismos queden sujetos a una protección similar a la existente al momento de su recolección.

Veamos un ejemplo con el escenario del tratamiento de datos mediante servicios de computación en la nube según las guías aprobadas por la RIPD sobre el tema.

En el mes de abril del año 2020 la RIPD publicó las "Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube"[23]. En este documento la RIPD concluyó que el procesamiento de datos personales en la nube puede implicar la transferencia

[20] Cfr. Literal h) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017).
[21] En el capítulo VII de los Estándares se establecen los principales aspectos sobre las autoridades de control y supervisión en materia de protección de datos.
[22] Ver RIPD, Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube. Disponible en https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf
[23] Ver RIPD, Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube. Disponible en https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

internacional de datos personales[24]. Las recomendaciones contienen sugerencias para que los proveedores de servicios de computación en la nube (PSCEN) puedan prestar sus servicios respetando las reglas de datos personales de los Titulares.

En sus Recomendaciones, la RIPD señala lo siguiente: "Si los "data center" o los equipos de almacenamiento de los PSCEN están ubicados fuera del país en donde se encuentra el contratante de los servicios de CEN, los datos personales serán remitidos o exportados desde un país a empresas y organizaciones PSCEN ubicadas en un territorio diferente al del país de envío. Se trata de un proceso de exportación de datos personales".

Luego de esta explicación el documento precisa: "*En este caso, la empresa contratante de los servicios de CEN será el Exportador y el PSCEN obrará como el destinatario de dicha exportación de datos. Los Estándares definen al Exportador como la "persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares". Así las cosas, el contratante de los servicios de CEN debe observar las reglas locales de la transferencia internacional de datos*".

Las citadas Recomendaciones de la RIPD concluyen que "*Es importante que el contratante de los servicios de CEN sea plenamente consciente y en su caso, pueda aceptar o limitar, los países en los que van a estar alojados los servidores, además de estar informado de las garantías adecuadas que se adopten*".

Todo esto se explica con el fundamento de las TIDP: "*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 estos deben ser exportados o transferidos 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. La exportación de información personal no puede 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. En ese sentido, se deben cumplir las reglas de transferencias internacionales que rigen en el país del contratante de los servicios de CEN. En el caso de los Estándares, en el artículo 36 se prevén las alternativas permitidas para exportar los datos*".

En el caso concreto analizado, la empresa contratante de los servicios de CEN será el Exportador y el PSCEN será el Importador de Datos. Ambas partes podrían firmar un contrato basado en las CCM donde el Importador actúa como Encargado usando el modelo respectivo de CCM.

[24] RIPD, Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube, p. 15.

5. Regla general en las TIPD. Excepciones y mecanismos de transferencia más usados

5.1. Regla general

Las disposiciones sobre TIDP que se encuentran en las leyes de protección de datos de los países iberoamericanos tienen como finalidad garantizar la continuidad del nivel de protección provisto en sus leyes cuando se produce una transferencia de datos personales a un tercer país que se considere no adecuado o que tenga un nivel distinto de protección de datos personales.

Los países pueden reconocer a otras jurisdicciones como “adecuadas” a su legislación de datos personales. En virtud del principio general de prohibición de TIDP, a falta de una decisión de adecuación o referencia específica en el país exportador de datos, el Responsable o el Encargado solo pueden transferir datos personales a un tercer país si se han ofrecido garantías adecuadas y a condición de que los Titulares cuenten con derechos exigibles y acciones judiciales eficaces para tutelar sus derechos. Dichas garantías pueden aportarse, entre otros medios, por normas corporativas vinculantes (NCV) o por CCM.

En términos generales, se considera que un país es adecuado cuando tiene ciertos elementos en su sistema jurídico que permita concluir que los datos personales son amparados adecuadamente. Los siguientes elementos suelen ser evaluados para determinar el nivel de adecuación:

- El “Estado de Derecho”, el respeto de los derechos humanos y los derechos fundamentales en ese sistema jurídico.
- La legislación vigente tanto general como sectorial sobre datos personales.
- las medidas de seguridad aplicadas,
- Las normas sobre Transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país.
- Derechos reconocidos a los titulares de datos personales mediante recursos administrativos y acciones judiciales que sean efectivos.
- La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país.
- Los compromisos internacionales asumidos por el tercer país u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.
- El acceso de las autoridades públicas del país de destino a los datos transferidos y en forma mas general, el régimen de excepciones que pueda existir en ese país de destino a las reglas de protección de datos personales.

