RESOLUCIÓN Nº SPDP-SPD-2026-0004-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el numeral 19 del artículo 66 de la Constitución de la República del Ecuador ("CRE") les reconoce y garantiza, a todas las personas, el derecho *"a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección"*;

Que el artículo 213 CRE establece que *"[l]as superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general (...)"*; que forman parte de la Función de Transparencia y Control Social; y que, conforme lo dispone el artículo 204 *idem,* detentan *"personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa (...)"*;

Que el artículo 3 de la Decisión N° 897 de la Comunidad Andina ("CAN"), publicada en la Gaceta Oficial del Acuerdo de Cartagena N° 4499 del 14 de julio del 2022, define como usuario a la *"[p]ersona natural o jurídica que en forma eventual o permanente, use algún servicio de telecomunicaciones, de conformidad con la normativa interna de los Países Miembros"*;

Que el artículo 4 de la indicada Decisión N° 897 de la CAN les reconoce y garantiza a todos los usuarios de la CAN *"el derecho que tienen todos los usuarios de la Comunidad Andina al debido tratamiento de sus datos personales y a la titularidad sobre los mismos, así como el derecho de acceso, uso, rectificación, eliminación, cancelación, oposición, limitación al tratamiento o circulación de los mismos y a la portabilidad de su información"*;

Que a través de la Ley Orgánica de Protección de Datos Personales ("LOPDP") se creó la Superintendencia de Protección de Datos Personales ("SPDP") como un órgano de control, con potestad sancionatoria, de administración desconcentrada, con personalidad jurídica y autonomía administrativa, técnica, operativa y financiera, cuyo máximo titular es, de acuerdo con el inciso primero del artículo 76 ídem, el Superintendente de Protección de Datos Personales;

Que el artículo 76 de la LOPDP establece que *"[l]a* [Superintendencia de] *Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la* [Ley Orgánica de Protección de Datos Personales]";

Que el numeral 5 de ese mismo artículo 76 de la LOPDP le confiere a la SPDP funciones, atribuciones y facultades para *"[e]mitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales"*;

Que el numeral 10 del señalado artículo 76 de la LOPDP le atribuye a la SPDP, además, la facultad de *"[e]jercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos"*;

Que varios aspectos relacionados con la transferencia o comunicación de datos personales están definidos y regulados por los artículos 4, 12, 17 de la LOPDP, así como por el capítulo V de este mismo cuerpo legal;

Que, de igual manera, los artículos que van del 55 al 61, inclusive, de la LOPDP, regulan de forma específica la transferencia internacional de datos personales;

Que los artículos 21, 22, 23, 38 del Reglamento General de la LOPDP ("RGLOPDP"), así como los que están contenidos en su capítulo XII, precisan los procedimientos y criterios para la transferencia nacional e internacional de datos personales, entre los cuales se incluyen la obligación de obtener el consentimiento del titular o contar con una causal legal de excepción; la exigencia de registrar las actividades de tratamiento, cuando corresponda; los aspectos que deben estimarse para determinar el nivel adecuado de protección de países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales; y la validez de instrumentos jurídicos tales como las normas corporativas vinculantes, las cláusulas contractuales tipo, los códigos de conducta y los mecanismos de certificación;

Que la SPDP es miembro de pleno derecho de la Red Iberoamericana de Protección de Datos Personales ("RIPD"), con voz y voto, de acuerdo con la resolución unánimemente acordada en la Sesión Cerrada del 27 de mayo del 2024, que se llevó a cabo en el marco del XXI Encuentro Iberoamericano 2024 de la RIPD realizado en Cartagena de Indias, Colombia;

Que, de acuerdo con el literal a) del artículo 1 de su Reglamento, la RIPD persigue, entre otros objetivos, *"[p]romover la cooperación, el diálogo y el uso compartido de la información para el desarrollo de iniciativas y políticas de protección de datos y privacidad"*;

Que en el marco del XV Encuentro Iberoamericano de la RIPD se aprobaron y presentaron, el 20 de junio del 2017, los Estándares de Protección de Datos Personales de los Estados Iberoamericanos ("Estándares Iberoamericanos"), que constituyen *"un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso,* [que] *sirvan como referente para la modernización y actualización de las legislaciones existentes"*;

Que el artículo 36 de los Estándares Iberoamericanos instituyen, entre otros aspectos, las reglas generales para las transferencias de datos personales, mientras que el literal c) del apartado 36.1. prevé, como uno de los supuestos para realizarlas, el hecho de que *"[e]l 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"*;

Que la RIPD tiene publicada la Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales ("Guía de Implementación"), cuyo anexo contiene, en su primer apartado, el denominado "*acuerdo modelo de transferencia internacional de datos personales entre responsable y responsable"*;

Que, no obstante lo anterior, en la Guía de Implementación se declara que aquella *"no reemplaza a las normativas nacionales ni a las orientaciones o criterios expresados por las distintas autoridades de protección de datos de la región en el ejercicio de sus facultades"*;

Que a través de la resolución Nº SPDP-SPDP-2024-0022-R, publicada en el Registro Oficial Nº 734 del 31 de enero del 2025, se expidió el Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la SPDP;

Que mediante la resolución N° SPDP-SPD-2025-0002-R del 3 de febrero del 2025 se aprobó el Plan Regulatorio Institucional del año 2025, en el cual se estableció la necesidad de expedir **la normativa aplicable a las transferencias o comunicaciones de datos personales;**

Que la Intendencia de Regulación de Protección de Datos Personales ("IRD"), a través del informe técnico **Nº INF-SPDP-IRD-2025-0082** del **29** de **septiembre** del **2025,** justificó la pertinencia y la necesidad de emitir la **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales;** informe técnico que, en su parte pertinente, señala: *"[l]a SPDP en ejercicio de sus funciones y atribuciones está facultada de conformidad con el numeral 5 del artículo 76 de la LOPDP para emitir la Norma General de Transferencias*

o Comunicaciones Nacionales e Internacionales de Datos Personales con el fin de regular los mecanismos, procedimientos y garantías aplicables a las transferencias o comunicaciones de datos personales dentro y fuera del Territorio de la República del Ecuador."; y, recomendó: "(...) iniciar con el proceso de socialización del proyecto de la Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales, en cumplimiento con lo dispuesto por la Resolución N° SPDP-SPDP-2024-0022-R para que en el término de veinte (20) días la ciudadanía pueda realizar sus aportes";

Que por medio del memorando **N° SPDP-IRD-2025-0188-M,** suscrito el **29** de septiembre del **2025,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") tanto el proyecto normativo denominado **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales se Datos Personales,** como el informe técnico **N° INF-SPDP-IRD-2025-0082,** para que, dentro del término de diez días, se pronuncie sobre la concordancia con la normativa y la legalidad, de conformidad con lo dispuesto en la resolución N° SPDP-SPDP-2024-0022-R del 31 de diciembre del 2024, que contiene el Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales, publicado en el Registro Oficial N° 734 del 31 de enero del 2025;

Que a través del informe jurídico **N° INF-SPDP-DAJ-2025-0044,** remitido a la IRD mediante memorando **N° SPDP-DAJ-2025-0087-M** suscrito el **29** de **septiembre** del **2025,** la DAJ determinó que el proyecto de **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales** es congruente con los principios establecidos en la LOPDP, por cuanto no transgrede o contradice normas matrices, cumple con el principio de legalidad y, por ello, recomendó que *"[l]a IRD debe disponer a quien corresponda la publicación a través de la página web institucional e informar su publicación a través de las redes sociales institucionales, con la finalidad de que la ciudadanía, las organizaciones de la sociedad civil o interesados en general, de manera motivada, puedan remitir sus observaciones o realizar aportes respecto del contenido, para lo cual se debe indicar la forma para recibir dichas observaciones y aportes que será dentro de un término de veinte (20) días contados desde su publicación (...)"*;

Que mediante memorando **N° SPDP-IRD-2025-0189** suscrito el **29** de **septiembre** del **2025,** la IRD solicitó a las unidades administrativas de la SPDP que procedan con las acciones pertinentes, a fin de que publiquen el proyecto que contiene la **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales,** en la página web institucional y en las redes sociales de la SPDP, para que el proyecto de normativa esté disponible para la ciudadanía, las organizaciones de la sociedad civil o los interesados en general, desde el **1** al **29** de **octubre** del **2025,** con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que, para cumplir con la resolución Nº SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización del proyecto que contiene la **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales,** dentro del término de veinte días, de conformidad con el artículo 12 de dicha resolución;

Que a través del informe técnico **Nº INF-SPDP-IRD-2025-0113,** suscrito el **30** de **diciembre** del **2025,** la IRD incorporó las observaciones y aportes que se consideraron relevantes y adecuados, previa justificación de las modificaciones realizadas al proyecto normativo;

Que mediante memorando **N° SPDP-IRD-2025-0271-M** suscrito el **31** de **diciembre** del **2025,** la IRD remitió todo el expediente al suscrito Superintendente de Protección de Datos Personales para que realice las observaciones correspondientes o, en su caso, para que lo apruebe;

Que mediante memorando **N° SPDP-SPD-2026-0002-M** del **9** de **enero** del **2026,** el suscrito Superintendente de Protección de Datos Personales comunicó a la IRD las observaciones que realizó al proyecto de **Norma General de Transferencias o Comunicaciones Nacionales e**

Internacionales de Datos Personales; y, además, solicitó que aquellas sean revisadas de conformidad con el artículo 14 del Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

Que mediante memorando N° **SPDP-IRD-2026-0007-M** del **27** de **enero** del **2026,** la IRD puso en conocimiento del Superintendente de Protección de Datos Personales el proyecto que contiene la **Norma General de Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales** debidamente subsanado, de conformidad con el artículo 14 del aludido Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias,

RESUELVE:

EXPEDIR LA NORMA GENERAL DE TRANSFERENCIAS O COMUNICACIONES NACIONALES E INTERNACIONALES DE DATOS PERSONALES

TÍTULO I
DISPOSICIONES GENERALES

Art. 1.- Esta norma general tiene por objeto regular los procedimientos y requisitos técnicos y jurídicos, que procuran garantizar el ejercicio de los derechos de protección de datos en las transferencias o comunicaciones nacionales e internacionales de datos personales.

Art. 2.- Las disposiciones de esta norma general son de cumplimiento obligatorio para los responsables del tratamiento que formen parte en las acciones de transferencia o comunicación de datos personales ya sean nacionales o internacionales, de acuerdo con el artículo 3 de la LOPDP.

De igual manera, estarán sujetos a esta norma los encargados que, a nombre y por cuenta del responsable del tratamiento, nacional o internacionalmente transfieran o comuniquen datos personales.

Art. 3.- En esta norma general se entenderá por *flujo transfronterizo de datos personales* a la transferencia o comunicación internacional realizada a un destinatario situado en un país distinto al del origen de los datos personales, sin importar el soporte en que aquellos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban, siempre y cuando se realice en el marco de un organismo internacional de integración supranacional.

Art. 4.- Todo responsable o encargado deberá mantener, durante al menos tres (3) años, la documentación que respalde, demuestre y acredite la legalidad y legitimidad de la transferencia o comunicación, tales como contratos, evaluaciones de impacto, medidas de seguridad adoptadas, entre otros, los cuales deberán ser puestos a disposición de la Superintendencia de Protección de Datos Personales ("SPDP") si fueren requeridos.

Art. 5.- El responsable del tratamiento deberá facilitarles a los titulares el derecho a la información que está reconocido en la Ley Orgánica de Protección de Datos Personales ("LOPDP").

TÍTULO II
TRANSFERENCIAS O COMUNICACIONES NACIONALES DE DATOS PERSONALES A TERCEROS

Art. 6.- Las transferencias nacionales de datos personales deberán sujetarse a las siguientes condiciones:

6.1. Que exista una finalidad lícita, legítima y determinada, vinculada a las funciones del responsable y del tercero;

6.2. Que se cuente con una base de legitimación de conformidad con la LOPDP; y,

6.3. Que se disponga del consentimiento informado del titular, salvo en los casos de excepción previstos en la LOPDP.

Art. 7.- Cuando la transferencia se fundamente en el consentimiento del titular, aquel deberá otorgarse de manera previa, libre, específica, informada e inequívoca, luego de haber sido informado sobre la finalidad de la comunicación, la identidad o categoría del tercero destinatario y las garantías aplicables. El consentimiento podrá revocarse en cualquier momento.

Art. 8.- Se deberán implementar, en todo momento, medidas que garanticen la protección de los datos transferidos, entre las que podrán considerarse:

8.1. Limitar la transferencia a los datos estrictamente necesarios para el cumplimiento de la finalidad legítima previamente declarada;

8.2. Emplear mecanismos de transferencia o comunicación seguros, incluidos el cifrado u otras técnicas que preserven la confidencialidad e integridad de los datos personales;

8.3. Formalizar un acuerdo escrito con el tercero o el destinatario en el que este último se comprometa a utilizar los datos personales solo para los fines autorizados, así como a aplicar un nivel de protección equivalente y abstenerse de comunicarlos ulteriormente sin legitimación para ello; y,

8.4. Limitar o controlar transferencias o comunicaciones ulteriores.

Art. 9.- Cuando un titular ejerciere sus derechos respecto de datos que hayan sido transferidos, el responsable del tratamiento deberá notificárselo al destinatario para que adopte los mecanismos necesarios para garantizar la rectificación, actualización, supresión u oposición.

Art. 10.- El destinatario que reciba datos personales asume la calidad de responsable del tratamiento y, por ello, quedará obligado a:

10.1. Respetar las finalidades para las que se le comunicaron los datos;

10.2. Aplicar íntegramente la normativa nacional de protección de datos;

10.3. Atender directamente las solicitudes de derechos de los titulares o, en su caso, cooperar con el responsable que efectuó la transferencia; y,

10.4. Abstenerse de transferir posteriormente los datos sin legitimación adecuada.

TÍTULO III
TRANSFERENCIAS O COMUNICACIONES INTERNACIONALES

CAPÍTULO I
DECLARATORIA DE NIVEL ADECUADO DE PROTECCIÓN

Art. 11.- El reconocimiento de nivel adecuado de protección podrá efectuarse, de oficio, por la SPDP, o también a petición de países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales.

