



FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

**PLAN DE IMPLEMENTACIÓN DE NORMAS
CORPORATIVAS VINCULANTES. PROPUESTA DIRIGIDA A
GRUPO EMPRESARIAL MULTINACIONAL DEL SECTOR
INDUSTRIAL**

Profesor

Alexandra Maldonado Navarro

Lorena Naranjo Godoy

Autores

Israel Vincent Castro Enríquez

Juan Sebastián Auz Valdez

2023 – 2024

Tabla de Contenido

1. Introducción	6
1.1. Ámbito Político Nacional	6
1.2. Ámbito de Control Nacional	7
1.3. Ámbito de Seguridad Informática	7
1.4. Ámbito de Tecnología	8
2. Identificación del Objeto de Estudio	8
3. Planteamiento del Problema	9
3.1. Problema de investigación	9
3.2. Pregunta General de Investigación	9
3.3. Preguntas específicas de investigación	9
3.4. Efectos del problema de investigación	9
3.5. Causas del Problema de investigación	10
3.6. Escenarios	10
4. Revisión de la Literatura	10
4.1. Marco conceptual	11
4.1.1. Datos personales	11
4.1.2. Categorías de datos personales objeto de transferencias internacionales	12
4.1.3. Transferencias Internacionales de datos personales	12
4.1.4. Actores intervinientes en transferencias internacionales de datos personales	13
4.1.5. Protección de Datos Personales y Normas Corporativas Vinculantes	13
4.1.6. Principios aplicables en Normas Corporativas Vinculantes	14
4.1.7. Elementos esenciales de las Normas Corporativas Vinculantes	14
4.1.8. Cumplimiento normativo y Normas Corporativas Vinculantes	15
4.2. Antecedentes teórico-práctico del problema	15
4.2.1. Régimen jurídico de las normas corporativas vinculantes en Ecuador	16
4.2.2. Régimen jurídico de las normas corporativas vinculantes en Brasil	17
4.2.3. Régimen jurídico de las normas corporativas vinculantes en Perú	18
4.2.4. Régimen jurídico de las normas corporativas vinculantes en República Dominicana	19
4.3. Estándar Internacional	20
4.4. Evaluación de riesgos en protección de datos personales	21
4.5. Evaluación de impacto en protección de datos personales	23

4.6. Medidas de control para mitigar riesgos en protección de datos personales	24
4.7. Marco normativo y de la literatura aplicado al Grupo Empresarial Multinacional del Sector Industrial	25
5. Objetivo General	25
6. Objetivos Específicos	25
7. Justificación y aplicación de la metodología	25
8. Resultados y Propuesta de solución	26
8.1. Niveles de Madurez del Grupo Empresarial Multinacional del Sector Industrial	26
8.2. Registro de Actividades de Tratamiento	27
8.3. Matriz	28
8.4. Finalidades de tratamiento	28
8.5. Base de legitimación	29
8.6. Evaluación de Riesgo del proceso de transferencias internacionales	30
8.7. Evaluación de Impacto del proceso de transferencias internacionales	32
8.7.1. Juicio de Idoneidad	33
8.7.2. Juicio de Necesidad	34
8.7.3. Juicio de Proporcionalidad	34
8.8. Medida de Control	35
8.8.1. Normas Corporativas Vinculantes para el Grupo Empresarial Multinacional del Sector Industrial	35
9. Conclusiones	36
10. Recomendaciones	36
11. Referencias	38
12. Legislación	39
13. Índice de Tablas	42
14. Índice de Gráficos	42
15. Anexos	43
Anexo I	43
Anexo II	49

Resumen

Las normas corporativas vinculantes son un mecanismo de autorregulación que garantiza el adecuado tratamiento en la transferencia internacional de datos personales, y para ello, prevén el íntegro cumplimiento a los principios rectores, los derechos de protección de datos personales y la gestión de derechos de los titulares afectados.

Se evidenció que la naturaleza jurídica de las normas corporativas vinculantes permite la transferencia internacional de datos personales, siempre y cuando estas prevean los requisitos establecidos por Ley, el proceso de aprobación y la autorización de la Autoridad de control; además, el desarrollo de estas se rige a la Ley local del país en dónde se constituyó o está domiciliada la corporación u organización.

Este mecanismo previene la red contractual infinita o la formalización múltiple de Acuerdos de Protección de Datos Personales de Corresponsabilidad o de Encargo; que pueden acarrear limitantes a las actividades comerciales, así como el incumplimiento de estos instrumentos por falta de mecanismos de seguimiento a la interna de la empresa.

El presente trabajo desarrolló e implementó normas corporativas vinculantes en el Grupo Empresarial Multinacional del Sector Industrial con presencia en Ecuador, Brasil, Perú y República Dominicana, factor que despliega los efectos de la transferencia internacional de datos personales.

Por ello, se analizó el régimen jurídico de Ecuador, Brasil, Perú y República Dominicana en materia de protección de datos personales, así como el Reglamento General de Protección de Datos como mejor estándar de protección a nivel internacional; y, se determinó que las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial deben elaborarse con la Ley Orgánica de Protección de Datos Personales y el Reglamento a la Ley Orgánica de Protección de Datos Personales, ya que la constitución y el domicilio de la matriz del grupo es Ecuador.

Finalmente, toda actualización respecto a garantías al derecho fundamental a la protección de datos personales, de transferencias internacionales y las referentes a las normas corporativas vinculantes fueron incorporadas en los Anexos I y II en vista al continuo desarrollo normativo ecuatoriano. Y, además, se advirtió de la necesidad de aprobación de las cláusulas tipo del Grupo Empresarial Multinacional del Sector Industrial en razón a la reciente posesión de la Autoridad de control.

Palabras Clave

Protección de datos personales, Transferencias Internacionales, Normas Corporativas Vinculantes, Garantías adecuadas, Ecuador.

Abstract

The binding corporate rules are a self-regulatory mechanism that guarantees the adequate treatment in the international personal data transfer, and for this purpose, they provide a full enforcement of the guiding principles, the rights of personal data protection ante the management of the rights of the affected data owners.

It was evidenced that the legal nature of the binding corporate rules allows the international personal data transfer, as long as they foresee the requirements established by law, the approval process and the authorization of the Control Authority; furthermore, the development of these rules is based on the local law of the country where the corporation or organization is established or domiciled.

This mechanism prevents the infinite contractual network or the multiple formalization of Data Protection Agreements of Co-responsibility or Entrustment, which may involve limitations to

commercial activities, as well as the non-compliance of these instruments due to the lack of monitoring systems within the company.

The present thesis developed and implemented binding corporate rules in the Multinational Business Group of the Industrial Sector with presence in Ecuador, Brazil, Peru and Dominican Republic, a key factor that deploys the effects of the international personal data transfer.

Therefore, the legal regime of Ecuador, Brazil, Peru and Dominican Republic was analyzed in the area of personal data protection, such as the General Data Protection Regulation as the best standard of protection at international level; and it was determined the binding corporate rules of the Multinational Business Group of the Industrial Sector must be elaborated with the Ley Orgánica de Protección de Datos Personales and the Reglamento a la Ley Orgánica de Protección de Datos Personales, due to the fact that the constitution and domicile of the headquarters of the group is in Ecuador.

Finally, all the updates regarding guarantees to the fundamental right of personal data protection, the international flows and those referring to the binding corporate rules were incorporated in Annexes I and II because of the continuous development of Ecuadorian regulations. In addition, the need for approval of the standard clauses of the Multinational Business Group of the Industrial Sector was noted in consideration of the recent possession of the Supervisory Authority.

Key words

Personal data protection, International Flows, Binding Corporate Rules, Adequate guarantees, Ecuador.

1. Introducción

Empresa del sector industrial¹ inicia sus operaciones en 1975 con la producción de rollos y bolsas de polietileno, destinados para empaque de productos alimenticios y textiles. En 2002 fundó una planta similar en República Dominicana, en Perú, y en Brasil, continuando con el mismo giro de negocio para cubrir con la demanda de la subregión (Grupo Empresarial Multinacional del Sector Industrial [GEMSI], 2023).

Actualmente, la corporación es una de las más importantes de la región en la industria y comercialización de empaques flexibles creativos, innovadores y de vanguardia, mediante el uso de tecnología de punta y su sistema integrado de producción, los cuales son principalmente ofertados a personas jurídicas, a nivel nacional e internacional (GEMSI, 2023).

Tabla No. 1. Productos y Servicios del Grupo Empresarial Multinacional del Sector Industrial

Productos y Servicios
Rollos de polietileno y polipropileno
Empaques flexibles
Tintas e impresión
Artes

Fuente: Elaboración propia a partir de Grupo Empresarial Multinacional del Sector Industrial (2023).

Por otra parte, se sabe que las principales empresas que compiten de manera directa con Grupo Empresarial Multinacional del Sector Industrial (2023) a nivel nacional son varias empresas de categoría grandes, medianas y pequeñas.

La estructura del Departamento Legal del Grupo Empresarial Multinacional del Sector Industrial (2023) está constituida por el área interna de la empresa y de las filiales adscritas a su régimen corporativo, y, también cuenta con asesoría y patrocinio legal externo.

A continuación, se presentan los datos más relevantes en materia de protección de datos personales en el ámbito político, de control, de seguridad informática y de tecnología, los cuales estudian los diferentes componentes sociales, económicos y culturales del Ecuador en la actualidad:

1.1. Ámbito Político Nacional

Ecuador durante el gobierno de turno del presidente Guillermo Lasso Mendoza, tuvo controversias sociales, económicas y políticas, sin embargo, es oportuno centrarse en el hito que ha provocado una afectación directa al derecho fundamental a la protección datos personales, el cual reviste en el Decreto Ejecutivo No. 741 de 17 de mayo de 2023, mismo que dispuso la disolución de la Asamblea Nacional por grave crisis política y conmoción interna (Decreto Ejecutivo 741, 2023, Art. 1).

¹ El presente trabajo al ser desarrollado con fines académicos utiliza el nombre de Grupo Empresarial Multinacional del Sector Industrial como método de anonimización al verdadero nombre societario de la compañía objeto de estudio para la implementación de Normas Corporativas Vinculantes.

Lo que resultó en la entrada en vigor extemporánea del Reglamento a la Ley Orgánica de Protección de Datos Personales el 13 de noviembre de 2023 mediante Decreto Ejecutivo N.º 904, así como la ausencia de Autoridad de Protección de Datos Personales como ente rector para ejecutar las funciones y atribuciones conferidas por Ley en favor de la protección de los derechos y libertades fundamentales de los titulares.

1.2. Ámbito de Control Nacional

La Ley Orgánica de Protección de Datos Personales (2023), en su artículo 76 establece que la máxima autoridad de control en la materia a nivel nacional será la Autoridad de Protección de Datos Personales, ente al que se le asignan funciones, atribuciones y obligaciones por mandato de ley.

Es importante destacar que el expresidente de la República Guillermo Lasso Mendoza el 29 de mayo de 2023 mediante Oficio N.º.T.321-SGJ-23-0143 envió de forma extemporánea la terna para designar al Superintendente de Protección de Datos Personales al Consejo de Participación Ciudadana y Control Social (Oficio Presidencia de la República del Ecuador [OPRE], 2023a).

Ante ello, la terna conformada por Vianna Di María Maino Isaías, Félix Gregory Chang Calvache y Blanca Esmeralda García Velíz fue retirada por el ejecutivo en Oficio No.T.321-SGJ-23-0269 en razón a que Félix Gregory Chang Calvache se excusó a continuar como postulante en el proceso de designación (OPRE, 2023b).

El 19 de octubre de 2023 la presidencia de la República en Oficio No.T.321-SGJ-23-0270 envió al Consejo de Participación Ciudadana y Control Social, CPCCS, otra terna conformada por Vianna Di María Maino Isaías, Denis Gustavo Marín Lavayen y María Alexandra Maldonado Navarro (OPRE, 2023c).

Sin embargo, esta última terna no fue considerada por el presidente de la República Daniel Noboa Azin, y, en Oficio No. T.004-SGJ-24-0072 envió al CPCCS una nueva terna conformada por Fabrizio Roberto Peralta Díaz, María Paula Casares Subia y Luis Enríquez Álvarez (OPRE, 2024d). A ello, el 6 de marzo de 2024 el CPCCS en resolución No. CPCCS-PLE-SG-010-O-2024-0079 se aprobó la terna del ejecutivo e inició el proceso de escrutinio público e impugnación ciudadana (Resolución CPCCS, 2024).

En la Resolución No. CPCCS-PLE-SG-019-E-2024-0106 de 28 de marzo de 2024 el Pleno del CPCCS designó a Fabrizio Roberto Peralta Díaz como Superintendente de Protección de Datos, y, notificó a la Asamblea Nacional del Ecuador para que proceda con la posesión como autoridad de control (Resolución CPCCS, 2024, art. 1 y 2). Y, el 23 de abril de 2024 en Sesión No. 918 de la Asamblea Nacional del Ecuador se posesionó a la Autoridad de Protección de Datos Personales.

A pesar de la entrada de la Ley Orgánica de Protección de Datos Personales tuvieron que pasar tres años desde su publicación en el Registro Oficial para que se designe y posea a la Superintendencia de Protección de Datos Personales, por lo que, dicha autoridad de control ecuatoriana carece de institucionalidad, debido a su reciente creación que supone grandes retos para garantizar el derecho fundamental a la protección de datos personales.

1.3. Ámbito de Seguridad Informática

La Unión Internacional de Telecomunicaciones, UIT, (2020), en su posición de mayor organización global en telecomunicaciones y tecnologías de la información y comunicación, investiga anualmente el índice de ciberseguridad mundial, determinando en qué posición y con qué puntaje clasifican los países según su nivel de ciberseguridad, según su infraestructura y las medidas técnicas, jurídicas, organizativas, cooperativas y de desarrollo de capacidad.

Según los resultados de 2020, de la última edición a la fecha del índice de ciberseguridad mundial, Ecuador ocupa el puesto 119 de 182 países, con un puntaje de 26,30 de 100 puntos,

en la parte inferior del promedio general (UIT, 2020, p.28). De ese resultado se determinó que el área de mayor fortaleza de Ecuador es la legal, siendo una nación con regulación para el área de telecomunicaciones, seguridad de la información y protección de datos personales (UIT, 2020, p.62).

Y, a nivel regional la Comisión Económica para América Latina y el Caribe, CEPAL, en un estudio de ciberseguridad realizado entre 2020 a 2021, estimó que el Ecuador se encuentra en una fase formativa, en razón a su reciente desarrollo de regulación y adaptación a estándares internacionales (Mariano Díaz, 2021, p.50).

1.4. Ámbito de Tecnología

Según los datos oficiales del Banco Mundial (2023), al 2022 Ecuador registra que el 70% de su población total usa el internet y tiene acceso a dicho servicio, además, registra una tendencia de crecimiento del 5 % anual. Por ello, es posible establecer que un porcentaje cercano a la totalidad de la población de Ecuador participa en el tráfico de internet, compartiendo y recibiendo todo tipo de información, incluyendo datos personales.

De igual manera, el acceso a internet y el desarrollo de las tecnologías de la información y comunicación han fortalecido el desarrollo del comercio, las relaciones comerciales y la continuidad de negocio, actividades que son un beneficio derivado de la transferencia internacional de datos personales, las cuales son ejecutadas a través de las siguientes tecnologías:

1. Nube: es una tecnología que facilita la transferencia internacional de datos personales. Permite almacenar, procesar y acceder a datos de forma remota a través de Internet (Pearson, 2013, p. 3-42). En Ecuador, donde se menciona que el 70% de la población tiene acceso a Internet, es probable que muchas transferencias de datos personales se realicen por servicios en la nube. Plataformas como *Google Drive*, *Dropbox* o *Microsoft Azure* permiten almacenar y compartir datos de manera segura internacionalmente.

2. Seguridad de nube: protege los datos personales durante su transferencia internacional. Esto implica implementar medidas como el cifrado de datos, la autenticación de usuarios y la monitorización constante de la actividad en la nube para detectar posibles amenazas (Subashini & Kavitha, 2011, p. 1-11). En el caso de Ecuador, donde se menciona que un gran porcentaje de la población participa en el tráfico de Internet, es crucial que las empresas y organizaciones implementen soluciones de seguridad robustas para proteger el derecho fundamental a la protección de datos personales de los ciudadanos ecuatorianos.

3. Mixto –nube y físico–: En algunas situaciones, las organizaciones pueden optar por un enfoque mixto que combina el almacenamiento y procesamiento de datos en la nube con sistemas físicos locales (Rittinghouse & Ransome, 2017). Esto es relevante para aquellas organizaciones que manejan un gran volumen de datos sensibles y que desean mantener un mayor control sobre su infraestructura. En Ecuador, empresas que operan a nivel internacional utilizarán esta combinación de tecnologías, y además cumplirán con las regulaciones en materia de protección de datos personales.

4. Interoperabilidad: La interoperabilidad es crucial para garantizar que las transferencias internacionales de datos personales se realicen de manera eficiente y segura. Esto implica que diferentes sistemas y plataformas, ya sean de nube o físicos, puedan comunicarse y compartir datos de manera coherente y segura (Loutas, Kamateri, Bosi & Tarabanis, 2011, p. 752-757). En el contexto de Ecuador, donde se menciona una tendencia de crecimiento del uso de Internet, es importante que las tecnologías utilizadas para la transferencia de datos sean compatibles entre sí y puedan integrarse fácilmente con sistemas existentes para garantizar un flujo de información fluido y seguro.