5.2. Excepciones

Los Estándares disponen en el art. 36.2 que la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

Numerosas normas contienen excepciones a la regla que prohíbe la TIDP a países o jurisdicciones no adecuadas. Las normas de jurisdicciones iberoamericanas que se han mencionado en el punto 3.3 de esta Guía contienen excepciones individuales basadas en estos principios mencionados en los Estándares.

Un punto importante a tener en cuenta es que estas excepciones a las TIDP no pueden aplicarse en forma continua para todo tipo de transferencias, sino que, debido a su naturaleza excepcional, se deben destinar para una transferencia específica y concreta.

5.3. Mecanismos de transferencia

Si el país de destino de la TIDP no es adecuado, y si no se aplica ninguna de las excepciones previstas, entonces la TIDP se pueden realizar mediante un mecanismo de transferencia que otorgue garantías adecuadas.

Los mecanismos de TIPD que otorgan garantías adecuadas suelen ser los siguientes:

- Cláusulas contractuales modelo (CCM).
- Normas corporativas vinculantes (NCV).
- Código de conducta aprobado con arreglo a la ley aplicable.
- Mecanismo de certificación.
- Instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos.

La función de las cláusulas contractuales tipo es asegurar que haya garantías suficientes de protección de datos en las transferencias internacionales de datos a jurisdicciones no adecuadas. El Responsable o el Encargado que transfiera los datos personales a un tercer país (Exportador de datos) y el Responsable o Encargado que reciba los datos personales (Importador de datos) pueden firmar un acuerdo con el fin de garantizar los derechos de los titulares a través de las CCM.

Si bien las CCM deberán emplearse en principio para las transferencias a jurisdicciones no adecuadas la RIPD exhorta su aplicación a todo tipo de transferencia internacional, en lo pertinente para asegurar el cumplimiento de los principios de protección de datos personales.

Finalmente, resulta importa señalar que el uso de CCM no implica en todos los casos el cumplimiento total de la legislación o normatividad en protección de datos personales de los Estados miembro, por lo cual, habría de estarse a los requerimientos relativos[25].

6. Las CCM como mecanismo de resguardo de las TIDP

6.1. Finalidad de las CCM

La finalidad de las cláusulas contractuales modelo es garantizar y facilitar el cumplimiento de los requisitos previstos por la ley de protección de datos del país del Exportador para la transferencia de datos personales a un tercer país no adecuado. La idea es que la protección inicialmente otorgada a los datos personales siga presente con independencia del lugar donde estos datos se encuentren.

Es por eso que también se regulan las Transferencias ulteriores con recaudos para evitar la disminución del nivel de protección. Se da intervención a los Titulares a través de un concepto universal del derecho de los contratos denominado Tercero beneficiario. Y se regula el acceso por parte de autoridades públicas en la jurisdicción del Importador que puedan afectar derechos del Titular.

6.2. Ventajas y beneficios de las CCM

El uso de cláusulas contractuales modelo puede ayudar a superar cualquier limitación a la transferencia de datos que se derive de las diferencias existentes en el nivel de protección entre los diferentes países. El instituto del contrato está presente en todos los ordenamientos jurídicos iberoamericanos y sirve para comprometer al Importador a respetar los datos personales del Titular una vez que los datos personales están en la jurisdicción de destino.

En otras palabras: las cláusulas modelo o cláusulas tipo contribuyen a construir la convergencia a nivel contractual, creando un régimen de protección de datos autónomo, sin necesariamente requerir convergencia a nivel de país (en esto, pueden ir más allá del nivel de protección en ciertos países).

Al mismo tiempo, la expansión de principios de protección de datos personales a través de redes de contratos internacionales tiene un fuerte impacto en la convergencia general en la región, ya

[25] Por ejemplo, en el caso del sector público de México, cuando se lleven a cabo transferencias de datos personales que o cuenten con un nivel de protección adecuado, deberán presentarse previamente una Evaluación de impacto en la protección de datos personales.

que establecen estándares comunes con los que las empresas se familiarizan. Esto facilita en el futuro la alineación de la legislación nacional con las normas y estándares internacionales de protección de datos personales.