En caso de peticiones cursadas por países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales, la solicitud deberá presentarse debidamente motivada y acompañada de información suficiente que acredite y demuestre:

11.1. Detalle de la legislación nacional y normativa sectorial del país, que tuviere incidencia en materia de protección de datos personales;

11.2. Detalle de la legislación en materia de seguridad nacional, pública y, en general, aquella que tuviere relación con la defensa y seguridad del Estado, así como la legislación en materia penal. Se debe hacer especial énfasis en las disposiciones que habiliten el acceso a datos personales por parte de las autoridades del país, la organización internacional, la persona jurídica o el territorio económico internacional;

11.3. Detalle de la normativa sobre transferencias o comunicaciones ulteriores de datos personales a terceros países, organizaciones o personas jurídicas;

11.4. Detalle de la jurisprudencia vinculada a la protección de datos personales;

11.5. Detalle de los derechos y de los mecanismos reconocidos a favor de los titulares para que los puedan ejercer de manera efectiva;

11.6. Detalle de los deberes y obligaciones de los responsables y encargados del tratamiento de datos personales en el país u organización internacional;

11.7. La existencia de una autoridad de protección de datos personales o similar, que sea independiente y que tenga competencias de control y vigilancia del cumplimiento de la normativa en materia de protección de datos personales, así como de competencia para aplicar el régimen sancionatorio respectivo en el caso del cometimiento de infracciones en esta materia. Adicionalmente, se deberá especificar si la autoridad brinda asistencia y asesoría a los titulares, así como si coopera con instituciones y organismos internacionales y sus pares a nivel internacional;

11.8. Detalle de los compromisos internacionales asumidos por el país, organización internacional, persona jurídica o territorio económico internacional en cuanto a la materia de protección de datos personales;

11.9. Todo otro elemento que demuestre la existencia de un nivel de protección equivalente o superior al ecuatoriano; y,

11.10. Domicilio electrónico para notificaciones.

Toda la información remitida deberá indicar el lugar y la forma en que pueda ser verificada.

Sin perjuicio de lo anterior, la SPDP podrá requerir información complementaria y/o realizar consultas con la autoridad de protección de datos del Estado del solicitante, así como con organismos internacionales especializados en la materia.

Art. 12.- El procedimiento para el reconocimiento de nivel adecuado de protección se desarrollará de conformidad con las siguientes fases, bajo la competencia de la SPDP y de sus unidades administrativas correspondientes:

12.1. **Admisión de la solicitud:** La Intendencia General de Regulación de Protección de Datos Personales (“IRD”) calificará la petición presentada por el país, organización internacional, persona jurídica o territorio económico internacional, previa verificación del cumplimiento de los requisitos formales previstos en el artículo precedente.

12.2. **Subsanación:** En caso de determinarse omisiones o incumplimientos relacionados con los requisitos respectivos, se concederá al solicitante el término improrrogable de treinta (30) días para su subsanación, con la advertencia de que, en caso de no hacerlo o no haber acreditado suficientemente lo requerido, se dispondrá el archivo del expediente, sin perjuicio de que lo pueda volver a presentar después de transcurridos seis (6) meses desde la notificación de archivo.

12.3. **Requerimiento de información adicional:** Cuando la documentación presentada resultare insuficiente para un análisis integral o surgieren dudas sobre el cumplimiento de los requisitos, la IRD podrá requerirle al solicitante que remita la información faltante o la que fuere complementaria, para lo cual habrá de señalar, de manera expresa, el alcance de lo solicitado y el plazo concedido para su entrega.

12.4. **Informe técnico:** Una vez que la solicitud estuviere completa, o que aquella hubiese sido completada satisfactoriamente en caso de subsanación, la SPDP tendrá un plazo de hasta seis (6) meses para declarar al país, organización internacional, persona

jurídica, o territorio económico internacional con nivel adecuado de protección o, en su caso, negar la solicitud. La IRD elaborará un informe técnico, debidamente motivado, en el cual verificará si el solicitante reúne los criterios y condiciones para recibir la calificación de nivel adecuado de protección de datos personales.

El informe deberá analizar si la documentación remitida es pertinente, suficiente y coherente con los estándares establecidos en la LOPDP y el RGLOPDP.

A base de dicho análisis, la IRD deberá recomendarle al Superintendente de Protección de Datos Personales ("Superintendente"), de manera expresa, la procedencia o no de declarar el nivel adecuado de protección.

12.5. Decisión jerárquica: El expediente será remitido al Superintendente, quien dispondrá que la DAJ que elabore el proyecto de resolución, el cual deberá ser preparado y remitido a la máxima autoridad en el término de diez (10) días. A base de dicho proyecto, el Superintendente podrá expedir una resolución motivada para reconocer o, en su caso, negar el nivel adecuado de protección; resolución que será notificada al solicitante de acuerdo con las normas de procedimiento administrativo aplicables.

12.6. Registro y publicidad: Expedida la resolución, será remitida a la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales ("IIT") para que se inscriba en el Registro Nacional de Datos Personales.

Art. 13.- Cuando la SPDP actúe de oficio para reconocer el nivel adecuado de protección de un país, organización internacional, persona jurídica o territorio económico internacional, el procedimiento se desarrollará conforme a las siguientes fases:

13.1. Determinación inicial: La IRD identificará, por propia iniciativa, países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales respecto de los cuales existan antecedentes relevantes que justifiquen la evaluación de su nivel de protección de datos personales, para cuyos efectos emitirá el informe técnico respectivo.

13.2. Apertura del expediente: Emitido el informe técnico antes señalado, la IRD dispondrá la apertura de un expediente administrativo, en el que se consignarán las fuentes de información iniciales a fin de cumplir con los requisitos establecidos en el RGLOPDP.

13.3. Recolección de información: La IRD recabará, de manera directa o mediante requerimientos formales a organizaciones internacionales, personas jurídicas públicas o a las privadas que considerare necesarias, información oficial disponible sobre:

13.3.1. Detalle de la legislación nacional y normativa sectorial del país o territorio económico internacional, que tuviere incidencia en materia de protección de datos personales;

13.3.2. Detalle de la legislación en materia de seguridad nacional, pública y, en general, aquella que tuviere relación con la defensa y seguridad del Estado, así como la legislación en materia penal. Se hará especial énfasis en las disposiciones que habiliten el acceso a datos personales por parte de las autoridades del país, organización o persona jurídica al que se le pudiere reconocer, de oficio, el nivel adecuado de protección;

13.3.3. Detalle de la normativa sobre transferencias ulteriores de datos personales a terceros países, organizaciones o personas jurídicas;

13.3.4. Detalle de la jurisprudencia vinculada a la protección de datos personales;

13.3.5. Detalle de los derechos y de los mecanismos reconocidos a favor de los titulares para que los puedan ejercer de manera efectiva;

13.3.6. Detalle de los deberes y obligaciones de los responsables y encargados del tratamiento de datos personales en el país u organización internacional;

13.3.7. Verificación de la existencia de una autoridad de protección de datos personales que sea independiente y que tenga competencias de control y vigilancia del cumplimiento de la normativa en materia protección de datos personales, así como la competencia para aplicar el régimen sancionatorio en caso del cometimiento de infracciones en esta materia. Adicionalmente, se debe especificar si la autoridad brinda asistencia y asesoría a los titulares y cooperan con instituciones internacionales y/o sus pares a nivel internacional;

13.3.8. Detalle de los compromisos internacionales asumidos por el país, organización internacional persona jurídica o territorio económico internacional en cuanto a la materia de protección de datos personales; y,

13.3.9. Cualquier otro elemento que demuestre la existencia de un nivel de protección equivalente o superior al ecuatoriano.

La IRD podrá solicitarles a las instituciones de educación superior con quienes tuviere suscrito un acuerdo de entendimiento, que realicen la recolección de información.

13.4. Consulta especializada: La IRD podrá requerir la intervención técnica de la Intendencia General de Control y Sanción ("ICS"), así como recabar informes de organismos internacionales, autoridades extranjeras homólogas, entidades académicas o centros de investigación especializados, en particular de universidades con las que la SPDP mantuviere convenios de cooperación interinstitucional vigentes, dentro de los términos adecuados establecidos por dicha unidad administrativa. Dichos informes deberán incorporarse íntegramente al expediente administrativo respectivo, en caso de ser recibidos.

13.5. Informe técnico: Una vez realizada la recolección de información, la SPDP tendrá hasta seis (6) meses para declarar a un país, organización internacional, persona jurídica o territorio económico internacional con nivel adecuado de tratamiento de datos personales. La IRD elaborará un informe motivado que verificará el cumplimiento de los criterios para otorgar la calificación de nivel adecuado.

El informe deberá analizar si se cumple de forma suficiente con los estándares establecidos en la LOPDP y el RGLOPDP.

A base de dicho análisis, la IRD deberá recomendarle al Superintendente, de manera expresa, la procedencia o no de declarar el nivel adecuado de protección.

13.6. Decisión jerárquica: El expediente será remitido al Superintendente, quien dispondrá que la DAJ elabore el proyecto de resolución, el cual deberá ser remitido a la máxima autoridad en el término de diez (10) días. A base de dicho proyecto, el Superintendente podrá expedir una resolución motivada para reconocer o, en su caso, negar el nivel adecuado de protección; resolución que se notificará de acuerdo con las normas del procedimiento administrativo aplicable.

13.7. Registro y publicidad: Expedida la resolución, será remitida a la IIT para que se inscriba en el Registro Nacional de Datos Personales.

Art. 14.- La resolución motivada que se expida para reconocer o negar el nivel adecuado de protección, deberá, como mínimo, contener:

14.1. La identificación del país, organización internacional, persona jurídica o territorio económico internacional;

14.2. El alcance del reconocimiento, incluidas las categorías de datos y finalidades de tratamiento autorizadas, en caso de haberlas;

14.3. Las condiciones y limitaciones específicas;

14.4. La vigencia del reconocimiento, que no podrá exceder de cuatro (4) años; y,

14.5. La obligación de revisión anual, de acuerdo con la normativa aplicable.

La resolución se mandará a publicar en el Registro Oficial así como en el portal institucional de la SPDP. Se inscribirá, además, en el Registro Nacional de Protección de Datos Personales, que contendrá el listado público de países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales declarados con nivel adecuado de protección.

Art. 15.- Las resoluciones de reconocimiento de nivel adecuado de protección tendrán una vigencia máxima de cuatro (4) años, contados desde su expedición; sin embargo, la SPDP revisará su cumplimiento anualmente.

Art. 16.- La SPDP cada año revisará, de oficio o a petición de parte —o también en cualquier momento— si existieren circunstancias supervinientes que pudieren afectar las condiciones que motivaron el reconocimiento.

Para ejecutar dicha revisión, se seguirá el procedimiento de revisión establecido en estas normas generales; y, en caso de que se determinare que han dejado de existir las condiciones fácticas o jurídicas que motivaron la declaratoria de nivel adecuado, la SPDP iniciará procedimiento de revocatoria.

Una vez expedida la resolución de revocatoria, deberán cesar, de manera inmediata, las transferencias o comunicaciones hacia el país, organización internacional, persona jurídica o territorio económico internacional, salvo que las transferencias se encontraren amparadas en garantías adecuadas o en otros fundamentos previstos en la normativa de protección de datos personales.

La revocatoria se mandará a publicar en el Registro Oficial y surtirá efectos desde su notificación, aunque sin retroactividad respecto de las transferencias o comunicaciones realizadas de manera anterior.

Art. 17.- Cada año la SPDP realizará, de oficio o de manera extraordinaria (cuando existieren circunstancias supervinientes que lo justifiquen), una revisión de los países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales reconocidos con nivel adecuado de protección, de acuerdo con el siguiente procedimiento:

17.1. Apertura de la revisión: La IRD dispondrá la apertura del expediente de revisión mediante oficio motivado, fundado en el cumplimiento del plazo de vigencia o en la existencia de circunstancias nuevas o imprevistas que generen dudas razonables sobre la continuidad del nivel adecuado de protección.

17.2. Recopilación de información: La IRD recabará información actualizada relativa al cumplimiento continuo de la LOPDP y el RGLOPDP, aunque no en forma exclusiva, especialmente cuando existieren:

17.2.1. Modificaciones legislativas o regulatorias en materia de protección de datos personales;

17.2.2. Cambios institucionales o funcionales en la autoridad de control extranjera;

17.2.3. Informes de organismos internacionales, autoridades homólogas y entidades académicas; y,

17.2.4. Antecedentes recientes de vulneraciones, brechas de seguridad o sanciones relevantes.

17.3. Consulta especializada: La IRD podrá solicitar a la IIT, así como a la ICS, la elaboración de informes técnicos destinados a evaluar la eficacia práctica del marco de protección de datos personales, así como las vulneraciones que, a su criterio, resultaren relevantes. De igual manera, podrá incorporar como fuentes los informes elaborados por organismos internacionales, entidades académicas y, en particular, con las instituciones de educación superior con las que la SPDP mantuviere acuerdos de entendimiento, además de las organizaciones de la sociedad civil, para que analicen la efectividad real de dicho marco de protección.

17.4. Informe preliminar y fase de observaciones: La IRD elaborará un informe preliminar con las conclusiones de la revisión, que será puesto a consideración del país, organización internacional, persona jurídica o territorio económico internacional para que solicite las aclaraciones que estimare necesarias; ello de conformidad con las siguientes reglas:

17.4.1. Revisión cuando la evaluación inicial del nivel adecuado se hubiese realizado por petición: El informe será notificado al país, organización internacional, persona jurídica o territorio económico internacional solicitante, otorgándole un término de treinta (30) días para presentar su contestación, observaciones o descargos;

17.4.2. Revisión cuando la evaluación inicial del nivel adecuado se hubiese realizado de oficio: El informe preliminar será publicado en el portal institucional de la SPDP por un término de treinta (30) días, con el fin de que cualquier interesado pueda presentar observaciones, objeciones o pruebas documentales que considere pertinentes.