2. Identificación del Objeto de Estudio

Para una adecuada transferencia internacional de datos personales realizada por el Grupo Empresarial Multinacional del Sector Industrial y sus filiales internacionales como

responsables de tratamiento se implementarán normas corporativas vinculantes de acuerdo con lo establecido en la Ley Orgánica de Protección de Datos Personales y el Reglamento a la Ley Orgánica de Protección de Datos Personales en Ecuador, 2023.

3. Planteamiento del Problema

La presente sección abarcará el planteamiento del problema jurídico del Plan de Implementación de Normas Corporativas Vinculantes para el Grupo Empresarial Multinacional del Sector Industrial, mismo que integra: 1. Problema de Investigación, 2. Pregunta General de Investigación, 3. Preguntas Específicas de investigación, 4. Efectos del problema de investigación, 5. Causas del problema de investigación, y, 6. Escenarios; secciones que serán abordadas a continuación.

3.1. Problema de investigación

El Grupo Empresarial Multinacional del Sector Industrial para mantener la continuidad de su negocio realiza transferencias internacionales de datos a los países de Brasil, Perú y República Dominicana, por lo que, a fin de evitar la creación de una red contractual infinita se desarrollarán normas corporativas vinculantes como un mecanismo de autorregulación de conformidad con lo establecido en la Ley Orgánica de Protección de datos personales.

3.2. Pregunta General de Investigación

¿Cómo establecer normas de autorregulación para mantener transferencias internacionales de datos personales en un grupo multinacional de empresas a través de normas corporativas vinculantes conforme la normativa de protección de datos personales?

3.3. Preguntas específicas de investigación

1. ¿Cuál es el régimen jurídico de las transferencias internacionales de datos personales para el desarrollo de normas corporativas vinculantes?
2. ¿Cuál es el estándar y/o normativa internacional aplicable para el desarrollo de las normas corporativas vinculantes?
3. ¿Cuál es el estado de conocimiento de las normas corporativas vinculantes para responsables de tratamiento en la empresa?
4. ¿Cómo establecer normas de autorregulación para evitar crear una red contractual masiva entre empresas del mismo grupo?

3.4. Efectos del problema de investigación

1. Medidas correctivas.
2. Sanciones.
3. Riesgo de filtración de datos sensibles.
4. Incumplimiento de los estándares normativos para realizar las transferencias internacionales de datos personales.
5. Protocolos de seguridad.
6. Interrupción en las operaciones normales de la empresas y continuidad del negocio, como:
 - a. Incumplimiento de obligaciones con proveedores –no entregar materia prima para ejecución de actividades–,
 - b. Afectación a las finanzas de la empresa,
 - c. Problemas legales, y,
 - d. Revelación de secreto empresarial.
7. Incumplimiento de políticas internas de protección de datos personales de la empresa.

3.5. Causas del Problema de investigación

1. Posibles vulneraciones del derecho de datos personales a nivel nacional e internacional, y, la existencia de amenazas internas y externas de los titulares.
2. Desconocimiento del régimen jurídico aplicable.
3. Falta de control por parte de una autoridad competente.
4. Precedentes internacionales en la materia.

3.6. Escenarios

1. Brindar soluciones y estrategias para el proceso de transferencias internacionales de datos personales entre empresas que forman parte del Grupo Empresarial Multinacional del Sector Industrial.
2. Grupo Empresarial Multinacional de Sector Industrial se ve beneficiada al implementar una medida de cumplimiento de carácter preventiva y de autorregulación.
3. Grupo Empresarial Multinacional del Sector Industrial al implementar las normas corporativas vinculantes se beneficiarían estableciendo un proceso que garantice seguridad en las transferencias internacionales de datos personales; y, de esta manera evitarían la imposición de sanciones y medidas correctivas, posibles ataques informáticos y filtraciones ilegales de datos personales, interrupción en las operaciones normales de la empresas y continuidad del negocio, así como el incumplimiento de políticas internas de protección de datos personales.
4. En el supuesto que no se implementen las normas corporativas vinculantes para el proceso de transferencia internacional de datos personales los problemas para Grupo Empresarial Multinacional del Sector Industrial recaen en vulneraciones del derecho de datos personales a nivel nacional e internacional, y, la existencia de amenazas internas y externas.

4. Revisión de la Literatura

Previo al análisis de las normas corporativas vinculantes, es importante estudiar a la transferencia de datos personales, puesto que sin esta institución jurídica dichas normas no desplegarían sus efectos. Por lo tanto, la transferencia abarca todo intercambio, transmisión, divulgación, cesión o acceso a los datos personales a terceros (Wugmeister et. al., 2007, p. 457), ejecutándose a nivel nacional y/o internacional.

En el ámbito internacional las transferencias de datos personales guardan la misma naturaleza jurídica, y, su prestación es la libre circulación de mercancías, capitales, servicios y/o productos ofertados a través del flujo de datos (Custers y Malgieri, 2022, p. 4) en las cuales intervienen terceros como filiales corporativas o autoridades gubernamentales (Wugmeister et. al., 2007, p. 457), no obstante, estas deben garantizar la protección de los derechos y libertades fundamentales de los titulares.

Las transferencias internacionales de datos personales se podrán realizar si concurren los siguientes escenarios: 1. Cumplimiento a la Ley Orgánica de Protección de Datos Personales, 2. Países con un adecuado nivel de protección, 3. Garantías adecuadas, y, 4. Normas corporativas vinculantes. Por ende, vale comentar que el objeto de estudio del presente trabajo radica en la última categoría.

Las normas corporativas vinculantes son una cláusula tipo con carácter de garantía adecuada que facilita la transferencia internacional de datos en actividades y operaciones empresariales de investigación o desarrollo de productos, servicios o procesos en el contexto del comercio exterior (Belli et. al., 2023, p. 5), siempre y cuando, cumplan con los estándares normativos internos, regionales o internacionales.

4.1. Marco conceptual

Los Estados en el marco del derecho a la protección de datos o *data privacy* plantean la necesidad de regular regímenes jurídicos (Dai, 2022, p.86) que establezcan garantías normativas, contractuales y/o medidas de control que brinden seguridad jurídica y transparencia a los derechos y libertades fundamentales de los titulares; en razón a los efectos generados por las tecnologías de la sociedad información y del conocimiento (Rallo Lombarte, 2019, p. 23).

Inclusive, los Organismos Internacionales también han optado por apoyar la regulación de estándares de protección que garanticen el adecuado tratamiento en razón al volumen, la naturaleza, el alcance y las finalidades; y así evitar la materialización de riesgos como vulneraciones a los derechos y libertades fundamentales de sus titulares (OECD/LEGAL/0188, 2023, p. 3).

Para ello, los diferentes cuerpos normativos que regulan la protección de datos personales no comprenden una restricción, sino se convierten en un mecanismo estratégico para ejecutar un tratamiento lícito y legítimo de los datos personales, y así promover su libre circulación mundial mediante transferencias internacionales para fomentar el desarrollo de las relaciones económicas y sociales entre los países (OECD/LEGAL/0188, 2023, p. 3 - 4).

En este sentido, en materia de transferencias internacionales de datos los Estados reconocen que son esenciales para el avance del comercio mundial y el desarrollo socioeconómico de los países (Moerel, 2012, p. 26), por lo que, han tomado la iniciativa de reforzar la protección de los datos personales mediante garantías de cumplimiento y estándares aplicables (Guamán et al., 2023, p. 2), para prevenir los riesgos a los derechos y libertades fundamentales de los titulares (Moerel, 2012, p. 25-26).

No obstante, se advierte que ante la multiplicidad de leyes en materia de transferencias internacionales de datos personales la seguridad jurídica se vería afectada en razón a los diferentes efectos, aplicación e interpretación de las normas territoriales (Moerel, 2012, p. 26), aunque este problema se evitaría con la armonización de leyes o con la aplicación de normas corporativas vinculantes (Moerel, 2012, p. 26).

4.1.1. Datos personales

El término socioeconómico de datos personales radica en que son la materia prima para mejorar la calidad productiva y competitividad de los mercados en beneficio de desarrollo económico, por tanto, equivalen a activo digital (Plana Arnaldos, 2020, pág. 562-563).

Y, el concepto jurídico de datos personales responde a la identidad física, fisiológica, psíquica, económica, cultural o social de una persona natural o física que le identifican o hace identificable a una persona natural o física (Santos Morón, 2020, pág.25).

No obstante, otros autores consideran que los datos personales son hechos y/o estadísticas de consulta o análisis procesados, almacenados o transmitidos por un ordenador, por lo que, el término información personal es el adecuado, ya que al combinarse con diferentes datos estos identifican o hacen identificable a una persona (Dai, 2022, pág. 42 - 43).

Ante ello, es oportuno destacar que el concepto normativo de información personal corresponde al sistema jurídico de países como China, Rusia, Japón o Corea del Sur, y, la definición jurídica de datos personales pertenece a los regímenes jurídicos de países de la Unión Europea, así como Latinoamericanos.

En este sentido, el presente trabajo al desarrollarse en el marco del ordenamiento jurídico ecuatoriano utilizará el término de datos personales como “dato que identifica o hace identificable a una persona natural, directa o indirecta” (Ley Orgánica de Protección de Datos Personales [LOPDP], 2021, art. 4 inciso 8vo).

4.1.2. Categorías de datos personales objeto de transferencias internacionales

Luego de realizar un levantamiento de información al respecto de las actividades de tratamiento de datos personales que involucren o requieran la realización de transferencias internacionales, podrían presentarse las siguientes categorías de datos personales, de acuerdo con lo que establece la normativa y la doctrina:

1. Datos de identificación.
2. Datos de características personales.
3. Datos laborales.
4. Datos patrimoniales.
5. Información comercial.
6. Datos financieros, bancarios, seguros.
7. Datos de transacciones, bienes y servicios.

4.1.3. Transferencias Internacionales de datos personales

Dai destaca que las transferencias internacionales de datos personales se fundan a partir de la comerciabilidad, puesto que estos factores otorgan a las empresas información sobre el verdadero valor del servicio que proveen a los consumidores, lo que se traduce en beneficios económicos (Dai, 2022, p. 113-120).

Empero, estas deben someterse "(...) a un régimen de garantías para impedir que los principios que rigen el derecho fundamental a la protección de datos se vean vulnerados por el mero traslado de dichos datos a otro país" (Red Iberoamericana de Protección de Datos [RIPD], 2022, pág. 12).

En tal sentido, se han regulado estándares técnico-jurídicos que deben cumplirse para garantizar la adecuada transferencia internacional de datos personales; en función a ello, Guamán et al. (2023, p. 3) en el marco del Reglamento General de Protección de Datos, RGPD, considera los siguientes estándares a verificarse:

1. Los datos personales están sometidos a un marco regulatorio específico, y su transferencia a terceros responde a una naturaleza internacional.
2. La ubicación de la empresa o grupos de empresas que ofertan el aplicativo y/o servicios a los ciudadanos.
3. Los países de destino garantizan una protección equivalente a la del RGPD.
4. Las garantías adecuadas o mínimas para ejecutar la transferencia internacional de datos personales.

Y, en la ejecución de las transferencias internacionales de datos personales el responsable de tratamiento siempre preverá que no se disminuya el nivel adecuado de protección, y para ello, debe respetarse el principio de continuidad en garantía a que, en la operación de transferencia de datos objeto de tratamiento, no se afecten los derechos y libertades fundamentales de sus titulares (Remolina, 2010, p. 377).

Asimismo, Gregory Voss, afirma que parte de las obligaciones del responsable de tratamiento en la ejecución de las transferencias internacionales de datos personales en cumplimiento al principio de transparencia, se debe informar al titular como mínimo lo siguiente:

"(...) 1. de los destinatarios o categorías de destinatarios de los datos personales objeto de tratamiento; 2. de si tiene o no la intención de transferir los datos a un tercer país u organización internacional; y 3. de si aplica una decisión de adecuación para permitir dicha transferencia o con sujeción a qué garantías apropiadas o adecuadas se están transfiriendo, y, cómo y dónde obtener una copia de dichas garantías" (Gregory Voss, 2022, p. 521).

Para ello, antes, durante y en la etapa posterior a la transferencia internacional de datos personales el responsable de tratamiento o el encargado de tratamiento deberá verificar tanto las anteriores obligaciones como “(...) la legalidad y sus finalidades” (García Lucas, 2023, p. 5) para garantizar el adecuado tratamiento de los datos personales y así evitar el cometimiento de violaciones a los derechos y libertades fundamentales de sus titulares.

4.1.4. Actores intervinientes en transferencias internacionales de datos personales

Los actores intervinientes comprenden: 1. Exportador de datos, 2. Importadores de datos, 3. Titular del dato personal, 4. Tercero beneficiario, y, 5. Autoridad de Control (RIPD, 2022, p. 19-20).

4.1.5. Protección de Datos Personales y Normas Corporativas Vinculantes

Las normas corporativas vinculantes son cláusulas tipo o códigos de autorregulación que incorporan compromisos rectores que deben incorporar garantías adecuadas y exigibles para el responsable o el encargado de tratamiento del país de destino en la ejecución de transferencias internacionales de datos (Gregory Voss, 2022, p. 508).

Para Ustrán y García (2019, p.476), las normas corporativas vinculantes son un conjunto de estándares con alcance internacional desarrollados de forma voluntaria por una organización empresarial que incluye el nivel más alto de protección para los datos personales en la operación de transferencias internacionales de datos.

Estas normas se clasifican por la organización al legitimar las transferencias de datos entre grupos de empresas mediante cláusulas contractuales tipo² con carácter de garantía adecuada que permite proteger los datos personales objeto de la transferencia a donde quiera que estén ubicadas las filiales de la empresa (Moerel, 2012, p. 27); y, por el territorio legitiman las transferencias de datos entre Estados por medio de acuerdos de cooperación bilaterales o multilaterales exclusivamente para la investigación y aplicación de sanciones a la protección de datos (Moerel, 2012, p. 27).

No obstante, el objeto de estudio del presente trabajo se centrará en las normas corporativas vinculantes basadas en la organización, ya que estas serán implementadas en el Grupo Empresarial Multinacional del Sector Industrial, debido a la estructura y el objeto jurídico que garantizan la adecuada protección de datos personales en transferencias internacionales.

De manera análoga las normas corporativas vinculantes deben garantizar la protección de los derechos y libertades fundamentales de los titulares en el ámbito nacional e internacional, y para ello, están sometidas a un régimen de evaluación que contempla categorías de cumplimiento en la regulación privada, la responsabilidad empresarial, así como la responsabilidad social corporativa (Moerel, 2012, p. 32-33).

La primera categoría de evaluación tiene por finalidad verificar la regulación privada internacional y extrapolarla con elementos de como legislar mejor mediante la incorporación de:

“(...) [1.] Idoneidad para la regulación privada internacional frente a los derechos humanos, [2.] Cuál de las distintas formas de regulación es la adecuada (...), [3.] La legitimidad de la regulación privada internacional en comparación con la regulación pública, [y, 4.] Cómo armonizar las prácticas comerciales restrictivas con los Principios Generales del Derecho, (...)” (Moerel, 2012, p. 33).

La segunda categoría de evaluación busca incluir al principio de responsabilidad frente al cumplimiento de los requisitos legales pertinentes y aplicables, en un estado de rendición de cuentas para exigir a las organizaciones un compromiso con sus responsabilidades y

² A nivel doctrinario y legal las cláusulas contractuales tipo que son utilizadas como normas corporativas vinculantes regula a nivel de la organización son reglas bajo la vertiente del Reglamento General de Protección de Datos de la Unión Europea o del US *Safe Harbors Framework* (Moerel, 2012, p. 27).

obligaciones mediante mecanismos de autorregulación que incorporen a la interna gobernanza y sistemas de gestión en materia de protección de datos (Moerel, 2012, p. 34).

Y, la tercera categoría de evaluación adopta códigos de conducta o de autorregulación que tiene por objeto superar las disparidades normativas y sistemas de regulación entre Estados, así como para mejorar la gestión empresarial, sin embargo, su principal propósito es verificar el nivel de garantías implementadas por las empresas en favor del derecho a la protección de datos, así como su responsabilidad en el tratamiento de datos personales (Moerel, 2012, p. 34).

4.1.6. Principios aplicables en Normas Corporativas Vinculantes

Entre los más importantes principios específicos que aplican a la incorporación de las normas corporativas vinculantes en las actividades de una organización destacan los siguientes:

1. *Binding Nature*, se refiere al principio por el cual un acuerdo celebrado *inter partes*, por su naturaleza, genera efectos legalmente vinculantes, por lo que todas las partes quedan obligadas a dar estricto cumplimiento a aquellos términos y condiciones. Es fundamental en el derecho de las empresas debido a que establecen la base para la ejecución de una serie de acuerdos previamente pactados. (WP 257, 2017, p. 5). Este principio otorga la garantía de íntegro cumplimiento, frente cualquier potencial o posible incumplimiento de las partes.

2. Efectividad, dispone que las normas legales o acuerdos legalmente vinculantes deben aplicarse de manera eficiente y efectiva para garantizar el funcionamiento adecuado de las empresas y promover la actividad económica. Este principio guarda su relevancia en el contexto de las relaciones comerciales y empresariales, donde la rapidez y la eficiencia en la resolución de disputas legales son cruciales para el correcto desarrollo de sus actividades (WP 257, 2017, p. 10).