Por otra parte, el uso de CCM sirve para garantizar los principios y deberes en la protección de datos personales. Esto a su vez lleva a la transparencia, la seguridad jurídica y, por tanto, la previsibilidad ya que:
(i) a través de su naturaleza vinculante y exigible como parte de un contrato, pueden garantizar la continuidad de la protección cuando los datos viajan al extranjero, y hacerlo de una manera que brinde seguridad jurídica;
(ii) al hacerlo de manera clara y transparente, ayudan a generar confianza, lo que a su vez brinda a las empresas que utilizan tales cláusulas una ventaja competitiva respecto a aquellas que tienen que recurrir a otros métodos.

Las CCM sirven para proteger a la parte "más débil" que por supuesto son las personas físicas cuyos datos personales en el marco de las TIDP son procesados tanto por el Exportador como por el Importador.

Por último, el uso de las CCM permite también una solución particularmente económica al problema de las TIDP: el motivo es que las empresas no tienen que negociar acuerdos en cada caso individual con el coste económico que ello implica en representación legal y en tiempo. La existencia de las CCM les permite confiar en el modelo pre-aprobado por la Autoridad competente, sabiendo que al hacerlo cumplen con sus obligaciones legales en materia de cesión internacional de datos personales con una solución sencilla y práctica. Esta es una gran diferencia con otras herramientas como, por ejemplo, los mecanismos de certificación o las NCV, que requieren un proceso de certificación a menudo largo y costoso.

En comparación con esos mecanismos, las CCM son un instrumento "listo para usar" y "listo para ejecutar". Esto es particularmente importante para las pequeñas y medianas empresas que no pueden permitirse otras opciones más costosas y que requieren más tiempo de implementación.

Es por ello que las CCM son el mecanismo legal más accesible y utilizado hoy en día para la TIDP a jurisdicciones no adecuadas. Se calcula que cerca del 80 al 90% de empresas que implementan mecanismos de TIDP utilizan como solución a las CCM[26]. Por supuesto esto implica que las Partes de una TIDP que usan una CCM no deben limitarse al requisito formal de su firma, sino que siempre deben estar preparadas para “rendir cuentas” del tratamiento que realicen de los datos personales a la Autoridad de control competente y a los Titulares y poder demostrar el acabado cumplimiento de la ley aplicable y de las obligaciones impuestas en las CCM.

[26] Un estudio realizado calcula que cerca del 85% usa como mecanismos de TIDP a las CCM. Ver Nigel Cory, Ellysse Dick, Daniel Castro, The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade, ITIF, December 17, 2020. Disponible en https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade . En igual sentido: Laura Bradford, Mateo Aboy, Kathleen Liddell, Standard contractual clauses for cross-border transfers of health data after Schrems II, publicado en Journal of Law and the Biosciences, Volume 8, Issue 1, January-June 2021, https://doi.org/10.1093/jlb/lsab007.

7.Cuestiones prácticas en la implementación y ejecución de las CCM

7.1. Aspectos generales

Dada la multiplicidad de leyes existentes en Iberoamérica, esta Guía se basa en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados en el XV Encuentro de esta Red, realizado en Santiago de Chile, Chile el 22 de junio de 2017. También se han tenido en cuenta los trabajos realizados con el Comité Jurídico Interamericano de la Organización de Estados Americanos para la modernización de los principios en privacidad elaborados por la citada organización, así como el RGPD y el Convenio 108 modernizado.

Las definiciones de las CCM están tomadas de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Lo mismo puede decirse de las obligaciones sustantivas que dimanan de las CCM. Asimismo, se han consultado las cláusulas contractuales modelo aprobadas por la UE, así como los modelos propuestos por las autoridades de Nueva Zelanda y la propuesta del Reino Unido.