En ambos casos, las observaciones recibidas se incorporarán al expediente y serán analizadas en el informe final.

17.5. Informe final: Sobre la base de la información recabada y de las observaciones recibidas, la IRD elaborará un informe final motivado en el que se recomendará:

17.5.1. Mantener el reconocimiento;

17.5.2. Modificar las condiciones del reconocimiento; o,

17.5.3. Revocar el reconocimiento del nivel adecuado de protección de datos personales.

El informe final será elevado al Superintendente.

17.6. Resolución de aprobación: El Superintendente, luego de la revisión del informe final remitido por la IRD, dispondrá que la DAJ elabore el proyecto de resolución correspondiente para que lo remita en el término de diez (10) días.

17.7. Registro y publicidad: La resolución de revisión será notificada al país, organización internacional, persona jurídica o territorio económico internacional. De igual manera, se la mandará a publicar en el Registro Oficial y será remitida a la

IIT para su inscripción en el Registro Nacional de Protección de Datos, con el objeto de facilitar su disponibilidad para la ciudadanía.

CAPÍTULO II
TRANSFERENCIAS O COMUNICACIONES A PAÍSES, ORGANIZACIONES INTERNACIONALES, PERSONAS JURÍDICAS O TERRITORIOS ECONÓMICOS INTERNACIONALES CON NIVEL ADECUADO

Art. 18.- En la transferencia o comunicación a países declarados con nivel adecuado de protección, el responsable del tratamiento, sin perjuicio de lo dispuesto en último inciso de este artículo, deberá:

18.1. Verificar y constatar que el destinatario figure en el listado de países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales con nivel adecuado de protección y que la resolución no haya sido revocada o suspendida a la fecha de la transferencia o comunicación;

18.2. Adoptar medidas contractuales y técnicas para garantizar que el destinatario cumpla con las obligaciones y principios de la LOPDP, incluidas aquellas cláusulas que propendan a garantizar la integridad, disponibilidad y confidencialidad de la información, la protección de los derechos de los titulares y la limitación de transferencias o comunicaciones ulteriores;

18.3. Mantener un registro actualizado de las transferencias o comunicaciones realizadas, que incluya las categorías de los datos, las finalidades y los destinatarios;

18.4. Informar a los titulares de los datos sobre las transferencias o comunicaciones y los mecanismos de protección existentes; y,

18.5. Cumplir con el registro de información sobre transferencias internacionales en el Registro Nacional de Protección de Datos, de conformidad con el RGLOPDP.

Estas mismas obligaciones las deberán cumplir los encargados que, a nombre y por cuenta del responsable del tratamiento, transfirieren o comunicaren datos personales nacional o internacionalmente.

Art. 19.- En las transferencias o comunicaciones de datos personales hacia países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales que hubiesen sido declarados con nivel adecuado de protección, el destinatario deberá:

19.1. Cumplir, en todo momento, con la normativa de protección de datos personales vigente en su jurisdicción y con los estándares reconocidos en la resolución de adecuación; y,

19.2. Respetar las finalidades para las cuales recibió los datos, así como abstenerse de transferirlos a otros destinatarios, salvo que contare con una base legal válida y cumpliere con las mismas condiciones de protección.

CAPÍTULO III
TRANSFERENCIAS O COMUNICACIONES POR GARANTÍAS ADECUADAS

Art. 20.- Cuando el país, organización internacional, persona jurídica, territorio económico internacional o destinatario no contare con un nivel adecuado de protección de datos personales, las transferencias o comunicaciones sólo podrán efectuarse si el responsable o el encargado del tratamiento implementaren garantías adecuadas, que aseguren la protección efectiva de los derechos de los titulares.

Se entenderán como garantías adecuadas:

20.1. Las cláusulas contractuales tipo adoptadas o reconocidas por la SPDP, por organismos internacionales de los que el Ecuador fuere parte, o por autoridades de

protección de datos de los países con los que la SPDP hubiere suscrito acuerdos de cooperación;

20.2. Las normas corporativas vinculantes por grupos empresariales, filiales o *joint ventures,* aprobadas por la SPDP de conformidad con el procedimiento aplicable;

20.3. Los códigos de conducta con carácter vinculante, que contaren con la aprobación de la SPDP; y,

20.4. Los mecanismos de certificación emitidos por entidades acreditadas, que incluyan compromisos jurídicamente exigibles y que aseguren el cumplimiento permanente de los estándares de la LOPDP y el RGLOPDP.

Art. 21.- Las garantías adecuadas señaladas en el artículo anterior deberán cumplir, al menos, las siguientes condiciones:

21.1. Vinculatoriedad y oponibilidad jurídica: Deben ser jurídicamente exigibles, claras, escritas y garantizarán el cumplimiento cabal de las obligaciones asumidas y la protección efectiva de los derechos de los titulares;

21.2. Principios de protección de datos: Deben asegurar la observancia de los principios previstos en la LOPDP;

21.3. Supervisión y cumplimiento: Deben incorporar mecanismos de supervisión que permitan verificar, periódicamente, la observancia de las obligaciones asumidas;

21.4. Derechos de los titulares: Deben reconocer los derechos previstos en la Ley Orgánica de Protección de Datos Personales y establecer procedimientos claros para su ejercicio, así como establecer los plazos y canales para ejercerlos tanto ante el destinatario como, en su caso, ante la Superintendencia de Protección de Datos Personales;

21.5. Transferencias o comunicaciones ulteriores: Deben garantizar que las transferencias o comunicaciones ulteriores a terceros países u organizaciones internacionales, sólo se podrán realizar si cumplen con los mismos requisitos y garantías previstas en la LOPDP, el RGLOPDP y esta norma general;

21.6. Aceptación de jurisdicción: Deben contemplar, de manera expresa, la obligación de que el destinatario acepte y se someta voluntariamente a la jurisdicción, a la normativa y a las decisiones o resoluciones que dictare la SPDP, así como a las providencias judiciales y resoluciones de los jueces, tribunales y cortes ecuatorianos que fueren expedidos o dictados en materia de protección de datos personales; y,

21.7. Reparación efectiva: Deben incluir mecanismos de responsabilidad y reparación integral a favor de los titulares, en caso de vulneración de sus derechos.

CAPÍTULO IV
CLÁUSULAS CONTRACTUALES MODELO – TIPO

Art. 22.- En lo que atañe a las transferencias de datos personales, la SPDP —en su calidad de miembro de pleno derecho de la RIPD— reconoce como propias las cláusulas contractuales modelo-tipo ("CCM") emitidas por y vigentes en el marco de dicha Red, específicamente las que están recogidas en el llamado *"acuerdo modelo de transferencia internacional de datos personales entre responsable y responsable",* que constan en anexo de la Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales; y, en consecuencia, las considera como válidas y suficientes para legitimar las transferencias o comunicaciones internacionales de los responsables o encargados hacia los destinatarios, con excepción de lo previsto en el artículo siguiente.

Las cláusulas contractuales modelo-tipo de la RIPD vigentes a la fecha, son las que constan en el Anexo I de esta norma general.

Art. 23.- De conformidad con la legislación ecuatoriana, el encargo de tratamiento no constituye una transferencia ni comunicación de datos personales. En consecuencia, las CCM entre responsables y encargados, emitidas por la RIPD, no son aplicables en la República del Ecuador.

Art. 24.- Sin perjuicio de lo establecido en el artículo anterior, cuando se usaren las CCM por parte de un responsable en un encargo de tratamiento, dicho uso de lo tendrá como una buena práctica dentro del marco dado por el principio de responsabilidad proactiva, en cuanto coadyuvan a la transparencia, seguridad jurídica y fortalecimiento de las obligaciones contractuales en materia de protección de datos personales.

Art. 25.- En caso de que las CCM no cumplieren con alguno de los requisitos de validez previstos en esta norma general, para que puedan ser consideradas válidas deberán incorporarse las disposiciones necesarias a fin de garantizar el cumplimiento de los estándares establecidos por la normativa ecuatoriana de protección de datos personales.

Art. 26.- La SPDP podrá verificar el cumplimiento y la adecuada implementación de las CCM en el marco de sus facultades de control y supervisión. El incumplimiento de las obligaciones derivadas de dichas cláusulas constituirá una infracción de acuerdo con lo previsto en la LOPDP.

Art. 27.- La SPDP podrá reconocer y actualizar los modelos de cláusulas contractuales tipo adoptados en el marco de la RIPD o en otros foros internacionales especializados, siempre que resulten compatibles con la normativa nacional y coadyuven al fortalecimiento de la protección de datos personales en la República del Ecuador.

CAPÍTULO V
NORMAS CORPORATIVAS VINCULANTES

Art. 28.- Las normas corporativas vinculantes son de obligatorio cumplimiento y exigibilidad para todas las empresas de un grupo empresarial o económico que actúen como responsables del tratamiento, así como para sus encargados del tratamiento y el personal involucrado. Dichas normas deberán integrarse de manera coherente e integral en todos los giros de negocio del grupo empresarial; y, por ello, deberán reflejarse en sus políticas internas, contratos laborales o instrumentos equivalentes.

Las normas corporativas vinculantes deberán cumplir con las obligaciones establecidas en el artículo 58 de la LOPDP, así como con los demás artículos concordantes del RGLOPDP.

Art. 29.- El grupo empresarial deberá, como parte de su gobernanza de datos personales:

29.1. Designar a la empresa que se encuentre domiciliada en el Ecuador como entidad principal responsable de la implementación, supervisión y respuesta frente a titulares y/o ante la SPDP para el cumplimiento de las normas corporativas vinculantes aprobadas, sin perjuicio de la responsabilidad de las demás empresas que formaren parte del grupo;

29.2. Designar un delegado de protección de datos personales, cuyos datos de contacto deberán mantenerse disponibles y actualizados en el portal del grupo empresarial; y,

29.3. Designar un apoderado especial cuando el grupo no cuente con establecimiento en el Ecuador, de acuerdo con la normativa de protección de datos personales. En todo caso, el apoderado especial no servirá para suplir al delegado de protección de datos personales; tampoco decidirá sobre el tratamiento, ni podrá desempeñar las funciones de delegado de protección de datos personales.

Art. 30.- La aprobación de las normas corporativas vinculantes por parte de la SPDP tendrá un plazo de vigencia de cuatro (4) años. El grupo deberá informar a la SPDP sobre cualquier modificación sustancial que se realizare en las normas corporativas vinculantes o en la estructura del grupo empresarial. La SPDP podrá suspender o revocar la aprobación por incumplimientos de la normativa de protección de datos personales, o que pudieren generar riesgos sistémicos.

Art. 31.- Para la autorización de las normas corporativas vinculantes se cumplirá el siguiente procedimiento:

31.1. Presentación de la solicitud: El responsable del tratamiento que pretendiere realizar una transferencia o comunicación internacional prevalido de normas corporativas vinculantes, deberá presentar una solicitud motivada ante la SPDP y acompañada de la siguiente documentación:

31.1.1. El proyecto de normas corporativas vinculantes desarrolladas para el grupo específico, las cuales deben cumplir con la LOPDP, el RGLOPDP, esta norma general y la demás normativa que emitiere la SPDP;

31.1.2. El análisis de riesgos y, si fuese exigible de acuerdo con el artículo 42 de la LOPDP, la evaluación de impacto;

31.1.3. La estructura y composición del grupo, en los que deberán identificarse todas las empresas cubiertas por las normas corporativas vinculantes, así como la identificación de la empresa principal responsable de su implementación y cumplimiento; y,

31.1.4. El detalle de los procesos y de las categorías de datos, en los que se describirán la naturaleza y finalidad de las transferencias o comunicaciones entre las empresas, las categorías de los datos que se transferirán y las categorías de los titulares a quienes corresponden.

31.2. Revisión técnica: La IRD analizará la solicitud y verificará que el instrumento presentado cumpla con las condiciones mínimas establecidas en la LOPDP, el RGLOPDP, esta norma general y la demás normativa aplicable.

31.3. Informe consolidado: La SPDP dispondrá de un plazo de hasta dos (2) meses, que se contarán desde que la solicitud hubiese sido presentada en forma completa, para aprobar, disponer la subsanación o negar la petición. Sobre la base de la documentación presentada, la IRD elaborará un informe consolidado donde constarán el análisis y los resultados de la revisión técnica realizada, así como la recomendación de aprobar, subsanar o negar las normas corporativas vinculantes.

En caso de que se dispusiere la subsanación de las normas corporativas vinculantes, el responsable del tratamiento que hubiere presentado la solicitud tendrá el término de treinta (30) días para ajustarlas y presentarlas a la SPDP. Si no se llegase a presentar la subsanación en la forma solicitada, se archivará la solicitud de autorización, sin perjuicio de que las pueda volver a presentar en el término de treinta (30) días contados desde que se emitiere la resolución de negativa o de archivo, según correspondiere.

31.4. Resolución de aprobación: En caso de que el informe recomiende la aprobación de las normas corporativas vinculantes, el expediente será remitido al Superintendente, quien dispondrá que la DAJ elabore el proyecto de resolución correspondiente para que lo remita en el término de diez (10) días contado desde la fecha de la notificación de dicha disposición.

El Superintendente expedirá una resolución motivada en virtud de la cual podrá:

31.4.1. Aprobar las normas corporativas vinculantes propuestas; o,

31.4.2. Negar la aprobación cuando no se cumplieren las condiciones establecidas.

31.5. Registro y publicidad: La resolución de aprobación será remitida a la IIT para que la haga constar en el Registro Nacional de Protección de Datos.

Art. 32.- Para la revisión o, en su caso, para la revocatoria de la aprobación de las normas corporativas vinculantes, se cumplirá el siguiente procedimiento:

32.1. Inicio del procedimiento: La ICS podrá iniciar, de oficio o a petición de parte, el procedimiento de revisión y posible revocatoria cuando existieren indicios razonables de que el grupo empresarial, ya sea una empresa o ya fueren varias integrantes del mismo grupo, incumplieron los requisitos establecidos en las normas corporativas vinculantes aprobadas.