3. Deber de cooperar, establece la obligación legal y ética que tienen las partes involucradas en una relación comercial o empresarial de colaborar y trabajar juntas de manera honesta y leal para alcanzar los objetivos comerciales comunes. Por tanto, este principio se basa en que las relaciones comerciales exitosas dependen de la confianza, la transparencia y la colaboración entre las partes involucradas (WP 257, 2017, p. 14).

4. Garantías de datos personales, determina la obligación de proteger y garantizar un alto nivel de protección y de seguridad de la información en lo que concierne a datos personales. Este principio es fundamental para cumplir la normativa en la materia en varias jurisdicciones del mundo, e insta proteger a los derechos y libertades fundamentales de los titulares respecto al procesamiento y tratamiento de sus datos personales por parte de organizaciones privadas (WP 257, 2017, p.16).

4.1.7. Elementos esenciales de las Normas Corporativas Vinculantes

Moerel (2012, p. 101) afirma que previo a operativizar las transferencias internacionales de datos mediante normas corporativas vinculantes es menester dar cumplimiento a los requisitos normativos habilitantes estimados por *Data Protection Work Party 29* de la Unión Europea, UE, para su aprobación según el RGPD, los cuales corresponden a los siguientes:

“(…) I. Si la sede la filial no está establecida en la UE, esta debe designar a una empresa del grupo de la UE que tenga responsabilidades delegadas en materia de protección de datos.

II. Las normas corporativas vinculantes deben someterse a la aprobación de la Agencia de Protección de Datos, APD del Estado miembro en el que la filial tenga su sede, en el caso que no tenga sede en la UE, deberá hacerlo en la APD más apropiada.

III. El ámbito geográfico y material de las normas debe disponer si se aplicarán en todo el mundo o sólo a un espacio territorial determinado, así como qué datos, titulares y países están cubiertos.

IV. Las normas corporativas vinculantes deben regular las categorías de los datos, las finalidades y legitimación objeto de tratamiento, así como el alcance de las transferencias en el grupo.

- V. Las normas corporativas vinculantes deben incluir los principios en materia de protección de datos personales, y las respectivas prohibiciones a transferencias a terceros.
- VI. Las normas corporativas vinculantes deben ser exigibles a la interna de la organización como y de forma externa si procede para el beneficio de los titulares.
- VII. Las normas corporativas vinculantes deberán integrar los datos de contacto del delegado de protección de datos personales para el ejercicio de reclamaciones y garantizar el cumplimiento de las normas.
- VIII. Contar con un proceso interno para reclamaciones.
- IX. El cumplimiento de las normas corporativas vinculantes debe ser exigible a los particulares mediante los Acuerdos de Protección de Datos y tribunales del Estado miembro de la empresa del grupo en el origen de la transferencia, o la sede delegada.
- X. La sede delegada debe asumir la responsabilidad de pagar las indemnizaciones y remediar las infracciones de las normas corporativas vinculantes.
- XI. La carga de la prueba con respecto a la supuesta infracción recaerá en la sede delegada y no en el titular.
- XII. Cooperación de las empresas con la APD en auditorías y cumplimiento de resoluciones.
- XIII. Las normas corporativas vinculantes deben prever auditorías para verificar métodos, mejora continua y aplicación de medidas correctivas.
- XIV. Las personas afectadas deben tener fácil acceso a las normas corporativas vinculantes, así como a la información sobre sus derechos.
- XV. Garantizar la formación adecuada de los empleados que tratan datos personales.
- XVI. Debe contemplar un proceso de actualización y un mecanismo para informar las modificaciones a la APD sobre las normas corporativas vinculantes.
- XVII. Deber de transparencia de las empresas (...)” (Moerel, 2012, p. 102-105).

4.1.8. Cumplimiento normativo y Normas Corporativas Vinculantes

Una vez desarrollados los elementos esenciales de las normas corporativas vinculantes que permiten la transferencia internacional de datos personales, el responsable de tratamiento cumplirá “(...) todas las obligaciones exigidas por la ley de protección de datos personales vigente en su jurisdicción” (RIPD, 2022, p. 37), para brindar las garantías adecuadas en el tratamiento de datos personales.

Es decir, se aplicará la normativa del país en el cual se encuentre domiciliada la organización multinacional con el objeto de dar íntegro cumplimiento a las obligaciones y al proceso de aprobación establecido por la ley local (Moerel, 2012, p. 116) en garantía a los derechos y libertades fundamentales de las personas frente a la implementación de las normas corporativas vinculantes a la interna del grupo empresarial.

Además, las cláusulas tipo nunca deberán “(...) facilitar, ni permitir la vulneración de los derechos de los titulares, ni la disminución de garantías” (RIPD, 2022, p. 36), dado el ánimo de preservar el nivel más alto de protección para los datos personales objeto de tratamiento.

4.2. Antecedentes teórico-práctico del problema

En primer lugar, el presente apartado deja en constancia que las normas corporativas vinculantes son el instrumento adecuado para ejecutar transferencias internacionales de datos personales en diferentes filiales empresariales, siempre y cuando su desarrollo y proceso de aprobación se funden en el régimen jurídico del país en el cual el grupo empresarial tenga su sede.

Por lo tanto, la propuesta de cláusulas tipo para el Grupo Empresarial Multinacional del Sector Industrial cumplirá con los requisitos establecidos en la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación, ya que la sede de esta empresa multinacional radica en Quito-Ecuador.

En segundo lugar, se estudiará la naturaleza jurídica y el proceso de aprobación de las normas corporativas vinculantes en las legislaciones de protección de datos personales de Brasil, Perú y República Dominicana; en razón a que son las naciones en donde radican las filiales del Grupo Empresarial Multinacional del Sector Industrial; y, de forma particular al RGPD, dado que en la actualidad es el estándar internacional más adecuado en la materia.

4.2.1. Régimen jurídico de las normas corporativas vinculantes en Ecuador

Pese a la entrada en vigor de la Ley Orgánica de Protección de Datos Personales desde el 26 de mayo de 2023, las empresas con filiales aún no han desarrollado normas corporativas vinculantes como mecanismo jurídico para realizar transferencias internacionales de datos personales, aunque en su mayoría ya cuentan con Sistemas de Gestión para la Protección de Datos Personales.

La Ley establece que las normas corporativas vinculantes son un mecanismo de autorregulación que garantiza el adecuado tratamiento de datos personales en la ejecución de transferencias internacionales a terceros países, y pueden realizarse por el responsable y/o encargado de tratamiento, siempre y cuando contengan los siguientes requisitos: i. Grupo empresarial perteneciente a una actividad económica específica, ii. Principios de tratamiento de datos, iii. Derechos aplicables; y, iv. Garantías de seguridad adecuadas (Reglamento LOPDP, 2023, art. 75).

Los principios de aplicación en materia de protección de datos personales para el adecuado desarrollo de las normas corporativas vinculantes a considerarse son:

1. Juridicidad, los datos personales se tratarán conforme a los principios, derechos y obligaciones prescritas en la Constitución, los Instrumentos Internacionales, la Ley en materia y la normativa como jurisprudencia pertinente (LOPDP, 2021, art. 10 literal a);
2. Lealtad, el tratamiento de datos personales deberá ser leal, por lo que, los titulares sabrán que están recogiendo, utilizando, consultando o tratando datos personales que les conciernen, así como cómo son y serán tratados. Y, en ningún caso estos deberán tratarse a través de medios o fines ilícitos o desleales (LOPDP, 2021, art. 10 literal b);
3. Transparencia, el tratamiento de datos personales es transparente, es decir, aplica a toda información como comunicación en materia de tratamiento, que será de fácil acceso y entendimiento para el titular, en un lenguaje sencillo y claro (LOPDP, 2021, art. 10 literal c);
4. Seguridad de datos personales, los responsables y encargados de tratamiento de datos personales implementarán todas las medidas de seguridad adecuadas y pertinentes de carácter organizativas, técnicas o de cualquier otra naturaleza para protegerlos ante riesgos, vulnerabilidades o amenazas según los datos personales, el ámbito y el contexto (LOPDP, 2021, art. 10 literal j)
5. Responsabilidad Proactiva y Demostrada, el responsable de tratamiento deberá acreditar el haber implementado mecanismos para la protección de datos personales, es decir, demostrar el cumplimiento de principios, derechos y obligaciones; e incluso, se podrá valer de mejores prácticas, esquemas de auto y correlación, códigos de protección, sistemas de gestión y entre otros (LOPDP, 2021, art. 10 literal k).

A nivel nacional, las normas corporativas vinculantes han de desarrollarse en concordancia al ámbito de aplicación y de la actividad empresarial de los responsables de tratamiento y/o los encargados de tratamiento. No obstante, siempre deberán someterse al procedimiento de aprobación establecido en la Ley Orgánica de Protección de Datos Personales, el cual es dirigido por la Superintendencia de Protección de Datos, y como mínimo deberán cumplir las siguientes consideraciones:

1. Obligatorio cumplimiento para el responsable de tratamiento y la empresa que transfieran datos personales (LOPDP, 2021, art. 58),
2. Brindar a los titulares mecanismos para el ejercicio de los derechos de protección de datos personales (LOPDP, 2021, art. 58),
3. Enunciar la estructura, datos de contacto, actividad económica conjunta e individual de las filiales del grupo empresarial, así como del responsable de tratamiento (LOPDP, 2021, art. 58),

4. Aparejar las empresas encargadas de tratamiento, las categorías de datos personales, el tipo de tratamiento y su finalidad (LOPDP, 2021, art. 58),
5. Mantener concordancia con los principios, derechos y obligaciones de la Ley, las medidas de seguridad, requisitos respecto de transferencia o comunicación internacional o de los organismos no sujetos a este instrumento (LOPDP, 2021, art. 58),
6. Ante una potencial o violación de las normas corporativas vinculantes, presentar la aceptación de responsabilidad del responsable o encargado de tratamiento de datos personales (LOPDP, 2021, art. 58),
7. Facilitar a los titulares canales o medios que contengan la información clara y completa sobre las normas corporativas vinculantes (LOPDP, 2021, art. 58),
8. Dar la información de contacto de todos los delegados de protección de datos personales o personas encargadas de la supervisión del cumplimiento de las normas corporativas vinculantes del grupo empresarial (LOPDP, 2021, art. 58),
9. Aparejar detalladamente los mecanismos establecidos en el grupo empresarial para verificar el cumplimiento de las normas corporativas vinculantes (LOPDP, 2021, art. 58),
10. Añadir mecanismos de cooperación coordinada con la Autoridad de control y el responsable de tratamiento de datos (LOPDP, 2021, art. 58),
11. Presentar la declaración de compromiso del responsable de tratamiento de datos en la cual promueve la protección de datos personales entre sus empleados de manera continua (LOPDP, 2021, art. 58).

Y en concordancia con el Reglamento de aplicación de la Ley Orgánica de Protección de Datos Personales se considerará lo siguiente:

1. Legalmente vinculantes (Reglamento LOPDP, 2023, art. 76),
2. Derechos exigibles de los titulares frente al tratamiento de sus datos personales, (Reglamento LOPDP, 2023, art. 76)
3. Cumplimiento de los requisitos dispuestos en la Ley (Reglamento LOPDP, 2023, art. 76).

4.2.2. Régimen jurídico de las normas corporativas vinculantes en Brasil

Con la aprobación de la Ley General de Protección de datos personales el 14 de agosto de 2018, no sería hasta el 18 de septiembre de 2020 que entraría en vigor (Diário Oficial da União, 2018), por tanto, las personas jurídicas privadas que integren grupos empresariales multinacionales en Brasil podrán implementar normas corporativas globales, siempre que estas sean aprobadas por la Autoridad Nacional de Protección de datos.

La *Lei 13.709* prescribe que las normas corporativas globales permiten la ejecución idónea de las transferencias internacionales de datos personales, siempre que el responsable de tratamiento garantice el cumplimiento de los principios y los derechos de los titulares en materia de protección de datos (*Lei 13.709*, 2018, art. 33 literal c).

Por lo tanto, los principios aplicables para la conceptualización de las normas corporativas globales son:

1. Finalidad, el tratamiento de datos personales deberá ser legítimo, determinado y explícito, siempre se comunicará al interesado, y se garantizará que ulteriores tratamientos no sean incompatibles a la finalidad de recogida (*Lei 13.709*, 2018, art. 6 numeral I).
2. Necesidad, el tratamiento de datos personales deberá limitarse al mínimo necesario para el cumplimiento de sus fines, abarcando los datos que sean pertinentes, proporcionados y no excesivos en relación con los fines del tratamiento (*Lei 13.709*, 2018, art. 6 numeral III).
3. Transparencia, garantizar a los titulares información clara precisa y fácilmente accesible sobre el tratamiento de sus datos personales (*Lei 13.709*, 2018, art. 6 numeral VI).

4. Seguridad, el responsable y encargado de tratamiento implementarán medidas técnicas y administrativas para proteger los datos personales del acceso no autorizado y de la destrucción, pérdidas, alteración, comunicación o difusión accidental o ilícita (Lei 13.709, 2018, art. 6 numeral VII).

5. Responsabilidad y rendición de cuentas, el responsable de tratamiento deberá implementar la adopción de medidas para acreditar el cumplimiento de la normativa en protección de datos personales, incluida su eficacia (Lei 13.709, 2018, art. 6 numeral X).

Dentro del régimen jurídico brasilero la Ley General de Protección de Datos Personales determina que las normas corporativas globales deberán dar íntegro cumplimiento al proceso de aprobación el cual de primer plano requiere la autorización de la Autoridad Nacional de Protección de datos personales (Lei 13.709, 2018, art. 35).

Y, la Ley 13.709 deja a salvedad del ente de control: 1. Solicitar información adicional de considerarlo pertinente, así como 2. Ejecutar una debida diligencia en las operaciones de tratamiento que persiguen las normas corporativas vinculantes de la organización (Lei 13.709, 2018, art. 35 inciso segundo).

4.2.3. Régimen jurídico de las normas corporativas vinculantes en Perú

A partir de la entrada en vigor de la Ley 29.733 de Protección de datos personales el 03 de julio de 2011 (Diario Oficial El Peruano, 2011), todas las personas jurídicas privadas que integren grupos empresariales multinacionales en Perú pueden implementar normas internas de protección de datos como instrumento para la ejecución de transferencias internacionales, siempre que cumplan con el procedimiento de aprobación del Reglamento a la Ley 29.733.

En la Ley 29.733 (2023, art.21), las normas internas de protección aseguran y mejoran el tratamiento de datos personales en transferencias internacionales de datos personales, y, previo a consolidarlo, el responsable debe cumplir con la aprobación del Reglamento a la Ley 29.733.

Para ello, los responsables de tratamiento que desarrollen normas corporativas vinculantes o internas de protección deberán prever los principios aplicables en materia de protección de datos personales (Ley 29.733, 2011, art. 31), los cuales son:

1. Legalidad, el tratamiento de datos personales se realizará de conformidad a la Ley, y está prohibida su recopilación ilícita, fraudulenta y/o desleal (Ley 29.733, 2011, art. 4).
2. Consentimiento, el tratamiento de datos personales deberá contar con el consentimiento del titular (Ley 29.733, 2011, art. 5).
3. Finalidad, toda recopilación de datos personales deberá contar con una finalidad determinada, explícita y lícita (Ley 29.733, 2011, art. 6).
4. Proporcionalidad, garantiza que el tratamiento de datos personales sea adecuado, relevante y no excesivo. (Ley 29.733, 2011, art. 7).
5. Seguridad, el responsable y su encargado de tratamiento deberán implementar las medidas técnicas, organizativas y legales, adecuadas y acordes al tratamiento para garantizar la seguridad a los datos personales (Ley 29.733, 2011, art. 9).
6. Disposición de recurso, los titulares de datos personales contarán con proceso administrativos o jurisdiccionales para ejercer sus derechos cuando estos sean vulnerados (Ley 29.733, 2011, art. 10).
7. Nivel de protección adecuado, garantiza que en toda transferencia internacional contemple un nivel suficiente de protección para los datos personales objeto de tratamiento, o una protección equivalente a lo dispuesto en la Ley o de conformidad con los estándares internacionales (Ley 29.733, 2011, art. 11).

En Perú, tanto los responsables como los encargados de tratamiento de datos personales desarrollarán sin obligatoriedad normas internas de protección de datos personales según el

ámbito de su actividad, de conformidad con la Ley 29.733. Para ello, deberán cumplir con el procedimiento de inscripción de códigos de conducta (Reglamento a la Ley 29.733, 2013, Capítulo III), que establece los siguientes criterios:

1. Tendrán carácter voluntario, sectorial y promoverán la totalidad de los tratamientos de datos personales ejecutados (Reglamento a la Ley 29.733, 2013, art. 89).

2. Deben redactarse en términos claros y accesibles, así como cumplir con los siguientes requisitos de Ley: a. Delimitación clara y precisa de su ámbito de aplicación y actividades, b. Previsiones específicas, c. Estándares homogéneos, d. Procedimiento para el ejercicio de derechos, e. Determinación de las transferencias internacionales de datos personales, con las garantías que deban adoptarse, f. Acciones de fomento y difusión, g. Mecanismos de supervisión (Reglamento a la Ley 29.733, 2013, art. 90.2).