A continuación, se indica las fuentes en las que se basan las cláusulas de las CCM:

Cláusula	Fuente
Cláusula 1.4 - Definiciones de las CCM	Art. 2 de los Estándares. La definición de anonimización se basa en el art. 4.3.b de los Estándares. Las definiciones de Importador de datos, de Transferencia Ulterior, de Ley Aplicable y del Tercero beneficiario no están en los Estándares iberoamericanos. Se elaboró con base del contenido de las cláusulas modelo.
Cláusula 6.1 - Principio de responsabilidad	Artículo 20 de los Estándares iberoamericanos
Cláusula 6.2 - Principio de finalidad	Artículo 17 de los Estándares iberoamericanos
Cláusula 6.3 - Principio de Transparencia	Artículo 19 de los Estándares iberoamericanos
Cláusula 6.6 y 6.7 Principios de seguridad y confidencialidad	Artículos 21, 22 y 23 de los Estándares iberoamericanos
Cláusula 6.9 - Transferencias ulteriores	Clausula 8.7 de las clausulas contractuales modelo de la UE
Cláusula 7 – Derechos del Titular	Artículos 24 a 28 de los Estándares iberoamericanos
Derecho a la indemnización	Artículo 44 de los Estándares iberoamericanos

Cláusula de acceso por parte de autoridades publicas	Cláusula contractual modelo de Nueva Zelanda
Cláusula 6.1. del modelo Responsable-Encargado	Artículo 34 de los Estándares iberoamericanos

En consecuencia, como un primer paso recomendable para la adopción de las CCM, se sugiere confrontar los requerimientos establecidos en los Estándares Iberoamericanos con la normativa de cada Estado Miembro, ya que en caso de que esta última prevea requisitos adicionales deberán incluirse previsiones complementarias en las CCM.

7.2. Características de las CCM. Forma de uso.

Los dos modelos de las CCM incluidas en el Anexo de esta Guía se caracterizan por lo siguiente:

- La CCM del Anexo contiene dos modelos para los distintos supuestos de TIDP de: i) Responsable a Responsable y ii) de Responsable a Encargado.
- Se incluye una primera hoja o carátula donde se insertan todos los datos de las partes y del contrato y sus domicilios. La idea es que no sea necesario modificar para nada el texto del contrato modelo.
- Las CCM tienen varios anexos para identificar a las nuevas partes que se suman al contrato con posterioridad a su firma inicial por Importador y Exportador (Anexo A), los datos personales involucrados en las transferencias y sus finalidades (Anexo B) las medidas de seguridad (Anexo C) y el listado de sub encargados del tratamiento para el caso del segundo modelo (Anexo D).
- Respecto al Anexo A, cada Parte nueva que se incorpora a las CCM debe firmar por separado un Anexo e indicar el tipo de actividad que realizará respecto a las TIDP.
- Respecto al anexo B, se debe poder distinguir claramente la información aplicable a cada transferencia o categoría de transferencias.
- Respecto al anexo C, se deben detallar las medidas de seguridad en forma precisa. No es posible incluir generalidades.
- Respecto al anexo D, se debe mencionar a los sub encargados para el caso que se haya optado por listarlos en forma previa.

Adicionalmente, se considera importante señalar que para el uso de las CCM deberán verificarse previamente los requisitos de la transferencia en el caso concreto, y, las características de las entidades o personas que las realizan, puesto que eventualmente las CCM podrían incorporar elementos adicionales dependiendo de dichos supuestos y los requerimientos regulatorios aplicables en cada uno de los países donde se lleve a cabo dicho tratamiento.

Así mismo, resulta importante señalar que las CCM están previstas para ser adoptadas como como parte o sección específica de un tratado, convenio, acuerdo o equivalente, o en su defecto como anexo de la cláusula relativa, por lo que en caso, de que se desarrollen específicamente estas cláusulas para acreditar una transferencia las CCM deberán adaptarse conforme a los requerimientos regulatorios respectivos y la formalidad del documento de referencia.

7.3. Posición de las partes. Incorporaciones de nuevas partes y uso del CCM con otros acuerdos. Modificaciones.

Si bien usualmente se hace alusión a cláusulas contractuales tipo o cláusulas contractuales modelo, el término se refiere a un modelo completo de contrato que puede ser usado como está o modificado en aspectos secundarios en tanto no se altere su esencia que es la protección del Titular. Es posible entonces agregar estas CCM como anexo a un contrato que las partes vayan a firmar o hayan firmado, pero luego deberán ejecutar dichos modelos en forma efectiva para que sean válidos y tengan efecto.

Las Partes tienen discrecionalidad para incluir en un contrato más amplio dichas cláusulas contractuales tipo, así como para añadir otras cláusulas o garantías adicionales siempre que no contradigan, alteren o modifiquen, directa o indirectamente, las cláusulas contractuales tipo ni perjudiquen los derechos fundamentales de los Titulares.