Sobre la base de tales indicios, la ICS deberá verificar la existencia del incumplimiento mediante el inicio de una actuación previa. Concluido dicho proceso, y de verificarse que el grupo empresarial o una de sus empresas se encontrare incursa en alguna causal de revocatoria o hubiere incumplido la normativa de protección de datos personales, se remitirá a la IRD un informe técnico en el que evidenciará cuál ha sido el incumplimiento constatado.

Si el incumplimiento fuere de aquellos constitutivos de infracción de acuerdo con la LOPDP, la ICS podrá continuar con la actuación previa y, eventualmente, disponer que se implementen medidas correctivas.

32.2. Causales de revocatoria: Constituyen causales de revocatoria:

32.2.1. El incumplimiento de las condiciones mínimas previstas en la LOPDP, el RGLOPDP, esta norma general y la demás normativa que emitiere la SPDP;

32.2.2. La comprobación de vulneraciones graves o reiteradas de datos personales que afecten a los derechos y las libertades de los titulares;

32.2.3. La ausencia de mecanismos internos efectivos de supervisión o auditoría frente a incumplimientos;

32.2.4. La negativa expresa o la imposibilidad del destinatario de sujetarse a la jurisdicción ecuatoriana; y,

32.2.5. La existencia de resoluciones internacionales o informes que evidencien deficiencias estructurales en la protección de datos del destinatario.

32.3. Informe técnico: Una vez que la IRD reciba el informe técnico emitido por la ICS, comenzará a discurrir el plazo de dos (2) meses para la emisión de la resolución correspondiente.

Luego de que la IRD tenga la información, elaborará un informe motivado en virtud del cual podrá recomendar que se rectifique la aprobación de las normas corporativas vinculantes, que se dispongan modificaciones o, en su caso, que la autorización sea revocada.

32.4. Modificación: En caso de que se concluyere modificar las normas corporativas vinculantes, el grupo empresarial o las empresas que correspondan deberán modificarlas en un término de treinta (30) días. Al efecto, se cumplirá el mismo procedimiento establecido para la autorización.

32.5. Resolución: Se le notificará al Superintendente con el informe técnico que recomiende la revocatoria o la rectificación, quien dispondrá que la DAJ elabore el proyecto de resolución correspondiente para que lo remita en el término de diez (10)

días contado desde la fecha de la notificación de su disposición. Hecho lo anterior, el Superintendente expedirá una resolución motivada en virtud de la cual podrá:

32.5.1. Ratificar las normas corporativas vinculantes;

32.5.2. Modificarlas, en cuyo caso el proceso volverá a la etapa prevista en el apartado 32.3.; o,

32.5.3. Revocar la aprobación de las normas corporativas vinculantes.

32.6. Efectos de la revocatoria: Expedida la resolución de revocatoria, el grupo empresarial deberá cesar inmediatamente, sin dilación alguna, las transferencias o comunicaciones internacionales amparadas en las normas corporativas vinculantes revocadas, salvo que pudiere justificar dicha transferencia o comunicación a través de otro mecanismo legal previsto en la LOPDP.

32.7. Registro y publicidad: La resolución de revocatoria será notificada al grupo empresarial y a la IIT para su registro y publicación en el portal institucional de la SPDP, con el objeto de facilitar su acceso público.

Art. 33.- A través de la ICS, y mientras se lleve a cabo el proceso de revisión o revocatoria, la SPDP podrá disponer, mediante resolución motivada, la suspensión temporal de la aplicación de las normas corporativas vinculantes previamente aprobadas, siempre y cuando existieren indicios razonables de que dicha garantía no asegura un nivel de protección equivalente al previsto en la LOPDP y el RGLOPDP.

La suspensión tendrá carácter preventivo y se mantendrá vigente hasta la conclusión del procedimiento de revisión o revocatoria correspondiente.

Durante el período de suspensión, el grupo empresarial únicamente podrá realizar transferencias o comunicaciones internacionales que no se fundamenten en la garantía suspendida. Las transferencias o comunicaciones previamente efectuadas sobre la base de dicha garantía serán objeto de un control posterior o *ex post facto.*

Art. 34.- Las normas corporativas vinculantes deberán incluir, al menos, los elementos esenciales que permitan demostrar su cumplimiento efectivo, con la posibilidad de adaptar su estructura según el tamaño, naturaleza y complejidad del grupo empresarial.

Los contenidos mínimos serán los siguientes:

34.1. Objeto y alcance de aplicación;

34.2. Principios y obligaciones generales;

34.3. Derechos de los titulares de datos y sus mecanismos de atención;

34.4. Estructura del grupo empresarial y roles de responsabilidad;

34.5. Datos de contacto de todas las empresas del grupo;

34.6. Procedimientos internos de cumplimiento, supervisión y reporte;

34.7. Auditorías y verificaciones periódicas internas;

34.8. Medidas de transparencia, control y cooperación con autoridades;

34.9. Compromiso de formación y cultura organizacional en protección de datos personales; y,

34.10. Anexos o listados actualizables de filiales y encargados.

CAPÍTULO VI
PROCEDIMIENTO PARA LA APROBACIÓN DE CÓDIGOS DE CONDUCTA

Art. 35.- Podrán presentar proyectos de códigos de conducta para la aprobación de la SPDP cualquier persona natural o jurídica, asociación, gremio, cámara, federación, consorcio, grupo de empresas o entidad que, debido a sus actividades, intervengan en operaciones de tratamiento de datos personales.

Art. 36.- Todo proyecto de código de conducta deberá contener obligatoriamente, y como mínimo, lo siguiente:

36.1. Una exposición de motivos que describa, de forma clara y comprensible, los objetivos del código y la forma en que facilitará el cumplimiento de la normativa de protección de datos personales;

36.2. El ámbito de aplicación que, de manera específica, determine:

36.2.1. Las operaciones de tratamiento reguladas;

36.2.2. Los responsables o encargados a los que se aplica de acuerdo con el giro del negocio o sector; y,

36.2.3. Las materias o riesgos específicos que aborda, incluidas unas soluciones prácticas proporcionales.

36.3. Los mecanismos de supervisión y control que aseguren el cumplimiento efectivo del código, con la identificación de los órganos responsables y que permitan estructuras internas adaptadas a la escala del sector o actividad;

36.4. Las medidas de protección de derechos que establezcan procedimientos claros, accesibles y gratuitos para que los titulares ejerzan sus derechos, así como los mecanismos para la gestión de reclamaciones y resolución de conflictos;

36.5. Las reglas de transparencia que obliguen a los responsables y encargados adheridos a informar a los titulares sobre su adhesión al código y las garantías que aquel les ofrece;

36.6. Los mecanismos de adhesión que describan cómo las entidades podrán adherirse al código, las condiciones de admisibilidad y las obligaciones derivadas de dicha adhesión;

36.7. Las medidas internas de advertencia, suspensión o exclusión en casos de incumplimiento;

36.8. Los mecanismos de auditoría y verificación anual que permitan evaluar el cumplimiento del código, con la obligación de emitir informes internos y externos cuyos resultados podrán ser solicitados por la SPDP, sin perjuicio de que la autoridad pueda disponer, en cualquier momento, la realización de una auditoría cuando lo considere necesario;

36.9. El compromiso de cooperación mediante el cual el órgano de supervisión del código se obligará a remitir informes cuando le fueren requeridos, así como a cooperar con la SPDP;

36.10. Los procedimientos de actualización y revisión que garanticen la adecuación permanente del código a los cambios normativos, tecnológicos y de buenas prácticas internacionales en materia de protección de datos;

36.11. El modelo de gobernanza del código, que incluya:

36.11.1. Los órganos internos de supervisión;

36.11.2. Los procedimientos de toma de decisiones; y,

36.11.3. Los mecanismos de control del cumplimiento.

36.12. Una cláusula de publicidad que obligue a difundir el código aprobado en medios accesibles al público, así como un listado de las entidades adheridas que deberá mantenerse actualizado.

Art. 37.- El proyecto de código de conducta podrá presentarse en formato electrónico ante la SPDP a través de su portal web institucional o en forma física, de ser el caso, con las debidas firmas de responsabilidad

La SPDP, dentro del término de treinta (30) días, verificará el cumplimiento de la presentación de los requisitos formales previstos en el artículo anterior y, en caso de hallarlos cumplidos, la IDR expedirá un acto de simple administración para notificarle tal particular al proponente, además de disponer la evaluación de fondo del proyecto.

De no cumplirse los requisitos formales, la SPDP dispondrá al proponente subsanar o aclarar la información en un término de treinta (30) días, para lo cual se identificarán expresamente los defectos o disconformidades observados.

Si el proponente no subsanare, no aclarare o lo hiciere de manera incompleta o errónea, la SPDP ordenará el archivo de la solicitud, sin perjuicio de que se la pueda volver a presentar en el término de treinta (30) días contados desde que se notifique el oficio en el que se informa tal archivo.

Art. 38.- Admitido a trámite el proyecto de código de conducta, la SPDP, dentro del término de sesenta (60) días, evaluará y verificará su conformidad con la normativa vigente, considerando la naturaleza del sector y las obligaciones de los responsables o encargados comprendidos.

Además de los criterios establecidos en la LOPDP, la SPDP analizará los siguientes aspectos:

38.1. **Relevancia sectorial:** El código deberá responder a una necesidad específica del sector o actividad de tratamiento, además de aportar con valor práctico a la aplicación de la normativa;

38.2. **Participación representativa:** El código reflejará la intervención de actores relevantes del sector que apliquen prácticas comunes y legítimas;

38.3. **Claridad y coherencia interna:** Las disposiciones del código deberán ser claras, consistentes y armonizadas con la LOPDP, el RGLOPDP, esta norma general y la demás normativa aplicable expedida por la SPDP;

38.4. **Proporcionalidad:** Las obligaciones previstas en el código deberán ser adecuadas y proporcionales al nivel de riesgo que implique el tratamiento de los datos;

38.5. **Mecanismos de adhesión y desvinculación:** En el código deberán preverse reglas claras para la adhesión voluntaria de entidades, así como procedimientos de suspensión o exclusión en caso de incumplimiento;

38.6. **Supervisión independiente y eficaz:** Los órganos o mecanismos de supervisión establecidos en el código deberán contar con independencia funcional, procedimientos transparentes, recursos suficientes y competencias claras para garantizar el cumplimiento;

38.7. **Gestión de reclamaciones:** En el código se deberán asegurar canales accesibles y gratuitos para los titulares;

38.8. **Auditorías y control periódico:** Deberán preverse auditorías internas o externas periódicas y sistemas de reporte que permitan verificar, objetivamente, el cumplimiento del código de conducta;

38.9. Medidas correctivas: Se deberán establecer mecanismos correctivos en caso de incumplirse el código de conducta (como máxima medida se puede contemplar la exclusión);

38.10. Transparencia: Se deberá disponer la obligación de informar públicamente sobre el código aprobado, sus adherentes y los mecanismos de supervisión, para así asegurarles a los titulares el acceso a esta información;

38.11. Adaptabilidad: Deberán contemplar mecanismos de revisión y actualización periódica del código frente a los cambios tecnológicos, regulatorios o de prácticas sectoriales; y,

38.12. Cooperación institucional: Se deberá prever la coordinación y cooperación permanente con la SPDP y, cuando sea pertinente, con los organismos internacionales en la materia.

Art. 39.- Todo código de conducta deberá prever mecanismos adecuados y eficaces de supervisión, que podrán incluir:

39.1. Auditorías periódicas internas o externas;

39.2. Requisitos de presentación de informes de cumplimiento;

39.3. Procedimientos de gestión de reclamaciones de titulares;

39.4. Mecanismos de solución de conflictos;

39.5. Medidas correctivas específicas en caso de incumplimiento al código de conducta; y,

39.6. Canales para la denuncia de incumplimientos.

Los resultados de las auditorías e informes deberán ser puestos en conocimiento del órgano de supervisión del código de conducta, del responsable o encargado del tratamiento auditado y, en caso así ser requerido, a la SPDP.

Art. 40.- Sobre la base del análisis de fondo antes detallado, la IRD elaborará un informe técnico que contendrá la recomendación de aprobación del código de conducta o, de ser el caso, de modificación.

En caso de que se ordenare modificar el texto propuesto, el proponente que lo hubiese presentado tendrá el término de treinta (30) días para ajustar los textos a las normas vigentes y presentarlos a la SPDP. Si no se llegase a presentar el texto modificado, se archivará la solicitud de aprobación, sin perjuicio de que se pueda volver a presentar una nueva en el término de treinta (30) días contados desde que se notifique la resolución que dispone tal archivo.

Art. 41.- En caso de que el informe recomiende la aprobación del código de conducta, el expediente será remitido al Superintendente, quien dispondrá que la DAJ elabore el proyecto de resolución para que lo remita en el término de diez (10) días contado desde la fecha de la notificación de su disposición. Hecho lo anterior, el Superintendente expedirá una resolución motivada en virtud de la cual podrá:

41.1. Aprobar el código de conducta propuesto; o,

41.2. Negarlo, si no se cumplieren las condiciones establecidas.

Art. 42.- La resolución de aprobación será remitida a la IIT para su inscripción en el Registro Nacional de Protección de Datos de la Superintendencia de Protección de Datos Personales y publicada en el portal institucional, a fin de que la ciudadanía pueda conocer los instrumentos autorizados.

Art. 43.- Los códigos de conducta tendrán una vigencia de cuatro (4) años contados a partir de la resolución de aprobación; sin embargo, deberán ser revisados y, de ser necesario,

actualizados para garantizar su adecuación a las reformas normativas o cambios sustanciales o supervivientes en las operaciones de tratamiento que regulen.

Toda actualización deberá ser presentada ante la SPDP, que seguirá el procedimiento previsto en este capítulo.