Y, contener cláusulas para Obtención de consentimientos, Información a los titulares, Modelos de ejercicios de derechos, y, Cumplimiento de requisitos formales para encargados de tratamiento (Reglamento a la Ley 29.733, 2013, art. 90.3),

3. Las normas internas de protección de datos personales deberán inscribirse en el Registro Nacional de Protección de datos personales con previa solicitud, la cual deberá contener como mínimo lo siguiente:

a. La acreditación de la representación (Reglamento a la Ley 29.733, 2013, art. 91.1),

b. El contenido de la resolución que aprueba el contenido del documento (Reglamento a la Ley 29.733, 2013, art. 91.2),

c. Se adjuntará el certificado de adopción del instrumento y copia de los estatutos de la organización, siempre que medie una decisión de la empresa para adoptar un código de conducta (Reglamento a la Ley 29.733, 2013, art. 91.3),

d. Se deberá aparejar la documentación de representatividad, cuando la organización sectorial haya aprobado un código de conducta a la interna (Reglamento a la Ley 29.733, 2013, art. 91.4), y,

e. Se presentará la descripción de los tratamientos a los que se refiere el código de conducta, en razón a las decisiones tomadas por la empresa (Reglamento a la Ley 29.733, 2013, art. 91.5).

4.2.4. Régimen jurídico de las normas corporativas vinculantes en República Dominicana

La Ley 172-13 que regula la protección integral de los datos personales en República Dominicana se publicó en la Gaceta Oficial el 15 de diciembre de 2013, acto que determinó su entrada en vigor (Gaceta Oficial No. 10737, 2013, p.44), por ello, las personas jurídicas privadas que cuenten con filiales a nivel internacional pueden implementar códigos tipo o normas corporativas vinculantes para efectuar transferencias internacionales de datos personales previo proceso de aprobación.

Los códigos tipo según la Ley 172-13 son condiciones, procedimientos y/o normas de seguridad para el adecuado tratamiento de datos (Ley 172-13, 2013, art. 73), en las transferencias internacionales de datos personales realizadas por el responsable de tratamiento a sus filiales internacionales.

Sin embargo, se requerirá de la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento para realizar transferencias internacionales de datos personales (Ley 172-13, 2013, art. 80 numeral 6), y para el desarrollo de códigos tipo se preverán los principios (Ley 172-13, 2013, art. 73) relativos a:

1. Licitud, el tratamiento de datos personales no tendrá finalidades contrarias a las leyes o al orden público, por lo que, estarán debidamente registradas y respetarán los principios definidos de Ley (Ley 172-13, 2013, art. 5 numeral 1).

2. Calidad de los datos, los datos personales objeto de tratamiento deberán ser adecuados, pertinentes, exactos y actualizados en relación con el ámbito y la finalidad para los que fueron recopilados (Ley 172-13, 2013, art. 5 numeral 2 literal a y b).

3. Seguridad de datos personales, el responsable de tratamiento adoptará medidas técnicas, organizativas y de seguridad para salvaguardar los datos personales, y así se evite su alteración, pérdida, tratamiento, consulta o acceso no autorizado (Ley 172-13, 2013, art. 5 numeral 5).

4. Lealtad, se prohíbe la recolección de datos personales por medios fraudulentos, desleales o ilícitos (Ley 172-13, 2013, art. 5 numeral 7).

5. Finalidad, los datos personales se tratarán de forma legítima cuando su recolección sea adecuada, pertinente y no excesiva en relación con el ámbito y las finalidades determinadas, explícitas y legítimas de recopilación (Ley 172-13, 2013, art. 5 numeral 8).

De forma particular, la Ley 172-13 no establece un procedimiento de aprobación a seguir para códigos tipo como mecanismo legal para realizar transferencias internacionales de datos personales entre filiales de un grupo empresarial, inclusive no se lo menciona en las facultades de la autoridad de control en materia de protección de datos personales como se ha analizado en los regímenes jurídicos que anteceden.

Ergo, el único supuesto regulado por la Ley 172-13 (2013, art. 80 numeral 6) es la transferencia internacional de datos personales entre privados, siempre que existan medidas contractuales o precontractuales celebradas entre el responsable y el titular de los datos, caso contrario no se podrá realizar dicha operación en concepto.

4.3. Estándar Internacional

El RGPD entró en vigor en 2016, por tanto, el responsable de tratamiento y el encargado de tratamiento deben cumplir con los requisitos establecidos para la garantía al nivel adecuado de protección de las personas físicas o naturales para la ejecución de transferencias internacionales de datos personales (RGPD, 2016, art. 44).

El RGPD determina que, por medio de la implementación o el desarrollo de garantías adecuadas (RGPD, 2016, art. 46), el responsable de tratamiento podrá ejecutar transferencias internacionales de datos a uno o más países terceros mediante la figura de normas corporativas vinculantes (RGPD, 2016, art. 46 numeral 2 literal b) o cláusulas tipo asumidas por el responsable dentro de un grupo empresarial dedicado a una actividad económica conjunta (RGPD, 2016, art. 4 numeral 20).

Las normas corporativas vinculantes deberán cumplir con el procedimiento de aprobación de la autoridad de control respectiva de los Estados de la Unión, los elementos sustanciales, el proceso de examen (RGPD, 2016, art. 47). Además, su desarrollo preverá los siguientes principios de aplicación:

1. Limitación de finalidad, los datos personales deben recogerse con fines determinados, explícitos y legítimos, y no se tratarán ulteriormente de manera incompatible con la finalidad principal (RGPD, 2016, art. 5 literal b).

2. Minimización de los datos, garantiza que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento (RGPD, 2016, art. 5 literal c).

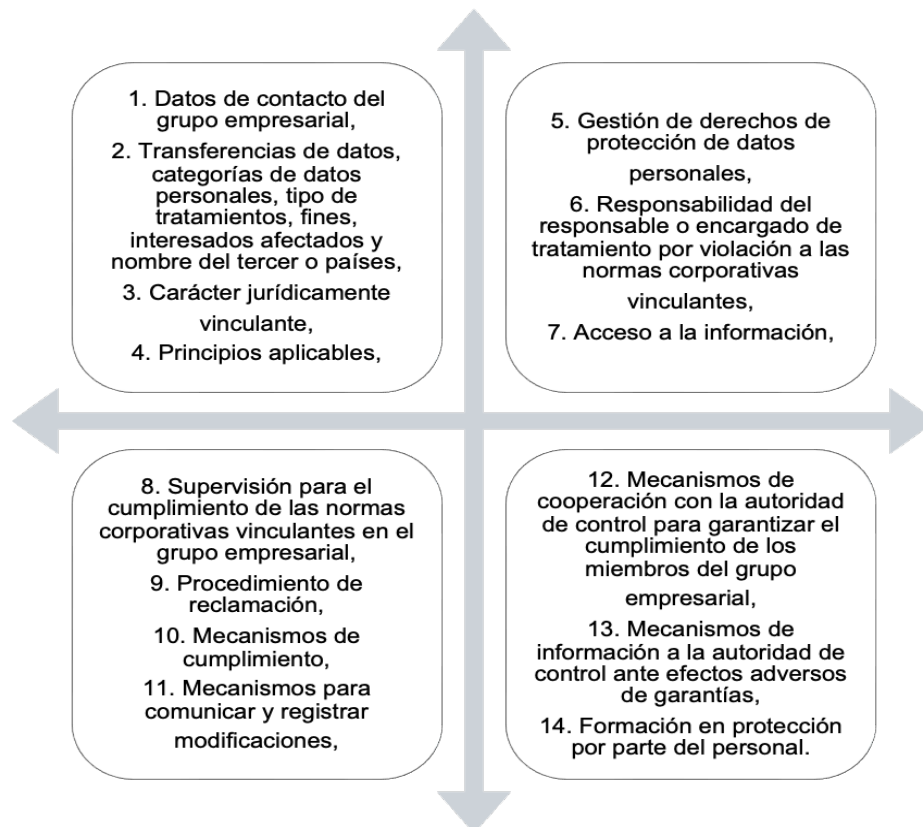
3. Limitación del plazo de conservación, determina la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos (RGPD, 2016, art. 5 literal e).

4. Calidad de los datos, garantiza que los datos personales objeto de tratamiento sean exactos, y de ser necesario actualizados (RGPD, 2016, art. 5 literal d). Cabe mencionar que el RGPD regula a este axioma como parte del principio de exactitud.

5. Protección de datos desde el diseño y por defecto, considera el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, además los riesgos de diversa probabilidad y gravedad en el tratamiento de los derechos y libertades fundamentales de las personas físicas (RGPD, 2016, art. 25).

6. Base del tratamiento, el tratamiento será lícito siempre que prevea una de las siguientes consideraciones: a. consentimiento, b. ejecución de un contrato o de medidas precontractuales, c. cumplimiento de obligación legal, d. Interés vital, e. Interés Público, y f. Interés legítimo (RGPD, 2016, art. 6 inciso primero).

Gráfico No. 1. Elementos mandatorios de las normas corporativas vinculantes



Fuente: Elaboración propia a partir del Reglamento General de Protección de Datos (2016).

Para ello, antes de aplicar en los procesos de transferencias de datos personales de las cláusulas tipo se deberá obtener la debida adaptación (RGPD, 2016, art. 57 inciso primero literal j) y/o la aprobación de las cláusulas tipo (RGPD, 2016, art. 57 inciso primero literal s) por parte la Autoridad de control de conformidad con el mecanismo de coherencia³.

4.4. Evaluación de riesgos en protección de datos personales

La evaluación de riesgos es un mecanismo de supervisión y cumplimiento normativo, complementado con un enfoque de responsabilidad proactiva para minimizar o evitar la materialización de los riesgos aplicando principios y derechos de protección de datos personales y de requerimientos en seguridad de la información (Puyol J, 2018, p. 10).

Asimismo, “(...) consiste en valorar y estimar la probabilidad y el impacto de que el riesgo se materialice” (Gadea Soler, 2020, p. 67) frente a los derechos y libertades fundamentales de

³ Ver, Reglamento (UE) N.º 182/2011 del Parlamento Europeo y del Consejo en el cual establece que el mecanismo de coherencia prevé mecanismos aplicables con condiciones uniformes de ejecución para los actos jurídicamente vinculantes en la Unión mediante la aplicación de principios y normas generales (Reglamento N.º 182/2011, 2011, art. 1).

los titulares, así como al umbral de riesgo que la organización está en condiciones de asumir (Puyol J, 2018, p. 78). El riesgo inherente versa sobre riesgo intrínseco porque este no implementa las medidas de control que lo mitigan o evitan (Gadea Soler, 2020, p. 67) su exposición dentro de una actividad de tratamiento.

En este sentido, el riesgo inherente se calcula a través de la fórmula de Probabilidad x Impacto = Riesgo (Puyol J, 2018, p. 91), misma que figurará como una parte de la metodología a ser aprobada y ejecutada por el responsable de tratamiento. Por consiguiente, el riesgo debe analizarse a través de la probabilidad y del impacto generado por la materialización.

El elemento probabilidad determina el nivel de ocurrencia del riesgo en las diferentes actividades de tratamiento de una organización; y, el elemento impacto vislumbra los posibles daños -físico, material y moral- producto de la materialización del riesgo (Gadea Soler, 2020, p. 68).

Tabla No. 2. Metodología de cálculo para el Análisis de Riesgos en Protección de datos personales

Probabilidad		Impacto o Magnitud de daño	
Despreciable	Baja	Despreciable	Bajo
Limitado	Media	Limitado	Medio
Significativo	Alta	Significativo	Alto
Máximo	Muy alta	Máximo	Muy alta

Fuente: Elaboración propia desde Gadea Soler (2020) y Puyol (2018).

Y, el riesgo inherente se calcula con valores asignados a las escalas de probabilidad e impacto y se representan con una gradiente de 1 como el más bajo y 4 como el más grave:

Tabla No. 3. Cálculo del Riesgos Inherente en Protección de datos personales

Probabilidad		Impacto o Magnitud de daño	
Máximo	1	Despreciable	1
Significativo	2	Limitado	2
Limitado	3	Significativo	3
Despreciable	4	Máximo	4

Fuente: Elaboración propia desde Gadea Soler (2020) y Puyol (2018).

Atributos que al poseer un valor numérico se obtiene como resultado una matriz de riesgos y al ejecutar una interpretación a la realidad de la organización se obtiene el resultado del riesgo inherente (Gadea Soler, 2020, p. 69), equivalente al análisis según el valor obtenido:

Tabla No. 4. Interpretación de valores ajustados al riesgo inherente

Nivel	Estándar
Bajo	De 1 a 2
Medio	Mayor que 2 y menor o igual que 6
Alto	Mayor que 6 y menor o igual que 9
Muy Alto	Mayor a 9

Fuente: Elaboración propia desde Gadea Soler (2020).

Durante el proceso de evaluación de riesgos esta metodología deberá aplicarse a cada una de las amenazas identificadas en las diferentes actividades de tratamiento que posea la organización. Por otro lado, el riesgo residual comprende la reducción al valor del riesgo inherente siempre que se apliquen las medidas de control que mitigan y/o reducen su nivel de exposición (Gadea Soler, 2020, p. 70).

En síntesis, la evaluación de riesgos como mecanismo dentro del Plan de Implementación de Normas Corporativas Vinculantes para el Grupo Empresarial Multinacional del Sector Industrial será ejecutado en el apartado pertinente de Resultados y este también se verá desarrollado en el Registro de Actividades de Tratamiento incluido en el Anexo II.

4.5. Evaluación de impacto en protección de datos personales

La evaluación de impacto debe garantizar la

“(…) protección más activa del derecho fundamental a la protección de datos personales y, por otro, potenciar las políticas preventivas entre las organizaciones para evitar tanto costosos rediseños de los sistemas una vez (...) desarrollados, como posibles daños a la reputación y a la imagen por un inadecuado tratamiento de datos personales” (Gadea Soler, 2020, p. 50).

El responsable de tratamiento tiene la obligación de gestionar adecuadamente los riesgos derivados del tratamiento de datos personales (WP 248, 2017, p. 7) y establecer las medidas de control que mitiguen o eviten los riesgos (Puyol, 2018, p. 13) para los derechos y libertades fundamentales de las personas.

El proceso para ejecutar la evaluación de impacto de forma adecuada debe ser sistemático, es decir, no figura una mera lista de cumplimiento, ya que adjudica una metodología para la eficaz gestión de riesgos a la intimidad de las personas (Gadea Soler, 2020, p. 50).

Antes de realizar la evaluación de impacto, se analiza su necesidad, con ello se debe verificar la procedencia de realizarla en los tratamientos de datos personales que tengan por objeto la satisfacción de: 1. Enriquecimiento, 2. Tratamiento de datos de menores de 14 años, 3. Predicción, 4. Monitoreo de comportamiento, 5. Decisiones que afecten a colectivos, 6. Tecnologías Invasivas, 7. Tratamiento afecta a un número significativo de personas, 8. Riesgos especiales en seguridad, y, 9. Pérdida de control (Gadea Soler, 2020, p. 53-54).

Los elementos⁴ que han de considerarse para ejecutar de forma adecuada a la evaluación de impacto en materia de protección de datos son los siguientes: 1. Descripción sistemática de las operaciones de tratamiento correspondientes a la finalidad de tratamiento, 2. Evaluación de necesidad y proporcionalidad (Recio Gallo, 2016, p. 361).

La fase de descripción sistemática de operaciones de tratamiento correspondientes a la finalidad de tratamiento busca identificar las amenazas y riesgos a los que están expuesto los datos personales dentro de cada una de las etapas del ciclo de vida del dato –Captura, Clasificación, Uso/tratamiento, Cesión, Destrucción–, a las cuales se identificará los elementos involucrados en las actividades de tratamiento, datos tratados, intervinientes y tecnologías (Gadea Soler, 2020, p. 63-64).

Sobre el análisis de la necesidad y proporcionalidad se verificará 1. Licitud del tratamiento —tratamiento de datos personales a partir de las bases de legitimación—, y, 2. Necesidad y Proporcionalidad del tratamiento –aplicando los principios de minimización de datos, y la proporcionalidad evalúa si la finalidad se puede perseguir con la ejecución de otros medios– (Gadea Soler, 2020, p. 64-65).

El estándar idóneo para la evaluación de impacto verifica que en la metodología de gestión de riesgos aplicada al tratamiento de datos personales se concrete la posibilidad de consumir los daños (Recio Gallo, 2016, p. 362) para reducir o mitigar los riesgos a un nivel aceptable para que no se vulneren los derechos y libertades fundamentales de las personas.

En sumativa, la evaluación de impacto en el Plan de Implementación de Normas Corporativas Vinculantes para el Grupo Empresarial Multinacional del Sector Industrial se realizará en el apartado pertinente de Resultados y estará desarrollado en el Registro de Actividades de Tratamiento incluido en el Anexo II.

4.6. Medidas de control para mitigar riesgos en protección de datos personales

Las medidas de control permiten a la organización cimentar una estructura que “(...) permite la identificación, diseño, implantación, administración y mantenimiento de las medidas y mecanismos necesarios para adecuar la gestión del cumplimiento (...) con los intereses del (n)egocio” (Chaveli et. al, 2023, p. 5).

Por otro lado, las medidas de seguridad evalúan a cada uno de los procesos internos de la organización de forma sistemática valorando el riesgo, coste de implementación y el impacto a partir de la seguridad de la información, la protección de datos y siempre bajo las necesidades de la empresa (Chaveli et. al, 2023, p. 7).

Para ello, este tipo de controles siempre han de desarrollarse conforme lo dispuesto por legislación vigente interpretada al diseño, operación, uso y administración de las necesidades de la organización, y así estén definidos como documentados a fin de evitar sanciones administrativas (Chaveli et. al, 2023, p. 22).