7.4. Ley aplicable a las TIDP

La implementación de las CCM tiene lugar cuando una entidad debe transferir datos a otra entidad que está localizada en otro país que no es adecuado. Las cláusulas contractuales tipo pueden utilizarse respecto de tales transferencias en la medida en que el Importador esté en un país tercero distinto al del Exportador.

En una situación normal, cada parte estaría sujeta en el procesamiento que hacen de los datos personales transferidos a las leyes de su respectivo país. Sin embargo, en materia de TIPD mediante CCM, la ley que resulta aplicable (definida en la CCM como “Ley aplicable”) es la ley del país o jurisdicción del Exportador.

La exportación de información personal no puede 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. Las TIDP no deben facilitar ni permitir la vulneración de los derechos de los Titulares ni la disminución de las garantías con que cuentan los Titulares en el país exportador[27]. Esto se basa en la lógica que los datos son recopilados y procesados bajo la ley del Exportador y cuando

[27] RIPD, Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube, p. 15.

son transferidos al exterior a un país que no es adecuado, resulta necesario preservar el nivel de tutela que los datos personales tienen en el país de origen.

7.5. Cumplimiento de las normas generales de protección de datos personales

Además de utilizar CCM para ofrecer garantías adecuadas en las transferencias internacionales de datos personales, el Exportador de datos tiene que cumplir las obligaciones generales que le incumben como Responsable o Encargado en virtud de la ley de protección de datos personales vigente en su jurisdicción.

Entre estas responsabilidades figuran la obligación del responsable de comunicar con claridad a los interesados en su política de privacidad la existencia de transferencias internacionales de sus datos personales a un tercer país que no es adecuado.

7.6. Transferencias ulteriores

Si el Importador necesita transferir los Datos personales a otra entidad luego de recibir los datos del Exportador (sea ese lugar de destino adecuado o no) entonces se produce una Transferencia ulterior y resulta necesario continuar amparando los datos personales.

Las Transferencias ulteriores por parte del Importador de datos a un tercero en otro tercer país solo deben permitirse si dicho tercero se adhiere a las CCM de similar tenor y si la continuidad de la protección está garantizada de otro modo o en situaciones específicas contempladas en las CCM.

7.7. Terceros beneficiarios

En las CCM el Titular es un Tercero beneficiario del contrato modelo firmado por las Partes. En caso de incumplimiento de los deberes contractuales por parte del Importador, el Titular puede en su carácter de tercero beneficiario reclamar al Importador o al Exportador por dicho incumplimiento. Ello es así porque ambas Partes realizan una estipulación a favor del Titular[28].

El principio del Tercero beneficiario está contemplado en la mayoría de los códigos de derecho privado de Iberoamérica. Así, entre otros, la encontramos en los códigos civiles de Argentina (art. 1027 del CCN), Bolivia (arts. 526 a 529 del código civil), Brasil (arts. 436 a 438 del Código Civil), Chile (arts. Art. 1449 Código Civil), Colombia (art. 1506 del Código civil), Costa Rica (art. 1026 del Código Civil de Costa Rica), Ecuador (art. 1465 Código Civil), El Salvador (art. 1320 Código

[28] La estipulación o contrato a favor de tercero es un acuerdo por el cual un sujeto (denominado promitente) se obliga frente a otro (el llamado estipulante) a darle algo a un tercero (o beneficiario) o a hacer o no hacer algo a favor de dicho tercero, quien, aunque ajeno a este contrato, adquiere por el mismo los derechos allí mencionados.

Civil), Guatemala (artículo 1531 Código Civil), Honduras (artículo 740 Código de Comercio), México (artículos 1868-1871 del Código Civil Federal), Nicaragua (artículo 1875 Código Civil), Paraguay (art.732 del Código Civil), Perú (artículos 1457-1459 del Código Civil) y Uruguay (art. 1256 del Código Civil).