Art. 44.- Los órganos de supervisión de cada código de conducta deberán cooperar activamente con la SPDP, para lo cual habrán de informar, cuando les fuere requerido, sobre su aplicación, los resultados de auditorías y las medidas correctivas implementadas.

La SPDP ejercerá sus facultades de supervisión y control de los códigos de conducta aprobados, para lo cual podrá requerir información, en cualquier momento, a través de la ICS.

CAPÍTULO VII
CERTIFICACIÓN

Art. 45.- Podrán acogerse a los procesos de certificación relativos a las transferencias o comunicaciones internacionales, los responsables o encargados del tratamiento que participen en transferencias o comunicaciones nacionales o internacionales de datos personales.

La certificación podrá referirse a operaciones específicas de tratamiento, a sistemas de gestión de protección de datos o a procesos determinados vinculados o relacionados con la transferencia o comunicación de datos personales.

Art. 46.- La certificación no eximirá al responsable, en ninguna circunstancia, de sus obligaciones legales en materia de protección de datos personales.

La certificación servirá como garantía adecuada en el marco de las transferencias o comunicaciones internacionales de datos personales, siempre y cuando cumplieren con las condiciones de validez establecidas en esta norma general y en la demás normativa aplicable que expidiere la SPDP.

Art. 47.- Las certificaciones expedidas en el marco de esta norma general serán reconocidas como garantías adecuadas, siempre y cuando cumplieren los requisitos establecidos en la normativa específica aplicable que, para el efecto, dictare la SPDP.

Art. 48.- Los responsables certificados estarán sujetos a la supervisión permanente de la SPDP, sin perjuicio de las auditorías o evaluaciones que deban realizar los organismos certificadores acreditados.

CAPÍTULO VIII
PROCEDIMIENTO PARA LA AUTORIZACIÓN DE TRANSFERENCIAS O COMUNICACIONES

Art 49.- Se regirán por el procedimiento establecido en este capítulo todas las transferencias o comunicaciones internacionales de datos personales que no se encuentren amparadas por una resolución de nivel adecuado de protección, o de garantías adecuadas reconocidas en esta norma general.

La obligación de solicitar autorización corresponderá al responsable del tratamiento o, de ser el caso, al encargado del tratamiento que ejecute la transferencia. En cualquier circunstancia, solamente la deberá solicitar quien realizare la transferencia o comunicación.

Art. 50.- La solicitud, dirigida a la SPDP, se presentará de manera física o electrónica a través del portal institucional. Aquella deberá contener:

50.1. Identificación de intervinientes y destino: Datos completos del responsable del tratamiento establecido en el Ecuador; país de destino, organización internacional, persona jurídica o territorio económico internacional que será el receptor de los datos;

50.2. Justificación legal y técnica: Exposición de la necesidad, finalidad y proporcionalidad de la transferencia o comunicación respecto de la causal aplicada o invocada;

50.3. Análisis de riesgos: Para cada transferencia o comunicación de datos personales, y en todos los casos, se deberá realizar y ejecutar un análisis de riesgos que incluirá su resultado;

50.4. Evaluación de impacto: En todos los casos se deberá realizar, en forma obligatoria, una evaluación de impacto, además de señalarse las medidas de mitigación correspondientes;

50.5. Medidas de seguridad: Descripción detallada de las medidas técnicas, organizativas, administrativas y jurídicas aplicadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales transferidos;

50.6. Instrumento contractual: Copia del contrato o del acuerdo de transferencia o comunicación con el destinatario, el cual deberá contener las obligaciones correspondientes establecidas en la LOPDP, el RGLOPDP, especialmente las de garantizar los derechos de los titulares de datos personales; establecer las medidas de seguridad para garantizar la transferencia de datos personales con las mayores medidas de seguridad posibles y posibles para cada caso concreto; sometimiento de todo tratamiento a la normativa y jurisdicción de la República del Ecuador, entre otras;

50.7. Consentimiento del titular y vías de reclamación: Certificación del responsable de haber solicitado el consentimiento al titular respecto a la transferencia o comunicación, así como de haberle informado la finalidad del tratamiento, sus derechos, los mecanismos eficaces de reclamación y tutela, los contactos del delegado de protección de datos personales y la información de los posibles riesgos;

50.8. Supuestos del RGLOPDP: Acreditar que se encuentra en uno de los dos supuestos del artículo 77 del RGLOPDP; y,

50.9. Motivación de imposibilidad: Explicación motivada acerca de la imposibilidad de cumplir la transferencia internacional de datos personales por garantías adecuadas o por nivel adecuado de protección.

Art. 51.- La IRD realizará una evaluación integral y rigurosa de la solicitud, para lo cual tendrá el plazo de tres (3) meses contados a partir de que la solicitud hubiese sido recibida en forma completa, considerando la totalidad de la información y la documentación presentada, y con la previa verificación de que se cumplen los requisitos señalados en el artículo anterior.

En caso de advertirse omisiones o incumplimientos, se concederá al solicitante el término improrrogable de treinta (30) días para su subsanación, con la condición de que, de no hacerlo, se dispondrá el archivo del expediente y de la solicitud presentada, sin perjuicio de que la pueda volver a presentar después de transcurrido el plazo de un (1) mes contado desde la notificación de tal archivo.

Art. 52.- La IRD elaborará un informe técnico que deberá contener, como mínimo, lo siguiente:

52.1. Antecedentes;

52.2. Base legal;

52.3. Identificación de los datos personales a transferirse o comunicarse, lo que incluye el tipo de datos y su categoría, destinatario, país al que se transfieren, finalidad;

52.4. Análisis de verificación del cumplimiento de los requisitos;

52.5. Justificación de la aceptación o del rechazo de la autorización;

52.6. Conclusiones; y,

52.7. Recomendaciones.

Art. 53.- El expediente será enviado al Superintendente, quien dispondrá que la DAJ elabore el proyecto de resolución para que lo prepare y remita en el término de diez (10) días contado desde la fecha de la notificación de su disposición. Hecho lo anterior, el Superintendente expedirá una resolución motivada en virtud de la cual podrá autorizar o rechazar la solicitud. La resolución será notificada al solicitante de conformidad con las normas del procedimiento administrativo aplicables.

Art. 54.- Expedida y notificada la resolución aprobatoria, será remitida a la IIT para su inscripción en el Registro Nacional de Protección de Datos, con el objeto de facilitar su disponibilidad para la ciudadanía.

Art. 55.- Una vez otorgada la autorización, el responsable del tratamiento estará sujeto a las siguientes obligaciones:

55.1. Notificar los incidentes de seguridad a la SPDP de acuerdo con lo establecido en la LOPDP; y,

55.2. Informarle a la SPDP los cambios materiales que se produjeren respecto de las condiciones de la transferencia o comunicación, el contrato suscrito con el destinatario o los cambios normativos en el país de destino que pudieren afectar a la protección de los datos personales.

Art. 56.- En circunstancias excepcionales, las resoluciones de autorización para las transferencias o comunicaciones internacionales tendrán una vigencia específica que será establecida en función de las finalidades de cada caso concreto; vigencia que no podrá ser mayor a un (1) año. Dicha autorización, bajo ningún caso, podrá ser otorgada por un tiempo indefinido.

La SPDP podrá ejercer sus facultades de control en caso de que lo considere necesario, o de que se llegase a tener indicios de incumplimiento de las garantías a los derechos de protección de datos personales de los titulares. Para tal efecto, la SPDP podrá revocar la autorización en forma directa.

Una vez emitida la resolución de revocatoria, deberán cesar, de manera inmediata, las transferencias o comunicaciones hacia el país, organización internacional, persona jurídica o territorio económico internacional, salvo que las transferencias o comunicaciones se encontraren amparadas en garantías adecuadas o en otros fundamentos previstos en la normativa de protección de datos personales.

La revocatoria se publicará en la página web institucional y surtirá efectos desde su notificación, aunque sin retroactividad respecto de las transferencias o comunicaciones realizadas de manera anterior.

Art. 57.- Para la revisión o, en su caso, para la revocatoria de las resoluciones de aprobación de las transferencias y comunicaciones, se cumplirá el siguiente procedimiento:

57.1. Inicio del procedimiento: La ICS podrá iniciar, de oficio o a petición de parte, el procedimiento de revisión y posible revocatoria cuando existieren indicios razonables de incumplimiento de los requisitos de la solicitud que se presentó para obtener la autorización.

Sobre la base de tales indicios, la ICS deberá verificar la existencia del incumplimiento mediante el inicio de una actuación previa. Concluido dicho proceso, y de verificarse que el responsable o encargado se encuentra en una causal de revocatoria o ha incumplido la normativa de protección de datos personales, se

remitirá a la IRD un informe técnico en el que evidenciará cuál ha sido el incumplimiento constatado.

Si el incumplimiento fuere de aquellos constitutivos de infracción de acuerdo con la LOPDP, la ICS podrá continuar con la actuación previa y, eventualmente, disponer que se implementen medidas correctivas.

57.2. Causales de revocatoria: Constituyen causales de revocatoria cualquiera de las siguientes:

57.2.1. El incumplimiento de las condiciones mínimas previstas en la LOPDP, el RGLOPDP, esta norma general y la demás normativa que emitiere la SPDP;

57.2.2. La comprobación de vulneraciones de datos personales;

57.2.3. La ausencia o ineficacia de mecanismos de tutela de los derechos de los titulares de datos personales;

57.2.4. El incumplimiento o la inobservancia, por parte del destinatario, de aquellas obligaciones contractuales que debe contraer con el responsable del tratamiento y que le compelen:

57.2.4.1. A acatar la normativa de protección de datos personales ecuatoriana, así como las resoluciones expedidas por la SPDP;

57.2.4.2. A abstenerse de presentar oposición, manifestar rechazo o argumentar la incompetencia de la SPDP o la falta de jurisdicción de los jueces, tribunales y cortes ecuatorianos; y,

57.2.4.3. A hacer efectivo que, en el país donde se encontrare establecido, se garantice el derecho de protección de datos personales de los titulares o el derecho a la tutela judicial efectiva en materia de protección de datos personales.

57.2.5. La existencia de resoluciones internacionales o informes que evidencien deficiencias estructurales en el régimen de protección de datos aplicable al destinatario.

57.3. Informe técnico: Una vez recibida la documentación, la IRD tendrá el plazo de tres (3) meses para emitir un informe técnico que recomiende revocar o ratificar la autorización. A base de la documentación obtenida, la IRD elaborará un informe técnico motivado que establecerá si se ratifica la autorización o si se la revoca.

57.4. Resolución: Se le notificará al Superintendente con el informe técnico que recomiende la revocatoria o la rectificación, quien dispondrá que la DAJ elabore el proyecto de resolución correspondiente para que lo remita en el término de diez (10) días contado desde la fecha de la notificación de su disposición. Hecho lo anterior, el Superintendente expedirá una resolución motivada en virtud de la cual podrá:

57.4.1. Ratificar la autorización; o,

57.4.2. Revocarla.

57.5. Efectos de la revocatoria: Emitida la resolución de revocatoria, el responsable del tratamiento deberá cesar inmediatamente las transferencias o comunicaciones internacionales, salvo que pudieren sustentarse en otro mecanismo legal previsto en la LOPDP.

57.6. Registro y publicidad: La resolución de revocatoria será notificada al responsable del tratamiento y a la IIT para su registro y publicación en el portal institucional de la SPDP, con el objeto de facilitar su disponibilidad para la ciudadanía.

Art. 58.- A través de la ICS, y mientras se lleve a cabo el proceso de revisión o revocatoria, la SPDP podrá disponer, mediante resolución motivada, la suspensión temporal de la autorización de transferencia internacional, siempre y cuando existieren indicios razonables de que no se están asegurando los niveles de protección equivalentes a los previstos en la LOPDP y el RGLOPDP.

La suspensión tendrá carácter preventivo y se mantendrá vigente hasta la conclusión del procedimiento de revisión o revocatoria correspondiente.

Durante el período de suspensión, el responsable del tratamiento no podrá ampararse en la autorización ya suspendida para realizar nuevas transferencias o comunicaciones internacionales. Las transferencias o comunicaciones efectuadas de forma previa a la suspensión serán objeto de un control posterior o *ex post facto*.

TÍTULO IV
FLUJOS TRANSFRONTERIZOS, MECANISMOS DE TRANSPARENCIA, REGISTRO Y REGULARIZACIÓN

CAPÍTULO I
RÉGIMEN ESPECIAL "INTRA-CAN" PARA LA COMUNIDAD ANDINA

Art. 59.- Las transferencias o comunicaciones internacionales hacia los países miembros de la Comunidad Andina se considerarán, por mandato comunitario, como flujos transfronterizos de datos personales y, en consecuencia, dichos Estados serán reconocidos como países con nivel adecuado de protección sin necesidad de evaluación adicional por parte de la SPDP, salvo que se verificaren deficiencias graves en el cumplimiento de la normativa comunitaria o nacional que fuere aplicable.

Art. 60.- En las transferencias o comunicaciones de datos personales realizadas dentro de la Comunidad Andina, el responsable del tratamiento deberá garantizarle al titular el derecho a la información en los términos del artículo 12 de la LOPDP, especialmente en relación a:

60.1. La identidad del responsable y el destinatario;

60.2. La categoría y los tipos de datos personales transferidos o comunicados;

60.3. La finalidad de la transferencia o comunicación;

60.4. La duración del tratamiento; y,

60.5. La posibilidad de revocar el consentimiento en cualquier momento.

Art. 61.- Los responsables y encargados del tratamiento que realizaren transferencias bajo el régimen especial Intra-CAN, deberán adoptar y acreditar la adopción de medidas documentales que demuestren el cumplimiento de las obligaciones de protección de datos, incluidos contratos, políticas internas, análisis de riesgos, evaluaciones de impacto y reportes de seguridad.

Art. 62.- Cada bienio la SPDP elaborará un informe consolidado sobre el estado de las transferencias internacionales dentro de la Comunidad Andina, incluidas las estadísticas, las vulneraciones reportadas y las medidas adoptadas. Este informe será remitido a la Secretaría General de la CAN para efectos de supervisión y cooperación regional.