Así, estos mecanismos de protección pueden ser administrativos, técnicas, tecnológicas, físicas, organizativas y jurídicas (LOPD, 2021, art. 47 numeral 2), pues otorgan garantías de protección según las necesidades de empresa, gestión de derechos de protección de datos personales, transferencia o comunicación de datos, relaciones de encargo, corresponsabilidad o cesión de datos, entre otras.

Por ello, las medidas de control garantizan la protección a los derechos y libertades fundamentales de las personas respecto al tratamiento de sus datos personales, así como

⁴ Los requisitos para la correcta ejecución de la evaluación de impacto que son esgrimidos por Recio Gallo y corresponden a los determinados por el RGPD, debido a su amplio desarrollo normativo y línea de investigación del autor.

mitigan o minimizan los riesgos relacionados con las operaciones de tratamiento (Gadea Soler, 2020, p. 69).

4.7. Marco normativo y de la literatura aplicado al Grupo Empresarial Multinacional del Sector Industrial

A nivel doctrinario, las normas corporativas vinculantes integran un mecanismo de autorregulación que permite la transferencia internacional de datos personales entre un grupo empresarial multinacional, siempre que estas estén desarrolladas, aprobadas y autorizadas de acuerdo con el régimen jurídico local en dónde la compañía está constituida, domiciliada o tiene su sede.

A nivel regulatorio las cláusulas tipo se analizaron a partir de los regímenes jurídicos de Ecuador, Brasil, Perú y República Dominicana en razón a que el Grupo Empresarial Multinacional del Sector Industrial tiene filiales en los mencionados países; por lo que, se determinó que el desarrollo, la aprobación y la autorización se llevarán a cabo con la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación, ya que la sede la empresa objeto de estudio es ecuatoriana –ver Anexo I pág. 43 a 48–.

Se revisó el Reglamento General de Protección de Datos para conocer la naturaleza jurídica, los requisitos normativos, el proceso de aprobación y la autorización de la Autoridad de Control para las normas corporativas vinculantes; en razón a que este marco normativo a nivel internacional es el estándar de protección más adecuado y aportó al desarrollo las cláusulas tipo del Grupo Empresarial Multinacional del Sector Industrial.

Por otro lado, la Evaluación de Riesgos, la Evaluación de Impacto y las Medidas de Control en protección de datos se estudiaron para ser aplicadas en el registro de actividades de tratamiento –ver Anexo II pág. 49 a 71– del proceso Comercial y Financiero que ejecuta las transferencias internacionales de datos personales del Grupo Empresarial Multinacional del Sector Industrial, y que además, debe cumplir con los parámetros determinado en la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación.

5. Objetivo General

Proponer el plan de implementación de normas corporativas vinculantes como una medida de control jurídica para que el Grupo Empresarial Multinacional del Sector Industrial garantice el adecuado tratamiento de datos personales en el proceso comercial y financiero durante la ejecución de las transferencias internacionales de datos.

6. Objetivos Específicos

1. Determinar el régimen jurídico aplicable para el desarrollo de normas corporativas vinculantes.
2. Analizar los estándares y las normativas internacionales aplicables para la elaboración de las normas corporativas vinculantes de la empresa.
3. Evidenciar el estado de conocimiento de las normas corporativas vinculantes en la empresa para garantizar el derecho de protección de datos personales en las transferencias internacionales.
4. Desarrollar las normas corporativas vinculantes como medida de control jurídica para evitar las redes contractuales múltiples entre empresas del mismo grupo.

7. Justificación y aplicación de la metodología

La metodología que sustenta la presente investigación es de carácter exploratoria, porque se investiga la implementación de normas corporativas vinculantes como un mecanismo para la protección de datos personales durante la transferencia internacional entre la matriz y filiales de Grupo Empresarial Multinacional del Sector Industrial; organización que hoy en día no ha desarrollado a nivel corporativo interno esta medida de cumplimiento y de adecuación.

Así como, soporta un método de investigación de campo como documental, debido al diagnóstico de información del nivel de seguridad implementado en las transferencias internacionales de datos personales en cada territorio correspondiente a las filiales de Grupo Empresarial Multinacional del Sector Industrial.

Además, con el uso de la metodología analítica para realizar un estudio científico por medio del análisis de la información sobre las medidas de seguridad de las filiales y matriz de Grupo Empresarial Multinacional del Sector Industrial, para evitar potenciales vulneraciones a los datos personales durante el proceso de transferencias internacionales.

Con la metodología de procesamiento de datos enfocada en instrumentos que aportarán al diseño e implementación del Plan de implementación de normas corporativas vinculantes para responsables de tratamiento para Grupo Empresarial Multinacional del Sector Industrial mediante entrevistas, encuestas y registro de actividades de tratamiento.

8. Resultados y Propuesta de solución

Estudiado el marco normativo y doctrinario que rigen los requisitos normativos, el proceso de aprobación y la autorización de la Autoridad de Control para el desarrollo de las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial –ver Anexo I pág. 43 a 48–; ahora es preciso traer a colación el proceso de implementación de este mecanismo que permite la transferencia internacional de datos personales.

Por ende, este acápite desarrolla el cumplimiento de los requisitos dispuestos en la Ley Orgánica de Protección de Datos Personales y el Reglamento a la Ley en el proceso de implementación y elaboración de las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial, los cuales prevén: 1. Niveles de madurez de la empresa, 2. Registro de Actividades de Tratamiento, 3. Matriz de Registro de Actividades de Tratamiento, 4. Finalidades de tratamiento, 5. Base de legitimación, 6. Evaluación de riesgos, 7. Evaluación de Impacto, y 8. Medida de control –ver Anexo II pág. 49 a 71–.

Por consiguiente, los requisitos normativos establecidos en la normativa de protección de datos personales ecuatoriana –la Ley local aplicable, puesto que la empresa fue constituida y está domiciliada en Ecuador– previenen la creación de redes contractuales infinitas y proveen seguridad como celeridad en las operaciones comerciales de las filiales del Grupo Empresarial Multinacional del Sector Industrial ubicadas en Brasil, Perú y República Dominicana durante el proceso de transferencias internacionales.

8.1. Niveles de Madurez del Grupo Empresarial Multinacional del Sector Industrial

El proceso de implementación de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la Ley Orgánica de Protección de Datos Personales en el Grupo Empresarial Multinacional del Sector Industrial marcó un hito significativo en la gestión de datos personales. No solo se cumplió con la normativa local en la materia, sino, integró la protección de datos desde el diseño y por defecto en cada proceso organizativo, tecnológico, administrativo y jurídico, así como garantiza de manera preventiva y proactiva el derecho fundamental a la protección de datos personales.

Actualmente la organización se posiciona a la vanguardia de la protección de datos, aplicando las mejores prácticas y alcanzando el más alto nivel en el estado de la técnica para asegurar la confidencialidad, la integridad y disponibilidad de la información personal. Este enfoque proactivo no solo cumple con los requisitos legales, sino que también fortalece la confianza de los clientes y demás partes interesadas en la gestión responsable de sus datos.

Como resultado de este proceso integral, el nivel de madurez de la organización se define como administrado e integrado respecto al estado de conocimiento de las normas corporativas vinculantes, en razón a factores relativos a naturaleza de la empresa, industria, ubicación geográfica y nivel de experiencia en temas de protección de datos. En virtud de ello, se pueden apreciar cuatro niveles en el estado de conocimiento:

1. Conocimiento escaso: la empresa no comprende o conoce los efectos y los requisitos específicos del proceso de implementación de las normas corporativas vinculantes. Esto se debe a la complejidad técnica de la figura legal, la ausencia de recursos económicos o la falta de sensibilización al personal en protección de datos personales en la empresa.

2. Conocimiento básico: la empresa conoce de la existencia de las normas corporativas vinculantes, pero no la importancia de garantía al derecho fundamental a la protección de datos personales. Este conocimiento básico comprende que las cláusulas tipo son un conjunto de reglas internas adoptadas por la empresa multinacional para garantizar un nivel adecuado de protección de datos en el proceso de transferencias internacionales.

3. Conocimiento medio: la empresa conoce de la importancia de la protección de datos personales, pero depende de expertos o abogados especializados para obtener orientación y asistencia en la implementación de normas corporativas vinculantes y estas cumplan con los requisitos de la Ley, así como coordinar su proceso de solicitud y aprobación ante las autoridades de protección de datos pertinentes.

4. Conocimiento avanzado: la empresa es consciente sobre la importancia de las normas corporativas vinculantes como garantía al derecho fundamental a la protección de datos personales en cumplimiento a la regulación nacional y los estándares internacionales. Por lo que, las empresas que operan a nivel internacional y manejan datos personales de clientes, empleados u otras partes interesadas están cada vez más incentivadas a adoptar medidas proactivas para garantizar el cumplimiento de las leyes de protección de datos personales, lo que puede incluir la implementación de normas corporativas vinculantes.

El Grupo Empresarial Multinacional del Sector Industrial se encuentra en el tercer nivel por conocer la existencia de las normas corporativas vinculantes, su importancia en la protección de datos y por la necesidad de contar con la asesoría de expertos para cumplir los requisitos establecidos en la Ley Orgánica de Protección de Datos Personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

Al concluir con el proceso de implementación y elaboración de las normas corporativas vinculantes –ver Anexo I pág. 43 a 48–, se consolidó el cumplimiento de los requisitos normativos que integra a todos los niveles de la empresa y se convierte en parte fundamental de su cultura organizacional. Logro que representa el compromiso continuo con la protección de datos personales y la seguridad de los datos personales en un entorno empresarial cada vez más digitalizado y globalizado.

8.2. Registro de Actividades de Tratamiento

En el Grupo Empresarial Multinacional del Sector Industrial, se tratan datos personales en el ejercicio de sus operaciones financieras, económicas, tributarias y comerciales. Previo a la elaboración de las Normas Corporativas Vinculantes, se investigó y desarrolló un registro de las actividades de tratamiento –ver Anexo II pág. 49 a 71– en las cuales se transfieren a nivel internacional los datos personales. A continuación, se detallan las actividades de tratamiento de datos personales que se han registrado por concepto de las transferencias internacionales:

1. Mantenimiento de Comunicación: Se realizan el envío y recepción de todos aquellos datos necesarios para mantener las operaciones financieras, económicas, tributarias y comerciales entre Grupo Empresarial Multinacional del Sector Empresarial y sus filiales extranjeras. Esto incluye datos personales de accionistas, proveedores de servicios profesionales, trabajadores y otras partes interesadas –ver Anexo II pág. 50 a 52–.

2. Envío de Balances y Flujo Interno: Se envían los balances y el flujo interno de las compañías para garantizar la transparencia y la gestión eficiente de los recursos –ver Anexo II pág. 50 a 52–.

3. Envío de Actas de Junta de Accionistas: Las actas de las juntas de accionistas se envían oportunamente para mantener informados de las decisiones tomadas en dichas reuniones –ver Anexo II pág. 50 a 52–.

4. Envío de Actas de Junta de Directorio: Se envían las actas de las juntas de directorio para asegurar la transparencia en la gestión corporativa –ver Anexo II pág. 50 a 52–.
5. Gestión Comercial: Realizamos cotizaciones de productos y servicios para nuestros clientes, así como la emisión de notas de pedido. Estas actividades involucran el tratamiento de datos personales para garantizar una atención personalizada y eficiente –ver Anexo II pág. 50 a 52–.
6. Envío de Información de Embarque: Se envía información detallada de los embarques para el transporte de productos, lo cual puede incluir datos personales necesarios para el despacho aduanero y la logística –ver Anexo II pág. 50 a 52–.
7. Gestión de Información de Formas de Pago: Se realiza la gestión de la información relacionada con las formas de pago, lo que implica el tratamiento de datos personales para asegurar transacciones financieras seguras y eficientes –ver Anexo II pág. 50 a 52–.
8. Negociaciones: Durante procesos de negociación, se pueden tratar datos personales para facilitar acuerdos comerciales y contratos –ver Anexo II pág. 50 a 52–.
9. Gestión y Elaboración Documental: Se gestionan y elaboran documentos necesarios para realizar las operaciones como actividades comerciales y financieras de la empresa, lo que implicaría un tratamiento de datos personales –ver Anexo II pág. 50 a 52–.

8.3. Matriz

La matriz de registro de actividades de tratamiento es una herramienta fundamental para la gestión y el control de los datos personales dentro de una organización. En el contexto del presente documento, la matriz se diseñó de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

Por ende, la matriz de registro de actividades de tratamiento del proceso de transferencias internacionales de datos personales del Grupo Empresarial Multinacional del Sector Industrial proporciona una estructura organizada y transparente para la administración y documentación de las actividades de tratamiento -comerciales y financieras realizadas por la empresa con sus filiales- de datos personales conforme a la normativa aplicable.

El Anexo II –ver pág. 49 a 71– de la presente investigación contiene la matriz de registro de actividades de tratamiento, la cual ha sido elaborada de acuerdo con el proceso comercial y financiero del Grupo Empresarial Multinacional del Sector Industrial para garantizar la adecuada transferencia internacional de datos personales de conformidad con los elementos necesarios para cumplir con los requisitos legales y así facilitar la gestión interna de los datos personales.

Es importante recalcar que la matriz de registro de actividades de tratamiento se desarrolló partiendo del nivel de madurez del Grupo Empresarial Multinacional del Sector Industrial, parámetro que permite la gestión, el control, la modificación y la revisión periódica, en línea con la normativa aplicable en materia de protección de datos personales y con las prácticas internas de la empresa.

De esta manera, esta matriz permite identificar y registrar todas las actividades de tratamiento de datos llevadas a cabo por la organización, incluyendo la descripción de los datos tratados, las finalidades del tratamiento, las bases legales de legitimación, tecnologías aplicables incorporadas en la actividad, los plazos de conservación de los datos, evaluación de riesgos, evaluación de impacto, medidas de control y entre otros aspectos relevantes –ver Anexo II pág. 49 a 71–.

8.4. Finalidades de tratamiento.

La finalidad del tratamiento de datos en el contexto del Grupo Empresarial Multinacional del Sector Industrial es esencial para mantener la comunicación fluida y eficiente para enviar y recibir información necesaria para realizar operaciones financieras, económicas, tributarias y comerciales. Esta transferencia de datos involucra una amplia gama de información que incluye datos personales de los accionistas, los proveedores de servicios profesionales, los trabajadores y otras partes interesadas –ver Anexo II pág. 53–.

En primer lugar, la comunicación constante y efectiva entre la empresa matriz y sus filiales es crucial para coordinar las actividades comerciales y financieras en los países de Brasil, Perú y República Dominicana – ver Anexo II pág. 58–. Esto implica el intercambio de datos financieros para planificación y ejecución de estrategias empresariales, así como la gestión de riesgos y la toma de decisiones informadas.

Inclusive, el envío y la recepción de datos tributarios son fundamentales para garantizar el cumplimiento de las obligaciones fiscales en cada jurisdicción donde opera el Grupo Empresarial Multinacional del Sector Industrial con sus filiales. Esto incluye la presentación de declaraciones fiscales, la gestión de impuestos locales y extranjeros –ver Anexo II pág. 50 a 52–, así como el cumplimiento de normativas y regulaciones tributarias específicas de cada país.

La transferencia internacional de datos económicos es esencial para evaluar el desempeño financiero de la empresa y de cada filial, así como para identificar oportunidades de mejora y optimización de recursos. Esto implica el análisis de estados financieros, informes de ventas, costos operativos y otros indicadores clave de rendimiento –ver Anexo II pág. 50 a 52–.

Por otro lado, el tratamiento de datos personales de los accionistas, los proveedores de servicios profesionales, los trabajadores y otras partes interesadas también tiene como finalidad garantizar la gestión adecuada de las relaciones comerciales –ver Anexo II pág. 50 a 52–. Esto incluye la gestión de la información de contacto, la identificación de beneficiarios finales, la administración de nóminas y prestaciones laborales, así como el cumplimiento de normativas de protección de datos personales.

8.5. Base de legitimación

Las bases de legitimación que respaldan el tratamiento de datos personales para las transferencias internacionales del Grupo Empresarial Multinacional del Sector Industrial matriz y filiales están reguladas en la normativa legal –ver Anexo II pág. 50 a 52–, específicamente para este caso en el artículo 7 de la Ley Orgánica de Protección de Datos Personales de Ecuador (2021).

Estas bases son fundamentales para garantizar que dichas transferencias se realicen de manera adecuada y respetando los derechos de los titulares de los datos. A continuación, se detallan las principales bases de legitimación:

1. Consentimiento del titular: el tratamiento de datos personales para transferencias internacionales puede legitimarse mediante el consentimiento expreso del titular (LOPDP, 2021, art. 7 numeral 1). Este consentimiento debe ser otorgado de forma libre, informada y específica para una o varias finalidades específicas; y, el titular debe estar plenamente informado del destino de sus datos y dar su consentimiento voluntaria y conscientemente.

2. Cumplimiento de una obligación legal: el tratamiento de datos personales para transferencias internacionales será lícito y legítimo cuando el responsable de tratamiento de íntegro cumplimiento a una obligación legal (LOPDP, 2021, art. 7 numeral 2), es decir, siempre y cuando el responsable de tratamiento esté obligado a cumplir con mandatos legales, estará habilitado a ejecutar el tratamiento de datos personales.