7.8. Responsabilidad demostrada

El art. 20 de los Estándares[29] establece el principio de responsabilidad demostrada. La norma dispone que el responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

El Importador implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en las CCM, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al Titular y a la Autoridad de Control competente, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Entre los mecanismos que una de las partes del contrato podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:
a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del Importador.
d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.
e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

Lo anterior, aplicará cuando los datos personales sean tratados por parte de un Encargado a nombre y por cuenta del Responsable, así como al momento de realizar TIDP. La norma citada

[29] Artículo 20 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017).

luego enumera una serie de mecanismos que tanto el Responsable como el Encargado, según el caso, deben implementar. Este principio de responsabilidad demostrada (accountability) se aplica también a las transferencias internacionales de datos personales.

En igual sentido, las CCM establecen que las partes deben poder demostrar el cumplimiento de las cláusulas contractuales tipo. En particular, las CCM requieren al importador de datos que conserve la documentación que corresponda para las actividades de tratamiento bajo su responsabilidad y que informe al Exportador de datos en caso de que, por cualquier motivo, no pueda cumplir las cláusulas.

7.9. Imposibilidad de cumplimiento del Importador

El Importador de datos debe informar al Exportador de datos si, tras haber suscripto las CCM, tiene motivos para creer que no podrá cumplir las cláusulas contractuales tipo. Si el Exportador de datos recibe tal comunicación o descubre de otro modo que el Importador de datos ya no puede cumplir las cláusulas contractuales tipo, debe determinar las medidas adecuadas para hacer frente a la situación, consultando, en su caso, a la autoridad de control competente.

Dichas medidas pueden consistir en medidas complementarias adoptadas por el Exportador y/o el Importador de datos, como medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad. También podrá exigir al Exportador de datos que suspenda la transferencia si considera que no hay garantías adecuadas o si así lo dispone la Autoridad de control competente. Esta facultad está expresamente prevista en las CCM.

***

Glosario de la Guía

Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona física sin esfuerzos desproporcionados.

Autoridad de control competente: Autoridad de protección de datos personales del país del Exportador o del Importador de datos personales.

Computación en la nube: modelo para habilitar el acceso a un conjunto de servicios computacionales (e.g. Redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio.

Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

Datos Personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Decisiones individuales automatizadas: Decisiones que produzcan efectos jurídicos al Titular o le afecten de manera significativa y que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Encargado: prestador de servicios que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del Responsable, trata datos personales a nombre y por cuenta de éste.

Estándares: Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017.

Exportador de datos: persona física o jurídica de carácter privado, autoridad pública, prestador de servicios u organismo situado en el territorio de un país que efectúe transferencias internacionales de datos personales a otro país.

Importador de datos: persona física o jurídica de carácter privado, autoridad pública, prestador de servicios u organismo situado en un tercer país que recibe datos personales de un Exportador de datos mediante una transferencia internacional de datos personales.

Ley Aplicable: es la ley de protección de datos personales de la jurisdicción del Exportador de datos.

Medidas administrativas, físicas y técnicas: medidas destinadas a evitar el daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los Datos personales aun cuando ocurra de manera accidental, suficientes para garantizar la confidencialidad, integridad y disponibilidad de los Datos personales.

Responsable: persona física o jurídica de carácter privado, autoridad pública, prestador de servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

Terceros beneficiarios: Titular cuyos datos personales son objeto de una transferencia internacional en virtud del presente Acuerdo. El Titular es un tercero beneficiario de los derechos dispuestos en su favor en las CCM y por ende puede ejercer los derechos que las CCM le reconoce, aunque no haya suscripto el contrato modelo entre las partes.

Titular: persona física a quien le conciernen los datos personales.

Transferencia ulterior: Transferencia de datos realizada por el Importador de datos a un tercero situados fuera de la jurisdicción del Importador y del Exportador de datos que cumple las garantías establecidas en las CCM.

Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Vulneración de la seguridad de datos personales: cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental.

Siglas utilizadas

APD	Autoridad de Protección de Datos o Autoridad de Control.
Estándares	Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017.
CEN	Computación en la nube.
CIJ	Comité Jurídico Interamericano.
CCM	Cláusulas contractuales modelo.
OEA	Organización de estados americanos.
NCV	Normas corporativas vinculantes.
RGPD	Reglamento General de Protección de Datos o RGPD REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
RIPD	Red Iberoamericana de Protección de Datos.
PSCEN	Proveedor de servicios de computación en la nube.
TDP	Tratamiento de datos personales.
TIDP	Transferencia internacional de datos personales.
UE	Unión Europea.