Art. 63.- Si la SPDP detectare o determinare que un Estado miembro de la Comunidad Andina incumple con las garantías de protección de datos previstas en la Decisión N° 897, iniciará un proceso de verificación de acuerdo con el procedimiento de evaluación de país adecuado y, de ser lo procedente, podrá recomendarle al Consejo Andino de Ministros de

Relaciones Exteriores la adopción de medidas correctivas, sin perjuicio de ejercer sus facultades de control posterior o *ex post facto* dentro de la República del Ecuador.

CAPÍTULO II
REGISTRO Y TRANSPARENCIA

Art. 64.- Los responsables o encargados del tratamiento que realizaren transferencias internacionales de datos personales deberán inscribirlas, obligatoriamente, en el Registro Nacional de Protección de Datos, de conformidad con las siguientes reglas:

64.1. Información sujeta a registro: Todas las transferencias o comunicaciones internacionales de datos personales se sujetarán estrictamente a lo dispuesto en el artículo 78 del RGLOPDP.

64.2. Transferencias sujetas a inscripción individual: Se inscribirán, caso por caso, las transferencias o comunicaciones internacionales realizadas basadas en:

64.2.1. Las autorizaciones conferidas para casos excepcionales; y,

64.2.2. Flujos transfronterizos realizados bajo régimen especial Intra-CAN.

Para las trasferencias o comunicaciones sujetas a inscripción individual, la inscripción deberá realizarse con un término mínimo de diez (10) días previo a la operación; y, en caso de transferencias o comunicaciones continuas, desde el inicio de su ejecución.

64.3. Transferencias o comunicaciones sujetas a reporte agregado: Las operaciones de transferencias o comunicaciones realizadas hacia países, organizaciones internacionales, personas jurídicas o territorios económicos internacionales con nivel adecuado de protección reconocido por la SPDP, o que se efectuaren mediante la implementación de garantías adecuadas, no requerirán inscripción individual. En estos casos, el responsable o encargado del tratamiento deberá presentarle un reporte consolidado anual a la SPDP, dentro del primer trimestre de cada año, que incluya las salvaguardias adoptadas en pro de los derechos y libertades de los titulares, así como los demás elementos establecidos en el artículo 78 del RGLOPDP.

Art. 65.- La inscripción o reporte será requisito para acreditar la licitud de la transferencia o comunicación. La SPDP podrá verificar la veracidad de la información, solicitar aclaraciones y requerir documentación adicional en el marco de sus facultades de control.

Art. 66.- La SPDP publicará en su portal electrónico un extracto del Registro Nacional de Transferencias Internacionales, que contendrá el nombre del país, organización internacional, persona jurídica o territorio económico internacional hacia los cuales se hubieren realizado transferencias internacionales o comunicaciones.

La publicación no incluirá información sensible, datos personales, secretos empresariales ni otros elementos que pudieren comprometer la seguridad de los titulares o de los responsables y encargados del tratamiento.

CAPÍTULO III
ACUERDOS DE ENTENDIMIENTO CON INSTITUCIONES DE EDUCACIÓN SUPERIOR

Art. 67.- Los acuerdos de entendimiento son los instrumentos jurídicos de cooperación interinstitucional —celebrados entre la SPDP, a través de la IRD, y las instituciones de educación superior— que tienen por objeto exclusivo la preparación de informes técnicos acerca del nivel de protección de datos personales que tienen los países, las organizaciones internacionales, las personas jurídicas o los territorios económicos internacionales; todo ello con miras al posible reconocimiento del nivel adecuado de protección o, en su caso, para la revisión o revocatoria del nivel adecuado de protección que ya estuviere reconocido.

Art. 68.- La necesidad de suscribir un acuerdo de entendimiento podrá originarse de oficio o a petición de parte, siempre que se identifique la necesidad y el interés de la institución de educación superior.

Art. 69.- Para la suscripción de un acuerdo de entendimiento se seguirá el siguiente procedimiento:

69.1. Informe técnico de necesidad: La IRD elaborará un informe técnico de necesidad, que contendrá, al menos, lo siguiente:

69.1.1. Antecedentes y justificación del acuerdo de entendimiento;

69.1.2. Procedencia y necesidad de la suscripción del acuerdo de entendimiento;

69.1.3. País, organización internacional, persona jurídica o territorio económico internacional que será objeto de evaluación por parte institución de educación superior;

69.1.4. Objeto del acuerdo de entendimiento;

69.1.5. Metodología propuesta;

69.1.6. Alcance previsto;

69.1.7. Cronograma de ejecución;

69.1.8. Obligaciones y compromisos de la institución de educación superior; y,

69.1.9. Recomendación expresa sobre la procedencia o no de suscribir el acuerdo.

69.2. Determinación: De oficio, la IRD iniciará el procedimiento para la suscripción del acuerdo de entendimiento, siempre y cuando verifique, en su informe técnico de necesidad, la idoneidad de contar con un estudio técnico sobre el nivel adecuado de protección de datos personales en un país, organización internacional, persona jurídica o territorio económico internacional.

69.3. Presentación de la solicitud a la institución de educación superior: Con el objeto de comunicar la necesidad de suscribir el acuerdo de entendimiento, la IRD le cursará a la institución de educación superior una solicitud en la que constará la propuesta de suscripción y su finalidad.

69.4. Contestación de la institución de educación superior: La institución de educación superior dispondrá de un término de veinte (20) días para responder, afirmativa o negativamente, la solicitud cursada por la SPDP. Vencido el término, la falta de respuesta expresa se la tendrá como negativa.

Si se aceptare la solicitud, la SPDP preparará y remitirá el proyecto del acuerdo de entendimiento a la institución de educación superior.

Desde la fecha del envío del proyecto empezará a discurrir un término de sesenta (60) días para suscribir el acuerdo de entendimiento, incluido el tiempo que las partes empleen en las revisiones y los ajustes que quisieren realizarle al texto del borrador. En caso de que no se suscribiere el acuerdo de entendimiento dentro del término señalado, se entenderá que las partes han desistido de celebrarlo.

69.5. Contenido del acuerdo de entendimiento: El acuerdo de entendimiento contendrá el siguiente clausulado:

69.5.1. Antecedentes;

69.5.2. Objeto;

69.5.3. Obligaciones;

69.5.4. Responsabilidades;

69.5.5. Acuerdo de confidencialidad;

69.5.6. Acuerdo de tratamiento adecuado de datos personales;

69.5.7. Vigencia;

69.5.8. Plazo para el cumplimiento de la entrega del informe técnico del país, la organización internacional, la persona jurídica o el territorio económico internacional que es objeto del análisis; y,

69.5.9. Aceptación y firmas.

69.6. Suscripción: Una vez autorizado, el acuerdo de entendimiento será suscrito por el Intendente General de Regulación de Protección de Datos Personales (o por el funcionario delegado de la IRD) y el representante legal o convencional de la institución de educación superior.

Art. 70.- La institución de educación superior deberá entregar el informe técnico debidamente sustentado en un plazo máximo de noventa (90) días contado desde la suscripción del acuerdo de entendimiento, salvo que en el instrumento se hubiere estipulado un plazo diferente por razones justificadas.

En el informe técnico se deberá concluir si el país, organización internacional, persona jurídica o territorio económico internacional evaluado tiene o no un nivel adecuado de protección de datos personales.

Art. 71.- Los informes técnicos tendrán carácter consultivo y servirán como fuentes en los procedimientos de reconocimiento, revisión o revocatoria de niveles adecuados de protección, sin que por ello se sustituya la competencia exclusiva de la IRD.

Art. 72.- Las instituciones de educación superior podrán solicitar, a través de su representante legal, la suscripción de un acuerdo de entendimiento con la SPDP a través de la IRD, para cooperar en la investigación y análisis internacional sobre el nivel adecuado de protección de datos personales de un país, organización internacional, persona jurídica o territorio económico internacional.

La solicitud así presentada será tramitada de acuerdo con el siguiente procedimiento:

72.1. Solicitud de cooperación interinstitucional: La petición, debidamente motivada, será dirigida al Superintendente. Junto con la solicitud deberán presentarse los siguientes documentos:

72.1.1. Acreditación de la representación de quien suscribe la solicitud, para lo cual se adjuntará una copia certificada del acta de designación, nombramiento, poder o cualquier otro documento equivalente;

72.1.2. Certificado de inscripción en el Registro Único de Contribuyentes;

72.1.3. Dirección de correo electrónico para notificaciones; y,

72.1.4. Los demás documentos que la naturaleza del acuerdo requiriese.

72.2. Calificación de la solicitud: La IRD calificará la solicitud dentro del término de veinte (20) días contados a partir haber sido recibida, para lo cual verificará el cumplimiento de los requisitos formales y la pertinencia del pedido.

72.3. Subsanación: Si se detectaren omisiones, inconsistencias o falta de requisitos o documentos, la IRD se lo hará saber a la institución solicitante mediante notificación, para lo cual le concederá un término de treinta (30) días con el objeto de que proceda a subsanar lo que corresponda. Vencido el término, la solicitud será archivada de no haberse subsanado, aunque podrá presentarse nuevamente.

72.4. Informe técnico de necesidad: Una vez admitida la solicitud, la IRD elaborará un informe técnico de necesidad, dentro del término de treinta (30) días, que contendrá:

72.4.1. Antecedentes y justificación del acuerdo de entendimiento;

72.4.2. Procedencia y necesidad de la suscripción del acuerdo de entendimiento;

72.4.3. País, organización internacional, persona jurídica o territorio económico internacional solicitado para la evaluación de la institución de educación superior;

72.4.4. Objeto del acuerdo de entendimiento;

72.4.5. Metodología propuesta;

72.4.6. Alcance previsto;

72.4.7. Cronograma de ejecución;

72.4.8. Obligaciones y compromisos de la institución de educación superior; y,

72.4.9. Recomendación expresa sobre la procedencia o no de la suscripción del acuerdo.

72.5. Aprobación del acuerdo de entendimiento: Una vez realizado el informe técnico de necesidad, será remitido al Superintendente junto con el proyecto del acuerdo de entendimiento.

El Superintendente dispondrá que la DAJ elabore el proyecto de resolución, el cual deberá ser remitido a la máxima autoridad en el término de cinco (5) días. A base de dicho proyecto, el Superintendente podrá expedir una resolución motivada para aprobar o, en su caso, negar la suscripción del acuerdo de entendimiento. En todo caso, dicha resolución será notificada a la institución solicitante.

Si se negare la suscripción del acuerdo de entendimiento, se dispondrá el archivo de la solicitud sin perjuicio de poder volverla a presentar.

72.6. Suscripción del acuerdo de entendimiento: Una vez revisado y aprobado, el acuerdo de entendimiento será suscrito por el Intendente General de Regulación de Protección de Datos Personales (o por el funcionario delegado de la IRD) y el representante legal o convencional de la institución de educación superior, dentro de un término no mayor a veinte (20) días contados desde la notificación de la aprobación.

En caso de que no se suscribiere el acuerdo de entendimiento dentro del término señalado, se entenderá que las partes han desistido de celebrarlo.

Art. 73.- La institución de educación superior deberá entregar el informe técnico debidamente sustentado en un plazo máximo de noventa (90) días contado desde la suscripción del acuerdo de entendimiento, salvo que en el instrumento se hubiere estipulado un plazo diferente por razones justificadas.

Art. 74.- Los informes técnicos tendrán carácter consultivo y servirán como referencias en los procedimientos de reconocimiento, revisión o revocatoria de niveles adecuados de protección, sin que por ello se sustituya la competencia exclusiva de la IRD.

DISPOSICIONES TRANSITORIAS

Primera.- Las transferencias o comunicaciones internacionales de datos personales efectuadas con anterioridad a la vigencia de la LOPDP, o realizadas antes de la vigencia de esta norma general, deberán acogerse al siguiente procedimiento de regularización:

1.a. Notificación inicial: Dentro de los doce (12) meses posteriores a la vigencia de esta norma general, los responsables y encargados del tratamiento deberán notificarle a la SPDP la existencia de transferencias o comunicaciones internacionales previas, para lo cual especificarán:

1.a.1. País o entidad destinataria;

1.a.2. Categorías de datos transferidos;

1.a.3. Finalidad de la transferencia o comunicación; y,

1.a.4. Instrumento jurídico o práctica vigente que acredite la transferencia o comunicación.

1.b. Presentación del plan de adecuación: La notificación incluirá un plan de adecuación que contendrá:

1.b.1. Medidas de control y mitigación de riesgos adoptadas durante el período transitorio;

1.b.2. Mecanismo mediante el cual se ajustará la transferencia o comunicación ya sea por nivel adecuado, garantías adecuadas, o supuestos excepcionales; y,

1.b.3. Plazo máximo de implementación.

La IRD acusará recibo de la recepción de la información antes señalada; sin embargo, no será necesaria la emisión de ningún acto administrativo para ejecutar el presente proceso. En caso de que, por la información remitida, se pudiere presumir la existencia de riesgos respecto de una transferencia o comunicación internacional, la IRD elaborará un informe técnico motivado e iniciará las actividades que considere necesarias.

Segunda.- Mientras discurran los doce (12) meses posteriores a la vigencia de esta norma general, no se impondrán sanciones por incumplimiento de la obligación de regularización, siempre que los responsables y encargados del tratamiento:

2.a. Cumplieren con la notificación inicial prevista en el apartado 1.a. de la primera disposición transitoria;

2.b. Presentaren, ante la SPDP, el plan de adecuación respectivo; y,

2.c. Ejecutaren las medidas contempladas en dicho plan de adecuación.

Tercera.- Transcurrido el plazo para acogerse al procedimiento de regularización, las transferencias o comunicaciones internacionales de datos personales realizadas con anterioridad a la entrada en vigencia de la LOPDP que no se hubiesen regularizado, estarán sujetas a las sanciones y medidas correctivas establecidas en la normativa exigible, sin perjuicio de las demás responsabilidades que fueren aplicables de acuerdo con el ordenamiento jurídico vigente.