3. Ejecución de medidas precontractuales o contractuales: la Ley dispone que el tratamiento de datos personales para transferencias internacionales puede legitimarse cuando sea necesario para la ejecución de medidas precontractuales a solicitud del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento,

el encargado o un tercero legalmente habilitado (LOPDP, 2021, art. 7 numeral 5). Esto implica que el tratamiento de datos es necesario para formalizar o ejecutar un contrato en el que el titular es parte.

4. Interés legítimo del responsable o tercero en el tratamiento de datos personales para transferencias internacionales también puede basarse en el interés legítimo del responsable del tratamiento o de un tercero. Sin embargo, esta legitimación está sujeta a la condición de que no prevalezcan los intereses o derechos fundamentales de los titulares de los datos (LOPDP, 2021, art. 7 numeral 8). Es decir, el interés legítimo debe equilibrarse con la protección de los derechos y libertades fundamentales de las personas.

Estas bases de legitimación prevén un marco jurídico claro y sólido para el adecuado tratamiento de datos personales en las transferencias internacionales, pues aseguran que se ejecuten legalmente, éticamente y respetando los derechos de los titulares de los datos.

8.6. Evaluación de Riesgo del proceso de transferencias internacionales

El riesgo inherente asociado al proceso de transferencia internacional de datos personales del Grupo Empresarial Multinacional del Sector Industrial obtuvo una puntuación de 8 sobre 10 tal y como se puede apreciar en la siguiente tabla contenida en el Anexo II –ver pág. 69–:

Tabla No. 5. Resultados de la Riesgo Inherente en transferencia internacional de datos personales.

Riesgo Inherente	
Nivel de riesgo inherente	8
Impacto	Alto
Probabilidad	Alta

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

Las transferencias internacionales de datos personales efectuadas en el proceso comercial y financiero del Grupo Empresarial Multinacional del Sector Industrial integran un riesgo inherente alto, debido al nivel de probabilidad alta —establecido por la materialización de incidentes contra la confidencialidad, la integridad y la disponibilidad de la información— y, al nivel de impacto alto —por posibles o potenciales vulneraciones a la seguridad—.

A ello, la valoración de 8 puntos sobre 10 del riesgo inherente se determinó en concordancia al análisis de los siguientes factores:

1. Alta Sensibilidad de los Datos: Los datos personales transferidos incluyen información sensible como datos financieros y/o datos de identificación personal.
2. Entornos Regulatorios Variables: La transferencia internacional de datos personales se realiza en el marco de múltiples jurisdicciones con diferentes niveles de protección, algunos de los cuales pueden no ofrecer garantías adecuadas según la Ley Orgánica de Protección de Datos Personales y el Reglamento General de Protección de Datos.
3. Amenazas Cibernéticas: Aumento de las amenazas cibernéticas globales, incluyendo ataques de *hackers*, *malware* y otros tipos de intrusiones que pueden comprometer la confidencialidad y la seguridad de los datos personales.

4. Vulnerabilidades Tecnológicas: Existencia de vulnerabilidades en los sistemas tecnológicos utilizados para la transferencia internacional y el almacenamiento de datos personales, que podrían ser explotadas por actores malintencionados.

5. Cumplimiento Legal y Regulatorio: incumplimiento de las leyes nacionales y las regulaciones internacionales en materia de protección de datos personales, lo que podría resultar en la imposición de multas y sanciones significativas, lo que traerían consigo la pérdida del buen nombre como reputación de la empresa.

En consecuencia, la implicación de obtener un riesgo inherente alto calificado en 8/10 –ver Anexo II pág. 69– para el Grupo Empresarial Multinacional del Sector Industrial vislumbra la obligación de implementar medidas de control eficaces y eficientes para reducir el riesgo frente los derechos y libertades fundamentales de las personas. Y, las recomendaciones para proveer un nivel aceptable de riesgo en la transferencia internacional de datos son las siguientes:

1. Mejorar las Medidas de Seguridad: Implementar medidas de seguridad avanzadas, como cifrado de extremo a extremo, autenticación multifactorial y monitoreo continuo de la red.

2. Acuerdos Internacionales y Evaluaciones de Impacto: Establecer acuerdos de transferencia de datos con cláusulas contractuales estándar y realizar evaluaciones de impacto sobre la protección de datos personales para todas las transferencias internacionales presentes y futuras.

3. Capacitación y Concienciación: Capacitar al personal sobre las mejores prácticas en protección de datos y concienciar sobre los riesgos asociados a la transferencia internacional de datos personales.

4. Auditorías: Realizar auditorías periódicas y revisiones de los procesos de transferencia internacional de datos personales para asegurar el íntegro cumplimiento a lo establecido en la Ley Orgánica de Protección de Datos Personales y el Reglamento Ley Orgánica de Protección de Datos Personales.

Por otro lado, una vez implementadas las normas corporativas vinculantes y otras medidas de control técnicas, tecnológicas, administrativas, organizativas, jurídicas y funcionales a la interna del Grupo Empresarial Multinacional del Sector Industrial, el riesgo residual asociado a la transferencia internacional de datos personales es de 3/10, conforme a la siguiente tabla –Anexo II ver pág. 71–:

Tabla No. 6. Resultados de la Riesgo Residual en transferencia internacional de datos personales.

Riesgo Residual	
Nivel de riesgo residual	3
Impacto	Menor
Probabilidad	Improbable

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

Este resultado refleja una significativa disminución del riesgo inherente, puesto que se le atribuyen las siguientes consideraciones:

1. **Cumplimiento Normativo:** Las normas corporativas vinculantes aseguran que todas las entidades del Grupo Empresarial Multinacional del Sector Industrial cumplan con los mismos estándares establecidos en la Ley Orgánica de Protección de Datos Personales y el Reglamento Ley Orgánica de Protección de Datos Personales ecuatoriana, independientemente de su ubicación geográfica.

2. **Reducción de Vulnerabilidades:** La implementación de políticas y procedimientos en materia de protección de datos personales reduce las vulnerabilidades asociadas a la transferencia de datos y mejora su seguridad.

3. **Respuesta Eficaz a Incidentes:** La existencia de protocolos claros para la gestión de incidentes y brechas de seguridad en los datos personales permite una respuesta rápida y efectiva, minimizando el impacto de posibles incidentes.

4. **Fomento de la Confianza y la Reputación:** El compromiso del grupo con la protección de datos personales, evidenciado por la implementación de las normas corporativas vinculantes, mejora la confianza de los clientes, socios y reguladores, reduciendo el riesgo reputacional.

Por ende, la reducción del riesgo inherente dejó un riesgo residual estimado en 3/10 tras la implementación de las normas corporativas vinculantes, mecanismo de autorregulación que demuestra su efectividad para la mitigación de riesgos asociados a la transferencia internacional de datos personales.

8.7. Evaluación de Impacto del proceso de transferencias internacionales

En el presente acápite adjunta los resultados de la evaluación de impacto en protección de datos personales –ver Anexo II pág. 66 a 67– en el proceso comercial y financiero del Grupo Empresarial Multinacional del Sector Industrial en el cual se efectúan las transferencias internacionales de datos personales.

Tabla No. 7. Resultados de la Evaluación de Impacto en la transferencia internacional de datos personales.

Evaluación de Impacto en Protección de Datos Personales	
Juicio de Idoneidad	
El tratamiento es adecuado para el fin perseguido	
Si	El presente tratamiento es pertinente y no excede los límites de lo necesario para cumplir su finalidad
No	
Juicio de Necesidad	
La finalidad puede alcanzarse de otro modo menos lesivo	
Si	

No	El presente tratamiento se ha limitado al mínimo necesario en la recolección y tratamiento de datos personales, un tratamiento distinto afectaría la calidad, veracidad y confidencialidad de la información
Juicio de Proporcionalidad	
La gravedad del riesgo para los derechos y libertades y su intromisión es adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de la actividad de tratamiento	
Si	Al tratarse de un tratamiento no exhaustivo ni sistemático, la urgencia en que se realiza es adecuada y garantiza en gran medida que los riesgos se mantengan al mínimo
No	
El tratamiento supone una negación al derecho a la protección de datos personales	
Si	
No	El Grupo de empresas pone a disposición diferentes canales de atención para las partes interesadas que desean ejercer sus derechos, así como la designación de un DPD como buena práctica de protección de datos personales

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

8.7.1. Juicio de Idoneidad

La transferencia internacional de datos personales ejecutada por el Grupo Empresarial Multinacional del Sector Industrial en el proceso comercial y financiero es adecuada conforme a la finalidad de tratamiento perseguida, ya que los datos personales recopilados y procesados son los necesarios y los pertinentes para cumplir con los objetivos establecidos. Por ende, este tratamiento es idóneo en concordancia con lo siguiente:

1. **Objetivos Claros y Específicos:** Los datos personales se recopilan y utilizan con fines claramente definidos, alineados con los objetivos comerciales y operativos del grupo.
2. **Adecuación al Propósito:** El tratamiento está diseñado para cumplir con estos objetivos sin exceder los límites de lo necesario.

Por ello, el tratamiento de datos personales es pertinente y no excede los límites para cumplir su finalidad, y, por ello, la evaluación de impacto confirma que el tratamiento está ceñido a lo necesario, pues no se recolectan ni procesan datos personales más allá de lo requerido para fines distintos, garantía que evita cualquier tratamiento excesivo o indebido de datos personales.

8.7.2. Juicio de Necesidad

El análisis de necesidad concluyó que no existen métodos o procedimientos alternativos menos invasivos en garantía al derecho a la intimidad de los titulares de los datos personales para conseguir las mismas finalidades de tratamiento, por concepto a:

1. **Recolección y Tratamiento Minimizado:** El tratamiento se ha limitado al mínimo necesario, garantizando que solo se recopilan los datos imprescindibles.
2. **Impacto en Calidad y Veracidad:** Un tratamiento distinto podría comprometer la calidad, veracidad y confidencialidad de la información, lo cual es crítico para la fiabilidad de los datos y la efectividad del tratamiento.

De esta manera, este tratamiento limita al mínimo necesario la recolección de datos personales para su tratamiento; porque, en el supuesto de adaptar un tratamiento diferente al estudiado se podría afectar la disponibilidad, la integridad y la confidencialidad de los datos personales.

Por consiguiente, la limitación al mínimo necesario asegura que se respetan los principios de legalidad, lealtad, transparencia, pertinencia y minimización de datos, seguridad y confidencialidad que son esenciales para proteger los derechos y libertades fundamentales de las personas y para mantener la integridad del tratamiento.

8.7.3. Juicio de Proporcionalidad

El juicio de proporcionalidad evalúa la relación entre el impacto del tratamiento en los derechos y libertades de las personas, así como la urgencia y la gravedad del objetivo perseguido. En función a ello, se determinó lo siguiente:

1. **Adecuación y Proporcionalidad:** La gravedad del riesgo es adecuada y proporcionada a los objetivos del tratamiento. La actividad de tratamiento no es exhaustiva ni sistemática, lo que ayuda a minimizar los riesgos.
2. **Urgencia Justificada:** La urgencia del tratamiento se justifica por la necesidad inmediata de alcanzar los objetivos establecidos, garantizando que los riesgos se mantengan bajo control.

Por tal razón, al ser un tratamiento no exhaustivo y sistemático, la urgencia en que se ejecutan las transferencias internacionales de datos personales es adecuada, puesto que la naturaleza no exhaustiva ni sistemática de la actividad de tratamiento prevé que los riesgos se encuentren en un nivel aceptable para garantizar que cualquier intromisión a los derechos de las personas siempre sea mínima y justificada.

De igual manera, la evaluación de impacto en la transferencia internacional de datos personales confirma que el tratamiento no niega el derecho fundamental a la protección de datos personales, ya que el Grupo Empresarial Multinacional del Sector Industrial implementó entre otras las siguientes medidas de control:

1. **Canales de Atención:** Se han establecido múltiples canales de atención para que las partes interesadas puedan ejercer sus derechos, como acceso, rectificación, supresión y oposición.
2. **Designación del delegado de protección de datos personales:** su designación asegura la supervisión y control para garantizar el cumplimiento de la normativa en materia de protección de datos personales.

En acorde con lo anteriormente desarrollado, el Grupo Empresarial Multinacional del Sector Industrial pone a disposición diferentes canales de atención para los titulares interesados que desean ejercer sus derechos, así como designa a un delegado de protección de datos personales como una buena práctica en la materia objeto de estudio –ver Anexo I pág. 46–.

Así, estas prácticas no solo garantizan el cumplimiento de la Ley Orgánica de Protección de Datos, el Reglamento a Ley Orgánica de Protección de Datos y demás normativa aplicable en la materia, sino que también demuestra el compromiso proactivo del Grupo Empresarial

Multinacional del Sector Industrial con la protección de los derechos y libertades fundamentales de las personas.

8.8. Medida de Control

Las normas corporativas vinculantes –ver Anexo I pág. 43 a 48– implementadas en el Grupo Empresarial Multinacional del Sector Industrial, son una medida de control con naturaleza jurídica que permite la transferencia internacional de datos personales en el proceso comercial y financiero entre la empresa matriz y las filiales.

Contemplan el cumplimiento a la Ley Orgánica de Protección de Datos Personales y al Reglamento a la Ley Orgánica de Protección de Datos Personales ecuatoriano, así como establecen reglas específicas para el tratamiento adecuado y la transferencia internacional de datos personales a fin de prevenir posibles infracciones legales y mitigar los riesgos asociados al incumplimiento normativo.

A fin de garantizar la eficacia de estas cláusulas tipo se preverán los requisitos legales, el proceso de aprobación y la autorización de la Autoridad de Protección de Datos Personales ecuatoriana, elementos que dotarán al Grupo Empresarial Multinacional del Sector Industrial de un estándar de control uniforme y vinculante durante toda transferencia internacional de datos personales.

Además, promueven una cultura de responsabilidad y transparencia en materia de protección de datos dentro de la empresa al definir roles y responsabilidades claras en relación con el tratamiento de datos personales, fomentan buenas prácticas de gobernanza de datos personales y facilitan el proceso de auditoría y supervisión interna –ver Anexo I pág. 43 a 48– para garantizar el monitoreo continuo al cumplimiento normativo.

8.8.1. Normas Corporativas Vinculantes para el Grupo Empresarial Multinacional del Sector Industrial

Estudiados los postulados doctrinarios y los requisitos jurídicos establecidos en los regímenes jurídicos de Ecuador, Brasil, Perú, República dominicana y el Reglamento General de Protección de Datos, se integraron en las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial los siguientes parámetros: principios aplicables, tratamiento legítimo, jurisdicción, ejercicio y gestión de derechos, delegado de protección de datos personales y procesos de auditoría –ver Anexo I pág. 43 a 48–.

Con ello, estas cláusulas tipo al ser una medida de control jurídica garantizan cumplimiento normativo, protección al derecho fundamental a la protección de datos personales y responsabilidad empresarial durante las transferencias internacionales de datos personales efectuadas en el proceso comercial y financiero del Grupo Empresarial Multinacional del Sector Industrial.

Inclusive previene la formalización de redes múltiples de Acuerdos de Protección de Datos Personales de Corresponsabilidad o de Encargo entre las filiales del Grupo Empresarial Multinacional del Sector Industrial durante las transferencias internacionales de datos personales en garantía a los principios de legalidad, lealtad, transparencia, pertinencia y minimización de datos, seguridad y confidencialidad, que guían el adecuado tratamiento de datos dentro de la empresa.

Para ello, el Anexo I contiene las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial –ver pág. 43 a 48–, las cuales fueron desarrolladas en contexto a la información y la naturaleza de las operaciones comerciales y financieras en dónde se efectúa la transferencia internacional de datos personales y fueron trabajadas en cumplimiento a la Ley Orgánica de Protección de Datos Personales y el Reglamento a la Ley Orgánica de Protección de Datos Personales, por ser la aplicable puesto que la empresa tiene su sede y se constituyó en Ecuador.

9. Conclusiones

- El presente trabajo estudió a las normas corporativas vinculantes al ser una medida de control de naturaleza jurídica que permite la transferencia internacional de datos personales en cumplimiento a los principios -de legalidad, lealtad, transparencia, pertinencia y minimización de datos, seguridad, así como confidencialidad-, los derechos de protección de datos personales y la gestión de derechos.
- La transferencia internacional de datos personales congrega cuatro garantías relativas a: 1. Cumplimiento a los requisitos establecidos por la Ley, 2. Transferencia a países, organizaciones y personas jurídicas con nivel adecuado de protección, 3. Transferencia que incluya garantías adecuadas –cumplimiento de principios, derechos y obligaciones, gestión de derechos y reparación integral–, y, 4. Normas corporativas vinculantes.
- Con el análisis de la información levantada en contexto al proceso comercial y financiero que efectúa la transferencia internacional de datos personales en el Grupo Empresarial Multinacional del Sector Industrial y sus filiales, se elaboraron las normas corporativas vinculantes a la luz de los requisitos y el proceso de aprobación establecidos en la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación –debido a que el domicilio y la constitución de la empresa radican en Ecuador–, así como con las necesidades previstas en las actividades comerciales de la empresa.
- Previo a elaborar las normas corporativas vinculantes se parametrizó una matriz de actividades de tratamiento que integra las finalidades de tratamiento, la legitimación, la evaluación de riesgos y la evaluación de impacto en el proceso de transferencia internacional de datos personales en el Grupo Empresarial Multinacional del Sector Industrial de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación.
- En garantía al adecuado tratamiento de datos personales en las transferencias internacionales ejecutadas por el Grupo Empresarial Multinacional del Sector Industrial; se documentó que las finalidades de tratamiento son financieras, económicas, tributarias, comerciales como societarias; y que están legitimadas mediante el Consentimiento del titular, el Cumplimiento de obligación legal, la Ejecución de medidas precontractuales o cumplimiento de obligaciones contractuales y el Interés legítimo -bases de legitimación establecidas en la Ley Orgánica de Protección de Datos Personales-, requisitos que proporcionaron la licitud y la legitimación del tratamiento para el adecuado desarrollo de las normas corporativas vinculantes de la empresa.
- Así, las normas corporativas vinculantes del Grupo Empresarial Multinacional del Sector Industrial establecen reglas específicas para el tratamiento adecuado y la transferencia internacional de datos personales a fin de prevenir la materialización de riesgos asociados a las vulneraciones a la seguridad o accesos no autorizados y la formalización múltiple de Acuerdos de Protección de Datos Personales de Corresponsabilidad y/o de Encargo, y, el incumplimiento interno por falta de procesos de seguimiento; así como, facilitar la ejecución y la celeridad de las actividades comerciales para la prestación de los servicios y/o productos en la consecución de los intereses de la empresa.
- No obstante, la ejecución de las normas corporativas vinculantes a la interna del Grupo Empresarial Multinacional del Sector Industrial se verá retrasada por concepto de la aprobación de la Autoridad de control, ya que recién el 23 de abril de 2024 fue posesionada para que ejercer sus competencias atribuidas por la Constitución y la Ley, acontecimiento que evidencia la falta de institucionalidad del ente de control.