Documentos consultados

Red Iberoamericana de Protección de Datos

Red Iberoamericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Disponibles en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

RIPD, Declaración de Cartagena de Indias, mayo de 2004, punto III - “Las transferencias internacionales de datos. Perspectivas europeas e iberoamericanas” en https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

RIPD, XVIII Encuentro Iberoamericano de Protección de Datos, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

Unión Europea

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DO L 119 de 4.5.2016, p. 1. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la

Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países de conformidad con la Directiva 95/46/CE del Parlamento

Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Sentencia del Tribunal de Justicia de la UE, sentencia del 16 de julio de 2020 en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems ("Schrems II"), ECLI:EU:C:2020:559.

EDPB
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020. Disponible en https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Mercosur
MERCOSUR/CMC/DEC. Nº 15/20, Disponible en https://normas.mercosur.int/public/normativas/4018 y https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf

Organización de Estados Americanos
OEA, Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con Anotaciones (CJI/RES. 266 (XCVIII-O/21)).

http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Trabajos_Actuales_CJI.asp
Disponible en https://rm.coe.int/1680080626

Argentina
Ley 25.326, Art. 12 ley n. 25.326 de protección de datos personales, art. 12 del decreto reglamentario n. 1558/2001
Disposición 60/2016 de la Dirección Nacional de Protección de Datos Personales. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

Brasil
Arts. 33 a 35 de la LGPD.

Cabo Verde
Art. 20, Ley nº 41/VIII/2013, de 17 de septiembre, de Protección de Datos Personales de las Personas Físicas.

Colombia
Art. 26 de la Ley Estatutaria 1581 de 2012.
Art 25 del Decreto 1377 de 2013 (Contrato de transmisión de datos personales)

SIC, Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales
Disponible en
https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf
SIC, Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)
Disponible en
https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Ecuador
Arts. 55 a 61 de la Ley Orgánica de Protección de Datos Personales.

México
Arts. 36 y 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicada en el Diario Oficial de la Federación el 5 de julio de 2010 disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el siguiente vínculo electrónico: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.).
Arts. 67 al 76 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011, disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011; sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por la Cámara de Diputados del H. Congreso de la Unión, disponible en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf; enlaces consultados por última vez el 06/10/2021).
Arts. 65 al 71 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados(Publicada en el Diario Oficial de la Federación el 26 de enero de 2017, disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017 , sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la

Cámara de Diputados del H. Congreso de la Unión, en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf).
Artículos 108 al 118 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Publicados en el Diario Oficial de la Federación el 26 de enero de 2018 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 y http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, modificados por última vez el 25 de noviembre de 2020, disponible en el vínculo electrónico https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020, www.dof.gob.mx/2020/INAI/ACT-PUB-11-11-2020-05.pdf, https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf).
Nota: Se incorporan las disposiciones legales específicas en torno a transferencias, no obstante, a fin de señalar el contexto completo de los requerimientos de transferencias en protección de datos personales la referencia debería ampliarse con artículos adicionales y normatividad complementaria.

Nicaragua
Art.14 de la Ley nº 787, Ley de Protección de Datos Personales.

Panamá
Arts. 5 y 33, Ley nº 81, de 26 de marzo de 2019, sobre Protección de Datos Personales.

Perú
Art. 15 de la 29.733.

República Democrática de Santo Tomé y Príncipe
Arts. 19 y 20, Ley 3/2016, de 2 de mayo de Protección de Datos Personales de las Personas Físicas.

República Dominicana
Art. 80 de la Ley Nº 172-13, de 13 de diciembre de 2013, sobre Protección de Datos de Carácter Personal.

Uruguay

Art. 23 de la Ley N° 18.331 de Protección de Datos Personales
Resolución N° 4/019, de 12 de marzo de 2019.
Resolución N° 41/021, de 8 de setiembre de 2021. Disponible en https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay

Nueva Zelanda

Comisionado de privacidad de Nueva Zelanda, Model contract clauses for sending personal information overseas. Disponible en https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/

Reino Unido

Standard Contractual Clauses (SCCs) after the transition period ends, disponible en https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/

UK Standard contractual clauses
https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx
https://ico.org.uk/media/for-organisations/documents/2620101/uk-sccs-c-c-202107.docx