Cuarta.- La IIT implementará el Registro Nacional de Datos Personales y el portal electrónico correspondiente en un plazo máximo de doce (12) meses contados a partir de la vigencia de este norma general.

DISPOSICIÓN FINAL

Esta resolución entrará en vigencia a partir de su publicación en el Registro Oficial.

Dada y firmada en Quito, D. M., el 28 de enero del 2026.

Firmado electrónicamente por:
FABRIZIO ROBERTO PERALTA DIAZ
Validar únicamente con FirmaEC

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

ANEXO 1

Cláusulas Contractuales Modelo-Tipo de la Red Iberoamericana de Protección de Datos Personales:

ACUERDO MODELO DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES ENTRE RESPONSABLE Y RESPONSABLE:

Las Partes del Contrato han acordado el presente Acuerdo basado en cláusulas contractuales modelo:

PRIMERA PARTE:

CUESTIONES GENERALES

Cláusula 1.

Finalidad, partes, ámbito de aplicación y definiciones

1.1. Finalidad

La finalidad de las presentes cláusulas contractuales modelo es garantizar y facilitar el cumplimiento de los requisitos previstos por la Ley aplicable para la transferencia internacional de Datos personales, a fin de cumplir los principios y deberes en la protección de los Datos personales y los derechos de los Titulares.

a. Cualquier interpretación del presente Acuerdo deberá tener en cuenta estos fines.

1.2. Partes del contrato

a. Las Partes del contrato son el Exportador de datos y el Importador de datos.

b. El presente Acuerdo permite la incorporación de importadores o exportadores adicionales como Partes mediante el formulario del Anexo A siguiendo el procedimiento previsto en la Cláusula 5.

1.3. Ámbito de aplicación

a. El presente Acuerdo se aplicará a las transferencias internacionales de Datos personales realizadas entre el Exportador de datos y el Importador de datos de conformidad con las especificaciones del Anexo B.

b. Todos los anexos forman parte del presente Acuerdo.

1.4. Definiciones

a. Los términos definidos se identifican en este Acuerdo con su inicial en mayúscula.

b. A los fines del presente Acuerdo se entenderá por

Acuerdo: El presente contrato de transferencia internacional de Datos personales basado en las cláusulas contractuales modelo junto con su caratula y sus anexos.

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, servicios, organismo o prestador de ser- vicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

Importador de datos: Persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios 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, 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.

Sub encargado: Cuando un Encargado del tratamiento recurre a otro Encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del Responsable

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 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.

Cláusula 2.

Efectos e invariabilidad de las cláusulas

2.1. Modificación de las cláusulas modelo. Límites

El presente Acuerdo basado en cláusulas modelo establece garantías adecuadas para el Titular en relación con las transferencias de datos de Responsables a Encargados, siempre que las Cláusulas no se modifiquen en su esencia respecto al modelo original, salvo para completar la carátula y los anexos. Esto no es óbice para que las Partes incluyan en un contrato más amplio las cláusulas contractuales modelo, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, a las presentes cláusulas contractuales modelo ni perjudiquen los derechos del Titular.

2.2. Jerarquía con la Ley Aplicable. Interpretación

a. El presente Acuerdo deberá leerse e interpretarse con arreglo a las disposiciones de la Ley Aplicable.

b. Las Partes podrán añadir nuevas definiciones de términos, resguardos y garantías adicionales en las presentes cláusulas modelo cuando ello resulte necesario para cumplir con la Ley aplicable y siempre y cuando ello no suponga un detrimento a las protecciones otorgadas por las cláusulas modelo.

c. El presente Acuerdo no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en la Ley aplicable.

d. El presente Acuerdo se entiende sin perjuicio de las obligaciones a las que esté sujeto el Exportador de datos en virtud de su legislación o de la Ley aplicable.

2.3. Jerarquía con otros acuerdos

En caso de contradicción entre el presente Acuerdo y las disposiciones de acuerdos conexos entre las Partes se establece que las cláusulas del presente Acuerdo prevalecerán.

Cláusula 3.

Terceros Beneficiarios

Los Titulares podrán invocar, como Terceros beneficiarios, las cláusulas del presente Acuerdo contra el Exportador de datos y/o el Importador de datos y exigirles su cumplimiento.

Cláusula 4.

Descripción de la transferencia o transferencias, y sus finalidades

Los detalles y características de la transferencia o las transferencias y, en particular, las categorías de Datos personales que se transfieren y las finalidades para los que se transfieren se detallan en el Anexo B del presente Acuerdo.

Cláusula 5.

Cláusula de incorporación

a. Las Partes aceptan que cualquier entidad que no sea parte en el presente Acuerdo podrá, previo consentimiento de todas las Partes intervinientes, adherirse al presente Acuerdo en cualquier momento, ya sea como Exportador de datos o como Importador de datos firmando el modelo del anexo A, y completando los demás Anexos si corresponde.

b. Cuando haya firmado el Anexo A y completado los demás anexos en caso de que corresponda, la entidad que se adhiera se considerará Parte del presente Acuerdo y tendrá los derechos y obligaciones de un Exportador de datos o un Importador de datos, según la categoría en la que se haya adherido al Acuerdo según lo indicado en el Anexo A.

c. La entidad que se sume al Acuerdo no adquirirá derechos y obligaciones del presente Acuerdo derivados del período anterior a su adhesión.

SEGUNDA PARTE:

OBLIGACIONES DE LAS PARTES

Cláusula 6

Garantías en materia de protección de datos

6.1. Principio de responsabilidad

a. El Exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el Importador de datos puede, aplicando Medidas administrativas, físicas y técnicas adecuadas, cumplir las obligaciones que le atribuye el presente Acuerdo.

b. El Importador de datos implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en el presente Acuerdo, así como rendirá cuentas sobre el tratamiento de Datos personales en su posesión al Titular y a la Autoridad de control competente.

c. El Importador de datos revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento presente Acuerdo.

6.2. Principio de finalidad

a. El Importador de datos no podrá tratar los Datos personales objeto de este Acuerdo para finalidades distintas a aquéllas indicadas en el Anexo B.

b. Solo podrá tratar los Datos personales con otros fines: (i) cuando haya recabado el consentimiento previo del Titular; (ii) cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; (iii) cuando el tratamiento sea necesario para proteger intereses vitales del Titular o de otra persona física.

6.3.Transparencia

a. A fin de que los Titulares puedan ejercer de forma eficaz los derechos que les otorga este Acuerdo, el Importador de datos les informará, directamente o a través del Exportador de datos: (i) de su identidad y datos de contacto; (ii) de las categorías de Datos personales procesados y sus finalidades; (iii) del derecho a solicitar en forma gratuita una copia del presente Acuerdo; (iv) cuando tenga la intención de realizar Transferencias ulteriores de los Datos personales a terceros, del destinatario o de las categorías de destinatarios y su finalidad.

b. Lo dispuesto no será de aplicación cuando el Titular ya disponga de la información o cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado para el Importador de datos.

c. En caso de que se solicite una copia del Acuerdo, las Partes podrán excluir aquellas secciones o anexos del Acuerdo que tengan secretos comerciales u otro tipo de información confidencial tales como Datos personales de terceros o información reservada en términos de la normatividad de las Partes.

6.4. Exactitud y minimización de datos

a. Las Partes se asegurarán de que los Datos personales sean exactos y, cuando proceda, estén actualizados. El Importador de datos adoptará todas las medidas razonables

para que se supriman o rectifiquen sin dilación los Datos personales que sean inexactos con respecto a los fines para los que se tratan.

b. Si una de las Partes tiene conocimiento de que los Datos personales que ha transferido o recibido son inexactos o han quedado obsoletos, informará de ello a la otra parte sin dilación indebida.

c. El Importador de datos se asegurará de que los Datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento.

6.5. Limitación del plazo de conservación

a. El Importador de datos no conservará los Datos personales más tiempo del necesario para los fines para los que se procesen.

b. El Importador de datos establecerá las medidas administrativas, físicas y técnicas adecuadas para garantizar el cumplimiento de esta obligación, tales como la supresión o anonimización de los datos y de todas las copias de seguridad al finalizar el período de conservación.

6.6. Principio de Seguridad

a. El Importador de datos y, durante la transferencia, también el Exportador de datos establecerán y mantendrán medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los Datos personales objeto de este Acuerdo.

   Para la determinación de las medidas de seguridad, el Importador de datos considerará los siguientes factores:

   i. El riesgo para los derechos y libertades de los Titulares. en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los Datos personales tratados para una tercera persona no autorizada para su posesión.

   ii. El estado de la técnica.

   iii. Los costos de aplicación.

   iv. La naturaleza de los Datos personales tratados, en especial si se trata de Datos personales sensibles.

   v. El alcance, contexto y las finalidades del tratamiento.

   vi. Las posibles consecuencias que se derivarían de una vulneración para los titulares.

   vii. Las vulneraciones previas ocurridas en el tratamiento de Datos personales.

b. Las Partes han acordado las Medidas administrativas, físicas y técnicas que figuran en el Anexo C al presente Acuerdo para los Datos personales objeto de la transferencia internacional.

c. El Importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

Vulneración a la seguridad de los datos personales

a. En caso de Vulneración de la seguridad de los datos personales tratados por el Importador de datos en virtud del presente Acuerdo, el Importador de datos adoptará las medidas adecuadas para ponerle remedio y para mitigar los posibles efectos negativos.

b. El Importador de datos documentará todos los hechos pertinentes relacionados con la vulneración de la seguridad de los datos personales, como sus efectos y las medidas correctivas adoptadas, y llevará un registro de las mismas.

c. Cuando alguna de las Partes tenga conocimiento de una Vulneración de seguridad de datos, notificará a la otra Parte, a la Autoridad de control competente y a los Titulares afectados dicho acontecimiento, sin dilación alguna y a más tardar dentro de un plazo no mayor a cinco (5) días.

d. La notificación que se realice en virtud del párrafo anterior estará redactada en un lenguaje claro y sencillo.

   La referida notificación contendrá, al menos, la siguiente información:

   i. La naturaleza del incidente.

   ii. Los Datos personales comprometidos.

   iii. Las acciones correctivas realizadas de forma inmediata.

   iv. En el caso de la notificación al Titular, las recomendaciones a estos sobre las medidas que éste pueda adoptar para proteger sus intereses.

   v. Los medios disponibles al Titular para obtener mayor información al respecto

e. En la medida en que el Importador de datos no pueda proporcionar toda la información al mismo tiempo, podrá hacerlo por fases sin más dilaciones indebidas.

f. La notificación a los Titulares no será necesaria cuando dicha notificación suponga un esfuerzo desproporcionado. En este caso, el Importador de datos realizará una comunicación pública o adoptará una medida semejante para informar al público de la Vulneración de seguridad de dato.

6.7. Tratamiento bajo la autoridad del Importador de datos y principio de confidencialidad

a. El Importador de datos se asegurará de que las personas que actúen bajo su autoridad solo traten los datos siguiendo instrucciones del Importador de datos, y establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el Exportador de datos.

b. El Importador de datos garantizará que las personas autorizadas para tratar los Datos personales se hayan comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza legal.

6.8. Tratamiento de Datos personales sensibles

a. En la medida que la transferencia incluya Datos personales sensibles, el Importador de datos aplicará restricciones específicas y garantías adicionales adaptadas a la naturaleza específica de los datos y el riesgo especial de que se trate.

b. Estas medidas pueden consistir en, por ejemplo, la reducción del personal autorizado a acceder a los Datos personales, acuerdos de confidencialidad especiales, medidas de seguridad adicionales (como la Anonimización) y/o restricciones adicionales con respecto a la comunicación ulterior.

c. En la medida que la transferencia incluya Datos personales concernientes a niñas, niños y adolescentes, las Partes privilegiarán la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales.

6.9. Transferencias ulteriores

a. El Importador de datos solo podrá comunicar los Datos personales a terceros situados fuera de la jurisdicción del Exportador de datos si el tercero está vinculado por el presente Acuerdo o consiente someterse a este. De no ser así, el Importador de datos solo podrá efectuar una Transferencia ulterior solamente si:

   i. Para el caso que la Ley Aplicable así lo disponga, esta transferencia ulterior va dirigida a un país que ha sido objeto de una declaración de adecuación de su nivel de protección de datos personales con arreglo a lo dispuesto en la Ley Aplicable, siempre que tal declaración cubra la Transferencia ulterior;

   ii. El tercero destinatario de la Transferencia ulterior aporta de algún modo garantías adecuadas, con arreglo a lo dispuesto en la Ley aplicable, respecto a los Datos personales sujetos a la Transferencia ulterior;

   iii. El tercero suscribe un instrumento vinculante con el Importador de datos que garantice el mismo nivel de protección de datos que el del presente Acuerdo, y el Importador de datos entrega una copia de estas garantías al Exportador de datos;

   iv. La Transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

   v. Si es necesario para proteger intereses vitales del Titular o de otra persona física; o

   vi. De no concurrir las demás condiciones, el Importador de datos ha recabado el Consentimiento expreso del Titular para una Transferencia ulterior en una situación específica, tras haberle informado de su finalidad, de la identidad del destinatario y de los posibles riesgos de dicha transferencia para el Titular debido a la falta de garantías adecuadas en materia de protección de datos. En este caso, el Importador de datos informará al Exportador de datos y, a pedido de éste, le remitirá una copia de la información proporcionada al Titular.

b. Toda Transferencia ulterior estará sujeta a que el Importador de datos adopte las demás garantías previstas en el presente Acuerdo y, en particular cumpla con el principio de finalidad.

6.10. Documentación y cumplimiento

a. Las Partes deberán poder demostrar el cumplimiento de las obligaciones derivadas del presente Acuerdo.

b. En particular, el Importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen bajo su responsabilidad, que pondrán a disposición del Exportador de Datos y en su caso de la Autoridad de control competente previa solicitud.