10. Recomendaciones

Como resultado al proceso de implementación de normas corporativas vinculantes en el Grupo Empresarial Multinacional del Sector Industrial se constató que el nivel de madurez de la empresa está en el grupo de conocimiento medio, es decir, requiere la asesoría de expertos

especializados en protección de datos personales para obtener orientación y asistencia para la debida aplicación de esta medida de control jurídica. Para ello, es importante considerar a la interna de la empresa las siguientes recomendaciones:

1. Adoptar un enfoque proactivo, coherente y coordinado que garantice que las normas corporativas vinculantes sean efectivas, claras y consistentes en cumplimiento a la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación, a fin de evitar las redes múltiples acuerdos entre las filiales de la empresa, el incumplimiento a los requisitos, así como vulnerar los derechos y libertades fundamentales de los titulares.
2. Promover la transparencia y la comunicación efectiva a la interna del Grupo Empresarial Multinacional del Sector Industrial con el objeto de garantizar que todas las filiales y los colaboradores comprendan sus responsabilidades y obligaciones en relación con las normas corporativas vinculantes.
3. Desarrollar, gestionar y mantener actualizados los canales de atención a derechos de protección de datos personales que receptan las solicitudes y/o quejas de los titulares afectados, así como designar a un Delegado de protección de datos personales para que supervise el cumplimiento de las normas corporativas vinculantes y actúe como punto de contacto con los titulares y la Autoridad de control.
4. Colaborar con la Autoridades de Protección de Datos Personales para garantizar que las normas corporativas vinculantes cumplan con el régimen jurídico ecuatoriano en materia de protección de datos personales. Esto incluye la presentación de las normas corporativas vinculantes para su proceso de aprobación y la predisposición a adoptar cualquier recomendación adicional que la Autoridad de control solicite regular para mejorar la protección de datos personales en el contexto de las transferencias internacionales.
5. Diseñar políticas, procesos o programas de auditorías y de capacitación enfocados en identificación y gestión de riesgos para asegurar el adecuado tratamiento de los datos personales de conformidad con la normativa de protección de datos de ecuatoriana; los cuales podrán ejecutarse en períodos anuales o semestrales en aras de conseguir una cultura de protección de datos en toda la empresa.
6. Designar un órgano central en el Grupo Empresarial Multinacional del Sector Industrial para supervisar y gestionar el cumplimiento a las normas corporativas vinculantes en todas las filiales relacionadas para identificar y mitigar potenciales conflictos o inconsistencias en las políticas y prácticas en la protección de datos dentro de la empresa.

11. Referencias

- Agencia Española de Protección de Datos. (2024, Mayo). *Evalúa Riesgo RGPD*. <https://evalua-riesgo.aepd.es>
- Banco Mundial. (2023, Diciembre). *Ecuador Data: Individuals using the Internet*. <https://data.worldbank.org/country/EC>.
- Belli, L., Brian Nougères, A., Mendoza Iserte, J., Palazzi, P., y Remolina Angarita, N. (2023) *Hacia un Modelo Latinoamericano de adecuación para la transferencia internacional de datos personales*, CETYS & CDYT.
- Chaveli, E., Haro, F., & Barrientos, D. (2023). *Medidas de cumplimiento*. AEC.
- Custers, B., & Malgieri, G. (2022). Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45(2), 1-11. DOI: [10.1016/j.clsr.2022.105683](https://doi.org/10.1016/j.clsr.2022.105683).
- Dai, Y. (2022). *Cross-Border Data Transfer Regulations of International Trade Law: A PRC Perspective*. Springer. DOI: [10.1007/978-981-16-4995-0](https://doi.org/10.1007/978-981-16-4995-0).
- Gabea Soler, E. (2020). Análisis de riesgos y evaluación de impacto relativa a la protección de datos: su aplicación a las sociedades cooperativas, *Boletín de la Asociación Internacional de Derecho Cooperativo*, 56(4), 47-72. DOI: <https://doi.org/10.18543/baidc-56-2020pp47-72>.
- García Lucas, P. (2023). *Transferencias Internacionales de Datos*. AEC.
- Gregory Voss, W. (2020). CROSS-BORDER DATA FLOWS, THE GDPR, AND DATA GOVERNANCE. *Washington International Law Journal*, 29(3), 485-531. <https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7>.
- Grupo Empresarial Multinacional del Sector Industrial. (2023, Diciembre). *Acerca de nuestra empresa*. <https://www.grupoempresarialmultinacionaldelsectorindustrial.com>.
- Guamán, D., Rodriguez, D., del Alamo, J., & Such, J. (2023). Automated GDPR compliance assessment for cross-border personal data transfers in android applications. *Computer & Security*, 130(07), 1-16. DOI: [10.1016/j.cose.2023.103262](https://doi.org/10.1016/j.cose.2023.103262).
- Loutas, N., Kamateri, E., Bosi, F., & Tarabanis, K. (2011, November). Cloud computing interoperability: the state of play. In 2011 IEEE Third International Conference on Cloud Computing Technology and Science (pp. 752-757). IEEE. DOI: [10.1109/CloudCom.2011.116](https://doi.org/10.1109/CloudCom.2011.116).
- Mariano Díaz, M. (2020). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Naciones Unidas & Comisión Económica para América Latina y el Caribe. <https://repositorio.cepal.org/4b04fcfe-c0f3.pdf>.
- Moerel, L. (2012). *Binding Corporate Rules. Corporate Self-Regulation of Global Data Transfers*. Oxford. DOI: [9780199662913.003.0007](https://doi.org/10.1017/9780199662913.003.0007).
- Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. En *Privacy and Security for Cloud Computing* (pp. 3-42). Springer. DOI: [10.1007/978-1-4471-4189-1_1](https://doi.org/10.1007/978-1-4471-4189-1_1).
- Plana Arnaldos, M. (2020). Los datos personales como contraprestación. En I. González Pacanowka (Coord.), *Protección de Datos Personales* (561-615). Tirant.
- Puyol, J. (2018). *El Modelo de Evaluación de Riesgos en la Protección de Datos EIPD/PIA's*. Tirant lo Blanch.
- Rallo Lombarte, A. (2019). Del derecho a la protección de datos a la garantía de nuevos derechos digitales. En A. Rallo Lombarte (Dir.), *Tratado de Protección de Datos* (23-52). Tirant lo Blanch.

- Remolina Angarita, N. (2010). Cláusulas contractuales y Transferencia Internacional de Datos Personales. En J. Oviedo Albán (Coord.), *Obligaciones y Contratos en el Derecho Contemporáneo* (357-403). Díké & Universidad de la Sabana.
- Recio Gallo, M. (2016). Aproximación basada en el Riesgo, Evaluación de Impacto relativa a la Protección de Datos Personales y Consulta Previa a la Autoridad de Control. En J. Piñar Mañas (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos* (351-366). Reus Editorial.
- Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud Computing: Implementation, Management, and Security*. CRC Press. DOI: <https://doi.org/10.1201/9781439806814>.
- Sánchez, L. F., & Torres, M. E. (2021). Acceso y uso de la nube en Ecuador. *Journal of Digital Innovation*, 8(2), 123-137. <https://doi.org/10.5678/jdi.2021.82123>
- Santos Morón, M. (2020). Tratamiento de datos, sujetos implicados, responsabilidad proactiva. En I. González Pacanowka (Coord.), *Protección de Datos Personales* (561-615). Tirant.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11. DOI:10.1016/j.jnca.2010.07.006.
- Unión Internacional de Telecomunicaciones. (2020). *Índice Mundial de Ciberseguridad*. ITU Publicaciones. <https://www.itu.int/D-STR-GCI.01-2021-PDF-S.pdf>.
- Red Iberoamericana de Protección de Datos. (2022). Guía de implementación de cláusulas contractuales para la transferencia internacional de datos personales (TIPD). Red Iberoamericana. <https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf>
- Ustrán, E., & García, P. (2019). Transferencias Internacionales de Datos. En A. Rallo Lombarte (Dir.), *Tratado de Protección de Datos* (459-490). Tirant lo Blanch.
- Wugmeister, M., Retzer, K., y Rich, C. (2007). Global solution for cross-border data transfers: Making the case for corporate privacy rules. *Georgetown Journal of International Law*, 38(3), 449-498. <https://www.law.georgetown.edu/international-law-journal/>.

12. Legislación

- Decreto Ejecutivo No. 741 de la Presidencia de la República del Ecuador, que disuelve la Asamblea Nacional por grave crisis política y conmoción interna. *Registro Oficial Primer Suplemento, No. 312, de 17 de mayo de 2023*. <https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/18664-suplemento-al-registro-oficial-no-312>
- Ley Orgánica de Protección de Datos Personales, 2021, por la que se regula el derecho fundamental a la protección de datos personales en Ecuador. *Registro Oficial Quinto Suplemento, No. 459, de 26 de mayo de 2021*. <https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14857-quinto-suplemento-al-registro-oficial-no-459>
- Ley No. 172-13, 2013, que regula la protección de los datos personales en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos públicos o privados. *Gaceta Oficial, No. 10737, de 15 de diciembre de 2013*. <https://www.consultoria.gov.do/Consulta/Home/FileManagement?documentId=3371233&managementType=1>
- Lei 13.709 o Geral de Proteção de Dados Pessoais, 2018, por la que se regula el tratamiento de datos personales y la protección de los derechos fundamentales de libertad e intimidad

- y libre desarrollo de la personalidad. *Diário Oficial da União*, de 14 de agosto de 2018. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
- Ley 29.733 de Protección de datos personales, 2011, por la que se regula el derecho fundamental a la protección de datos personales a través de su adecuado tratamiento. *Diario Oficial El Peruano*, No. 445746, de 3 de julio de 2011. <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf>
- OECD/LEGAL/0188 OECD, providing the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data, in 2023. <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf>
- Oficio N°.T.321-SGJ-23-0143 de la Presidencia de la República del Ecuador, que designa y envía la terna de Superintendente de Protección de Datos Personales al Consejo de Participación Ciudadana y Control Social, de 29 de mayo de 2023.
- Oficio No.T.321-SGJ-23-0269 de la Presidencia de la República del Ecuador, que informa el retiro de la terna para designar al Superintendente de Protección de Datos Personales, de 19 de octubre de 2023.
- Oficio No.T.321-SGJ-23-0270 de la Presidencia de la República del Ecuador, que designa y envía la nueva terna de Superintendente de Protección de Datos Personales al Consejo de Participación Ciudadana y Control Social, de 19 de octubre de 2023.
- Oficio No. T.004-SGJ-24-0072 de la Presidencia de la República del Ecuador, que designa y envía la terna de Superintendente de Protección de Datos Personales al Consejo de Participación Ciudadana y Control Social, de 29 de enero de 2024.
- Reglamento General de la Ley Orgánica de Protección de Datos Personales, relativo a la normativa de aplicación de la Ley y la protección de los derechos y libertades fundamentales de los titulares de datos personales. *Registro Oficial, Tercer Suplemento*, No. 435, de 13 de noviembre de 2023. <https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/19663-tercer-suplemento-al-registro-oficial-no-435>
- Reglamento a la Ley 29.733 de Protección de datos personales, emitido mediante Decreto Supremo No. 003-2013-JUS que desarrolla a la Ley 29.733 a fin de garantizar el derecho fundamental a la protección de datos personales, regulando su adecuado tratamiento. *Diario Oficial El Peruano*, No. 491320, de 22 de marzo de 2013. <https://diariooficial.elperuano.pe/Normas/obtenerDocumento?idNorma=23>
- Reglamento (UE) N°. 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, que regula las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución. *Diario Oficial de la Unión Europea*, L 55/13, de 28 de febrero de 2011. <http://data.europa.eu/eli/reg/2011/182/oj>
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos. *Diario Oficial de la Unión Europea*, L119, de 4 de mayo de 2016. <http://data.europa.eu/eli/reg/2016/679/2016-05-04>
- Resolución No. CPCCS-PLE-SG-010-O-2024-0079 del Consejo de Participación Ciudadana y Control Social, que aprueba la terna enviada por el ejecutivo para la designación de la Autoridad de Protección de datos personales, de 6 de marzo de 2024. http://blogs.cpccs.gob.ec/biblioteca/DocumentosCPCCS/Comunicacion/2024/02/resolucion_no_cpccs_ple_sg_010_o_2024_0079.pdf
- Resolución No. CPCCS-PLE-SG-019-E-2024-0106 del Pleno del Consejo de Participación Ciudadana y Control Social, por la que se designa a Fabrizio Roberto Peralta Díaz como Superintendente de Protección de Datos Personales, de 28 de marzo de 2024.

http://blogs.cpccs.gob.ec/biblioteca/DocumentosCPCCS/Comunicacion/2024/04/resolucion_no_cpccs_ple_sg_019_e_2024_0106.pdf

WP 248 de la Comisión Europea, 2017, que regula las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y que determina si el tratamiento entraña un alto riesgo a efectos del Reglamento (UE) 2016/679, de 4 de octubre de 2017. <https://ec.europa.eu/newsroom/article29/items/611236/en>

WP 256 of the European Commission, 2017, which regulates the Setting up a table with the elements and principles to be found in Binding Corporate Rules, on 29 November 2017. <https://ec.europa.eu/newsroom/article29/items/614109>

13. Índice de Tablas

Tabla No. 1. Productos y Servicios del Grupo Empresarial Multinacional del Sector Industrial	6
Tabla No. 2. Metodología de cálculo para el Análisis de Riesgos en Protección de datos personales	22
Tabla No. 3. Cálculo del Riesgos Inherente en Protección de datos personales	23
Tabla No. 4. Interpretación de valores ajustados al riesgo inherente	23
Tabla No. 5. Resultados de la Riesgo Inherente en transferencia internacional de datos personales.	30
Tabla No. 6. Resultados de la Riesgo Residual en transferencia internacional de datos personales.	31
Tabla No. 7. Resultados de la Evaluación de Impacto en la transferencia internacional de datos personales.....	32

14. Índice de Gráficos

Gráfico No. 1. Elementos mandatorios de las normas corporativas vinculantes.....	21
---	----

15. Anexos

Anexo I

Normas Corporativas Vinculantes del Grupo Empresarial del Sector Industrial

1. Introducción

Grupo Empresarial Multinacional del Sector Industrial es un grupo empresarial ecuatoriano con presencia en la región LATAM que actúa con ética y responsabilidad corporativa, manteniendo su compromiso con la protección de datos personales en todas sus actividades en relación con nuestros clientes, empleados, socios comerciales y demás partes interesadas en todas las jurisdicciones en las que opera.

1.1. Descripción

“Reconocemos la importancia fundamental de resguardar la información personal y privada confiada a nosotros. Nuestras Normas Corporativas Vinculantes o NCV cumplen con los estándares éticos más altos, así como con las leyes aplicables de cada país en los que tenemos presencia. Nos comprometemos a garantizar la confidencialidad, integridad y disponibilidad de los datos personales que gestionamos”.

Desde 2023 Grupo Empresarial Multinacional del Sector Industrial implementó la Ley Orgánica de Protección de Datos Personales de Ecuador, que contempla las Normas Corporativas Vinculantes como mecanismo para garantizar la transferencia internacional de datos personales segura.

Este instrumento denominado Normas Corporativas Vinculantes se ha implementado cumpliendo los requisitos legales vigentes para conseguir la aprobación de la Autoridad de Protección de Datos Personales ecuatoriana al designarse y vincularse a las filiales del grupo en sus jurisdicciones continuando con las buenas prácticas en protección de datos personales iniciadas en Ecuador.

1.2 Acceso

Las Normas Corporativas Vinculantes de Grupo Empresarial Multinacional del Sector Industrial se encuentran disponibles a través del siguiente enlace: www.grupoempresarialmultinacionaldelsectorindustrial.com/ncv

La Superintendencia de Protección de Datos Personales de Ecuador es el organismo estatal que supervisa las NCV de Grupo Empresarial Multinacional del Sector Industrial.