Cláusula 7

Derechos de los Titulares

a. El Importador de datos, en su caso con la asistencia del Exportador de datos, tramitará, de forma gratuita y sin dilación indebida y a más tardar en un plazo de quince días hábiles, salvo que la normatividad aplicable señale un tiempo menor, desde la recepción de la consulta o solicitud, las consultas y solicitudes que reciba de Titulares en relación con el tratamiento de sus Datos personales y el ejercicio de los derechos que les otorga el presente Acuerdo.

b. El Importador de datos adoptará medidas adecuadas para facilitar dichas consultas y solicitudes y el ejercicio de los derechos de los Titulares. Toda la información que se proporcione a los Titulares deberá ser inteligible y de fácil acceso, con un lenguaje claro y sencillo.

c. En particular, el Titular tendrá derecho a:

   i. Solicitar confirmación de la existencia del tratamiento de sus Datos personales, acceder a sus Datos personales que obren en posesión del Importador de datos, incluyendo copia completa de estos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento, incluyendo entre otras información sobre las categorías de datos procesados, la finalidad del tratamiento, el período de retención de los datos (o el criterio para determinarlo), las Transferencias ulteriores, incluyendo los destinatarios y la finalidad de las mismas, e información sobre el derecho a presentar un reclamo ante la Autoridad de control competente;

   ii. Obtener del Importador de datos la rectificación o corrección de sus Datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados;

   iii. Solicitar la cancelación o supresión de sus Datos personales de los archivos, registros, expedientes y sistemas del Importador de datos, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último, cuando los datos han sido tratados en contravención de los derechos de Terceros beneficiarios que deriven de este Acuerdo, o si el Titular retira el consentimiento en que se basa el tratamiento;

   iv. Oponerse al tratamiento de sus Datos personales cuando el tratamiento de sus Datos personales tenga por objeto la mercadotecnia directa, incluida la

elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

v. Solicitar y acceder al Acuerdo firmado entre el Importador de Datos y el Exportador de Datos, eliminando la información confidencial de terceros ajenos y reservada de acuerdo con la normativa del Importador de Datos.

7.1. Limitaciones en el ejercicio de derechos

a. El Importador de datos podrá denegar la solicitud de un Titular cuando ello esté permitido con arreglo al derecho del país de destino y sea necesario y proporcionado en una sociedad democrática para salvaguardar importantes objetivos de interés público general o los derechos y libertades de las personas.

b. Si el Importador de datos pretende denegar la solicitud de un Titular, le informará de los motivos de la denegación y de la posibilidad de presentar una reclamación ante la Autoridad de control competente o de ejercitar una acción judicial.

7.2. Derecho a no ser objeto de Decisiones individuales automatizadas

a. El Importador de datos no tomará una Decisión individual automatizada con respecto a los Datos personales transferidos.

b. Lo dispuesto en el párrafo anterior no resultará aplicable cuando (i) esté autorizado por la ley de país del Importador de datos que garantice medidas adecuadas para la salvaguarda de los derechos del Titular, o (ii) se base en el consentimiento demostrable del Titular.

c. Cuando el tratamiento de datos esté autorizado por una norma legal o el Titular hubiere manifestado su consentimiento, el Titular tendrá derecho a (i) recibir una explicación sobre la decisión tomada; (ii) ser oído y expresar su punto de vista e impugnar la decisión, y (iii) obtener la intervención humana.

d. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su 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, así como datos genéticos o datos biométricos.

Cláusula 8

Reclamaciones

a. El Importador de datos informará a los Titulares, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará las reclamaciones que reciba de los Titulares con la mayor brevedad. **[OPCIÓN: El Importador de datos se aviene a que los Titulares también puedan presentar una reclamación ante un organismo independiente de resolución de litigios sin coste alguno para el Titular. El Importador de datos informará a los Titulares, en la forma establecida en este párrafo, de este mecanismo de reparación y de que no están obligados a recurrir a este ni a seguir una secuencia concreta de vías de reparación.]**

b. En caso de litigio entre un Titular y una de las Partes en relación con el cumplimiento del presente Acuerdo, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las Partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán de buena fe para resolverlos.

c. El Importador de datos se compromete a aceptar y no controvertir, cuando el Titular invoque un derecho de Tercero beneficiario que deriven de este Acuerdo, la decisión del Titular de:

   i. Presentar una reclamación ante la Autoridad de control del Estado de su residencia habitual o su lugar de trabajo o ante la Autoridad de control competente;

   ii. Ejercitar una acción judicial sobre sus Datos personales de conformidad con lo dispuesto en la cláusula 14 de este Acuerdo.

d. El Importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo a la Ley aplicable o el derecho de que se trate.

Cláusula 9

Responsabilidad Civil

a. Cada Parte será responsable ante la otra de cualquier daño y perjuicio que le cause por la vulneración de los derechos y obligaciones establecidos en el presente Acuerdo.

b. Cada Parte será responsable ante el Titular. El Titular tendrá derecho a ser indemnizado por los daños y perjuicios materiales o inmateriales que alguna de las Partes ocasione al Titular por vulnerar los derechos de Terceros beneficiarios que deriven del presente Acuerdo. Ello se entiende sin perjuicio de la responsabilidad que le atribuye la Ley aplicable al Exportador de datos.

c. Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al Titular como consecuencia de una vulneración del presente Acuerdo, todas las partes responsables serán responsables solidariamente.

d. Las Partes acuerdan que, si una parte es considerada responsable con arreglo al presente, estará legitimada para exigir a la otra parte la indemnización correspondiente a su responsabilidad por el daño o perjuicio.

Cláusula 10

Supervisión de la Autoridad de control competente

a. El Importador de datos acepta someterse a la jurisdicción de la Autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente Acuerdo.

b. En particular, el Importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la Autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la Autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

c. Asimismo, el Importador de datos acepta someterse a las facultades de la Autoridad de control competente respecto a la suspensión de transferencias, suspensión de contratos y las demás medidas correspondientes que esta estime aplicar.

Cláusula 11

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

a. Las Partes confirman que, al momento de celebrar este Acuerdo, han realizado esfuerzos razonables para identificar si los datos transferidos están cubiertos por alguna ley o práctica local de la jurisdicción del Importador de datos que va más allá de lo que es necesario y proporcional en una sociedad democrática para salvaguardar importantes objetivos de interés público y puede razonablemente esperarse que afecte las protecciones, derechos y garantías otorgadas bajo este Acuerdo al Titular. En base a lo expuesto las Partes confirman que no están al tanto que dicha práctica o norma exista o afecte adversamente las protecciones específicas bajo este Acuerdo.

b. El Importador de datos se compromete a notificar en forma inmediata al Exportador de datos si alguna de estas leyes se le aplica en el futuro. De realizarse dicha notificación o si el Exportador de datos tiene motivos para creer que el Importador de datos ya no puede cumplir con las obligaciones de este Acuerdo, el Exportador de datos identificará las medidas apropiadas (por ejemplo, medidas administrativas, físicas y técnicas para garantizar la seguridad) para remediar la situación.

c. Asimismo, podrá suspender las transferencias objeto de este Acuerdo si considera que no pueden garantizarse las garantías adecuadas. En este caso, el Exportador de datos tendrá derecho a rescindir este Acuerdo de conformidad con lo dispuesto en la cláusula 12.

d. Si un tribunal o una agencia gubernamental requiere que el Importador de datos divulgue o utilice los datos transferidos de una manera que de otro modo no estaría permitida por este Acuerdo, el Importador de datos revisará la legalidad de dicha solicitud y la impugnará si, después de una evaluación legal cuidadosa, concluye que existen motivos razonables para considerar que la solicitud es ilegal según la legislación local y afecta los derechos garantizados por este Acuerdo. En la medida en que esto esté permitido por la ley local, también deberá informar de inmediato al Exportador de datos que ha recibido dicha solicitud. Si el Importador de datos tiene prohibido notificar al Exportador de datos según la ley local, hará todo lo posible para obtener una exención de la prohibición.

TERCERA PARTE:

DISPOSICIONES FINALES

Cláusula 12

Incumplimiento de las cláusulas y resolución del contrato

a. El Importador de datos informará inmediatamente al Exportador de datos en caso de que no pueda dar cumplimiento a alguna de las cláusulas de este Acuerdo por cualquier motivo.

b. En caso de que el Importador de datos incumpla las obligaciones que le atribuye el presente Acuerdo, el Exportador de datos suspenderá la transferencia de Datos personales al Importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato.

c. El Exportador de datos estará facultado para resolver este Acuerdo cuando:

   i. El Exportador de datos haya suspendido la transferencia de Datos personales al Importador de datos con arreglo al párrafo anterior y no se vuelva a dar cumplimiento al presente Acuerdo en un plazo razonable y, en cualquier caso, en un plazo de treinta (30) días hábiles a contar desde la suspensión;

   ii. El Importador de datos vulnere de manera sustancial o persistente el presente Acuerdo; o

   iii. El Importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o Autoridad de control competente en relación con las obligaciones que le atribuye el presente Acuerdo. En este supuesto, informará a la Autoridad de control competente de su incumplimiento.

d. Los Datos personales que se hayan transferido antes de la resolución del contrato deberán, a elección del Exportador de datos, devolverse inmediatamente al Exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos. El Importador de datos acreditará la destrucción de los datos al Exportador de datos. Hasta que se destruyan o devuelvan los datos, el Importador de datos seguirá garantizando el cumplimiento con el presente Acuerdo. Si el derecho del país aplicable al Importador de datos prohíbe la devolución o la destrucción de los Datos personales transferidos, el Importador de datos se compromete a seguir garantizando el cumplimiento del presente Acuerdo y solo tratará los datos en la medida y durante el tiempo que exija el derecho del país.

Clausula 13

Derecho aplicable

El presente Acuerdo se regirá por la Ley aplicable.

Cláusula 14

Elección del foro y jurisdicción

a. Cualquier controversia derivada del presente Acuerdo será resuelta judicialmente en los tribunales de la jurisdicción del Exportador de datos.

b. Los Titulares también podrán ejercer acciones judiciales contra el Exportador de datos y/o el Importador de datos, las que podrán ser iniciadas, a elección del Titular, en el país del Exportador de datos, o en el que el Titular tenga su residencia. Con respecto al Importador de datos, también podrán ejercer acciones judiciales en el país del Importador de datos.

c. Las Partes acuerdan someterse a la jurisdicción prevista en esta cláusula.

ANEXOS

ANEXO A

FORMULARIO DE ADHESIÓN DE NUEVAS PARTES

ANEXO B

DESCRIPCION DE LA TRANSFERENCIA

ANEXO C

MEDIDAS ADMINISTRATIVAS, FISICAS Y TECNICAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

ANEXO D

DOCUMENTACION LEGAL

ANEXO A

FORMULARIO DE ADHESIÓN DE NUEVAS PARTES

ADHESIÓN DEL EXPORTADOR DE DATOS

Nombre completo……
[Nombre del Exportador de datos]

Domicilio……

[Domicilio del Exportador de datos]

Contacto……

[Datos de contacto del Exportador de datos]

Actividades relacionadas con los datos transferidos en virtud del presente Acuerdo……

[…]

Ley Aplicable……
[Ley vigente de protección de Datos personales del país Exportador de datos]

Autoridad de control competente……
[Autoridad de protección de Datos personales del país Exportador de datos]

ADHESIÓN DEL IMPORTADOR DE DATOS

Nombre completo……
[Nombre del Importador de datos]

Domicilio……
[Domicilio del Importador de datos]

Contacto……
[Datos de contacto del Importador de datos]

Fecha de Firma: Firmado en *[Ciudad, País], el [MM/DD/AAAA]*

Firma del Exportador de datos:	**Firma del Importador de datos:**
X	**X**
……	**……**

Consentimiento de las partes: *[…….]*

ANEXO B

DESCRIPCIÓN DE LA TRANSFERENCIA

Adhesión del Exportador de datos

Categorías de Titulares cuyos Datos personales se transfieren: *[…]*
……..

Categorías de Datos personales transferidos: *[…]*
……..

Datos personales sensibles transferidos (si procede) y restricciones o garantías aplicadas: *[…]*
……..

Frecuencia de la transferencia: ……
[por ejemplo, si los datos se transfieren de una vez o de forma periódica].

Finalidad(es) de la transferencia y posterior tratamiento de los datos: […]
……..

Plazo: ……
[El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo].

ANEXO C

MEDIDAS ADMINISTRATIVAS, FÍSICAS Y TÉCNICAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

NOTA ACLARATORIA: [En este anexo C las partes deben establecer en detalle las Medidas administrativas, físicas y técnicas específicas que acuerden con el fin de garantizar la seguridad de los datos transferidos bajo el Acuerdo. Los ejemplos de tales medidas incluyen, entre otras, medidas de anonimización y cifrado de los datos personales, medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, medidas para restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas administrativas, físicas y técnicas para garantizar la seguridad del tratamiento, medidas para la identificación y autorización del usuario, medidas para la protección de los datos durante la transmisión, medidas para la protección de los datos durante el almacenamiento, medidas para garantizar la seguridad física de los lugares en los que se tratan los datos personales, medidas para garantizar el registro de incidentes, medidas para garantizar la configuración del sistema, en especial la configuración por defecto, medidas de gobernanza y gestión de la información y la seguridad informática internas, medidas para la certificación/garantía de procesos y productos, medidas para garantizar la minimización de datos, medidas para garantizar la calidad de los datos, medidas para garantizar la responsabilidad proactiva y medidas para garantizar una retención limitada de los datos. Este enunciado no reemplaza la especificación real de las medidas administrativas, físicas y técnicas que las Partes deben adoptar e implementar. Las Medidas administrativas, físicas y técnicas deben describirse de manera concreta y no de manera genérica].

ANEXO D

DOCUMENTACIÓN LEGAL ADICIONAL

[En el presente apartado se deberán incluir los documentos que las normativas de las Partes consideren obligatorios para el tratamiento de datos personales como pueden ser: *Avisos de privacidad o políticas de privacidad*].