2. *Binding Nature* o Naturaleza Vinculante

En un mundo cada vez más interconectado, es esencial mantener estándares consistentes en todas nuestras operaciones. Nuestras Normas Corporativas Vinculantes establecen los principios rectores que rigen nuestro comportamiento empresarial en áreas clave, como ética, gobernanza, sostenibilidad y responsabilidad social. Esto asegura que todas las filiales, independientemente de su ubicación geográfica, compartan los mismos valores fundamentales.

Reconocemos la importancia de respetar las leyes y regulaciones específicas de cada jurisdicción en la que operamos. Nuestras Normas Corporativas Vinculantes no solo establecen estándares generales, sino que también ofrecen flexibilidad para adaptarse a los requisitos locales. Esto garantiza el cumplimiento normativo en todas partes y refuerza nuestro compromiso con la legalidad y la responsabilidad.

Al adherirse nuestras filiales a las Normas Corporativas Vinculantes, no solo garantizamos la consistencia operativa, sino que también fortalecemos la reputación de nuestra marca a nivel

internacional. La confianza de nuestros clientes, socios comerciales y partes interesadas se construye sobre la base de la transparencia y la coherencia, lo que contribuye al crecimiento sostenible y al éxito a largo plazo de nuestro grupo empresarial.

El Grupo Empresarial Multinacional del Sector Industrial en Ecuador y en cada filial internacional realizarán tratamiento de datos personales y transferencias internacionales de datos personales, dentro del marco establecido por las NCV. El incumplimiento del contenido de las NCV acarrea consecuencias disciplinarias a nivel interno del Grupo.

3. Alcance

3.1 Jurisdicción

Las Normas Corporativas Vinculantes del grupo se aplican de manera uniforme en todos los países de América Latina donde operamos, con punto de partida en Ecuador, de acuerdo con el Anexo 3. Las NCV son de cumplimiento obligatorio para el desarrollo de todas las actividades que involucren la transferencia internacional de datos personales según el Anexo 1. Esta coherencia garantiza que nuestras prácticas comerciales y decisiones estén alineadas con los valores fundamentales de Grupo Empresarial Multinacional del Sector Industrial y cumplan con las leyes y regulaciones locales pertinentes.

3.2 Alcance territorial

Las NCV abarcan una amplia gama de áreas cruciales, especialmente las transferencias internacionales de datos personales que el Grupo Empresarial Multinacional del Sector Industrial requiere realizar para mantener sus operaciones habituales. Estas normas son aplicables a todas las entidades y empleados dentro de nuestro grupo empresarial, independientemente de su ubicación geográfica.

Por lo que, estamos comprometidos a mantener los más altos estándares éticos en todas nuestras actividades comerciales, contribuyendo así a la construcción de un entorno empresarial sostenible y responsable a nivel mundial.

Los principales beneficios que obtenemos en la aplicación material de nuestras NCV incluyen, pero no se limitan a:

1. Confianza del Cliente: Reforzamos la confianza de nuestros clientes al demostrar nuestro compromiso con prácticas empresariales éticas.
2. Atracción y Retención de Talentos: Las NCV atraen y retienen a profesionales comprometidos con los valores éticos y la responsabilidad corporativa.
3. Mitigación de Riesgos: Al adoptar un enfoque proactivo hacia la ética, reducimos los riesgos legales y reputacionales asociados con prácticas comerciales cuestionables.

4. Aplicación de los principios de protección de datos personales

En cumplimiento de la Ley Orgánica de Protección de Datos Personales y su Reglamento de aplicación, Grupo Empresarial Multinacional del Sector Industrial y sus filiales realizarán tratamiento de datos personales, y en concreto, transferencias internacionales de datos personales aplicando los principios que rigen la protección de datos personales y garantizando el correcto ejercicio de los derechos de los titulares de datos personales.

4.1 Tratamiento legítimo

Las actividades de tratamiento que realiza Grupo Empresarial Multinacional del Sector Industrial y sus filiales se encuentran debidamente legitimadas por justificaciones legales válidas de acuerdo con el artículo 7 de la LOPDP, contando con al menos una de las siguientes condiciones:

1. El titular haya otorgado su consentimiento de manera libre, voluntaria e informada al Grupo Empresarial Multinacional del Sector Industrial para alguna de las finalidades que constan en el Anexo 1.

2. El tratamiento de datos personales sea necesario para el cumplimiento de medidas contractuales o la correcta ejecución de un contrato.
3. El tratamiento de datos personales sea necesario para el cumplimiento de una obligación legal que mantenga el Grupo Empresarial Multinacional del Sector Industrial con las autoridades competentes.
4. El tratamiento de datos personales sea necesario por un interés legítimo de Grupo Empresarial Multinacional del Sector Industrial, luego de haber realizado la respectiva ponderación conforme lo exige el reglamento de aplicación de la LOPDP.

4.2 Transparencia

La transparencia es un elemento central de nuestras NCV. Creemos que la apertura y la honestidad son fundamentales para construir y mantener la confianza con nuestros colaboradores, clientes, proveedores y la sociedad en general. A través de la divulgación proactiva de información relevante por medio de los canales que pone a disposición el Grupo, buscamos ofrecer una visión clara de nuestras acciones y decisiones, demostrando nuestro compromiso con la integridad y la responsabilidad empresarial.

En Grupo Empresarial Multinacional del Sector Industrial, la transparencia no es simplemente un requisito, es un valor arraigado en nuestra cultura corporativa. Creemos que al ser abiertos acerca de nuestras prácticas comerciales y decisiones, fortalecemos nuestra relación con todas las partes interesadas y contribuimos a un entorno empresarial más ético y sostenible.

Por ello, continuamente nos aseguramos que las partes interesadas relacionadas con el Grupo Empresarial Multinacional del Sector Industrial y sus filiales en calidad de titulares tengan acceso a toda la información referente a las actividades de tratamiento de datos personales en un formato simple, claro y fácil de acceder, principalmente por medio de las políticas de protección de datos personales que hemos desarrollado.

4.3 Minimización y limitación

Grupo Empresarial Multinacional del Sector Industrial y sus filiales recopilan y tratan únicamente los datos personales relevantes, pertinentes y necesarios, asegurándose de que toda la información es la adecuada, actual y veraz, aplicando las medidas de seguridad necesarias.

Asimismo, el Grupo trata datos personales, en especial en el ámbito de transferencias internacionales de datos personales, limitándose únicamente a las finalidades que ha informado de manera previa a los titulares y por un plazo razonable para su conservación de acuerdo con la LOPDP.

4.4 Seguridad de la información

Grupo Empresarial Multinacional del Sector Industrial y sus filiales, en su plan de implementación de protección de datos personales, ha determinado y ejecutado medidas de control técnicas, organizativas, jurídicas, administrativas, tecnológicas y funcionales orientadas a prevenir la materialización de los riesgos identificados en las evaluaciones de impacto realizadas continuamente.

El Grupo ha adoptado un enfoque proactivo para garantizar la confidencialidad, integridad y disponibilidad de los datos que maneja en toda la organización a nivel internacional. Este compromiso con la seguridad de la información se refleja principalmente en los siguientes aspectos:

1. **Confidencialidad:** Implementamos medidas robustas para garantizar que la información confidencial sea manejada con la máxima seguridad. Esto incluye controles de acceso, cifrado y políticas claras sobre el manejo de datos sensibles.

2. **Integridad:** Nos comprometemos a mantener la integridad de la información en todo momento. Esto implica la implementación de controles de seguridad que evitan alteraciones no autorizadas y aseguran la precisión de los datos.
3. **Disponibilidad:** Reconocemos la importancia de la disponibilidad de la información para mantener la continuidad del negocio. A través de redundancias, respaldos regulares y planes de recuperación, garantizamos que la información crítica se encuentre siempre accesible.
4. **Cumplimiento Normativo:** Nos sometemos a auditorías internas periódicas, así como un plan de mejora continua para asegurar el cumplimiento continuo con las NCV y todas las leyes y regulaciones aplicables.

4.6 Responsabilidad proactiva y demostrada

Para el Grupo Empresarial Multinacional del Sector Industrial la responsabilidad proactiva es un pilar fundamental en su enfoque de negocio. Significa anticiparse a los desafíos y oportunidades, adoptando prácticas que aseguren un impacto positivo en todas las comunidades donde opera el Grupo.

A través de Registros de Actividades de Tratamiento, Evaluaciones de Impacto y gestión de riesgos, así como las Normas Corporativas Vinculantes del Grupo Empresarial Multinacional del Sector Industrial demuestran su compromiso con la responsabilidad proactiva. Adicional a las medidas mencionadas, el Grupo ha designado un delegado de Protección de Datos Personales aun cuando no está obligado a hacerlo como manifestación de buena práctica de protección de datos personales y en aplicación de la responsabilidad proactiva.

4.5 Ejercicio de derechos

Grupo Empresarial Multinacional del Sector Industrial y sus filiales ponen a disposición de sus titulares canales de atención a derechos de protección de datos personales por medio de los cuales se receptan y resuelven solicitudes de:

1. Acceso;
2. Rectificación;
3. Supresión;
4. Oposición; y,
5. No ser objeto de decisiones basadas en operaciones automatizadas.

En caso de requerir consultas adicionales sobre el ejercicio de derechos, o incluso hacer válido el contenido de las NCV, se encuentra a disposición el contacto del departamento de protección de datos personales de Grupo Empresarial Multinacional del Sector Industrial a través de la siguiente dirección de correo: protecciondedatos@grupoempresarialmultinacionaldelsectorindustrial.com

5. Delegado de protección de datos personales

Grupo Empresarial Multinacional del Sector Industrial ha designado como buena práctica de protección de datos personales un Delegado de Protección de Datos Personales cuyas funciones son las siguientes:

1. **Asesoramiento y Supervisión:** El DPD brinda asesoramiento sobre todas las cuestiones relacionadas con la protección de datos y supervisa la implementación de medidas de control de naturaleza técnicas, tecnológicas, administrativas, organizacionales y jurídicas en todas las áreas del Grupo.
2. **Colaboración con Autoridades de Protección de Datos:** Facilita la comunicación con las autoridades de protección de datos y actúa como punto de contacto principal en cuestiones de protección de datos personales.

3. Capacitación y Concienciación: Se encarga de sensibilizar continuamente a los empleados sobre la importancia de la protección de datos personales y brinda capacitación continua para garantizar el cumplimiento normativo.
4. Evaluación de Impacto de: Conduce evaluaciones de impacto de protección de datos personales para identificar y mitigar posibles riesgos asociados con el tratamiento de datos personales.

6. Capacitación al personal

Grupo Empresarial Multinacional del Sector Industrial y sus filiales tienen claro que la protección de datos es un esfuerzo colectivo que involucra a cada miembro de sus diferentes equipos. Por ello, se ha implementado un programa integral de capacitación que abarca todos los niveles y departamentos de nuestra organización, en especial aquellos que forman parte del Sistema de Gestión de Protección de Datos Personales. El personal recibe formación periódica para comprender la importancia de la protección de datos personales, las responsabilidades asociadas a ello y cómo aplicar las Normas Corporativas Vinculantes en las actividades que involucran transferencias internacionales de datos personales.

El fomento de la protección de datos personales es clave para mantener una cultura organizacional centrada en la protección de datos personales. Se organizan regularmente campañas de concientización para sensibilizar a los empleados sobre las últimas tendencias en protección de datos, riesgos potenciales y mejores prácticas. Además, se promueve un entorno en el que la comunicación abierta y la colaboración son fundamentales para fortalecer las defensas del Grupo contra las amenazas externas.

7. Mejora continua y auditoría

El Grupo Empresarial Multinacional del Sector Industrial ha implementado y mantiene operativo el Sistema de Gestión de Protección de Datos Personales, SGPD, que es responsable por evaluar el cumplimiento actual del Grupo frente a la regulación de protección de datos personales y mantener un control continuo de las medidas implementadas para proteger los datos personales y mitigar los riesgos identificados.

La mejora continua es el núcleo de la cultura organizacional de Grupo Empresarial Multinacional del Sector Industrial. El Grupo está comprometido con perfeccionar sus prácticas para adaptarse a las cambiantes regulaciones y expectativas del mercado. Para lograr esto, se ha implementado un enfoque basado en procesos que abarca todas las aristas de la gestión de datos personales. Regularmente se evalúan y actualizan nuestras políticas, procedimientos y controles para garantizar la eficacia y relevancia continua.

El equipo de expertos designado realiza auditorías internas periódicas para evaluar el cumplimiento de las políticas y procedimientos establecidos como parte del Plan de Auditoría del Grupo. También existe colaboración con auditores externos independientes para obtener una revisión imparcial y objetiva. Esta doble capa de auditoría garantiza una evaluación completa y precisa del sistema de protección de datos personales del Grupo.

8. Autoridades de control

Es obligación de Grupo Empresarial Multinacional del Sector Industrial y sus filiales cooperar y facilitar la información requerida a la Autoridad de Control de Protección de Datos Personales ecuatoriana y cumplir siempre sus decisiones y resoluciones.

9. Posibles conflictos normativos

En el supuesto de hecho que la normativa aplicable de una de las filiales internacionales de Grupo Empresarial Multinacional del Sector Industrial se contraponga a la ecuatoriana, la filial tendrá la obligación de reportar este hecho al Delegado de Protección de Datos Personales del Grupo.

El Grupo mantiene un enfoque colaborativo y de compromiso para resolver los conflictos normativos. Todo el equipo legal trabaja estrechamente con las filiales involucradas para

comprender plenamente las restricciones legales locales y explorar soluciones que permitan la alineación con las NCV sin infringir la normativa local aplicable.

En situaciones donde la adaptación directa resulta difícil o la normativa no lo permita, se buscarán alternativas creativas que preserven la esencia de las normas corporativas vinculantes sin comprometer la legalidad local. Esto puede incluir la implementación de procedimientos adicionales, capacitación especializada o la participación activa con las autoridades locales de control para encontrar soluciones viables.

El objetivo principal es alcanzar una armonización efectiva que permita a las filiales operar dentro de los límites legales locales sin sacrificar la integridad y los valores fundamentales del Grupo. Este enfoque proactivo refleja el compromiso continuo de Grupo Empresarial Multinacional del Sector Industrial con la ética empresarial y la construcción de relaciones sólidas en todas las jurisdicciones en las que opera.

10. Futuras actualizaciones

En función de posibles modificaciones normativas o adecuaciones a realizarse según nuevas decisiones de la Autoridad de Control, el Grupo Empresarial Multinacional del Sector Industrial deberá actualizar las normas corporativas vinculantes. En concordancia con ello, se deberá notificar inmediatamente a sus filiales y a la Superintendencia de Protección de Datos Personales de Ecuador sobre estos cambios, modificaciones o actualizaciones junto con una debida motivación que explique la razón del cambio realizado.

La página web de Grupo Empresarial Multinacional del Sector Industrial www.grupoempresarialmultinacionaldelsectorindustrial.com sirve como fuente centralizada para acceder a toda la información relevante. En dicho enlace se encontrarán las versiones más recientes de las normas corporativas vinculantes, junto con un historial detallado de revisiones para su referencia.

Además, se ha implementado un sistema de notificaciones por correo electrónico para aquellos interesados en recibir actualizaciones directamente en sus bandejas de entrada contando con su debido consentimiento.

Anexo II

Registro de Actividades de Tratamiento en Transferencias Internacionales

1. Información General – Datos de la organización

Rol de la Organización:	Responsable de tratamiento
Razón Social:	Grupo Empresarial Multinacional del Sector Industrial
Dirección:	Quito – Ecuador
Personal responsable del tratamiento:	Gerentes – Accionistas – Directorio
Sector de actividad:	Industrial y Comercialización de empaques flexibles
Marco normativo de aplicación:	Ley Orgánica de Protección de Datos Personales
Procesos relacionados con el tratamiento:	Comercial y Finanzas

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

2. Información General sobre el tratamiento

Proceso Interno	Transferencias Internacionales de datos personales
Áreas involucradas	Gerencia General Directorio

	Accionistas
Actividad de tratamiento	Transferencias Internacionales de datos personales entre empresas del grupo multinacional
Email del interlocutor del tratamiento	xyz@grupoempresarialmultinacionaldelsectorindustrial.com
Corresponsabilidad	Grupo Empresarial Multinacional del Sector Industrial.
Ámbito	Internacional

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

3. Finalidades de tratamiento

3.1. Tipo de Tratamiento

Finalidad	Base de legitimación	Justificación de legitimación
Comunicar, enviar y recibir los datos personales -accionistas, proveedores de servicios profesionales, trabajadores y otras partes interesadas- necesarios relativos a operaciones financieras, económicas, tributarias y comerciales	Art. 7.1.- Consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas (LOPD, 2021)	Consentimiento libre, voluntario, informado y expreso de las partes interesadas que se relacionan con el flujo de datos personales a nivel internacional

Envío de balances y flujo interno de las compañías	Art. 7.8.- Interés legítimo del responsable del responsable o tercero siempre que no prevalezca el interés o derechos fundamentales de los titulares (LOPDP, 2021)	Código Orgánico Tributario salvaguarda de derechos de la empresa
	Art. 7.2.- Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal (LOPDP, 2021)	Ley Orgánica de Compañías Código Orgánico Tributario
Envío de actas sobre juntas de accionistas	Art. 7.8.- Interés legítimo del responsable del responsable o tercero siempre que no prevalezca el interés o derechos fundamentales de los titulares (LOPDP, 2021)	Salvaguarda los derechos de la empresa
Envío de actas de junta de directorio	Art. 7.8.- Interés legítimo del responsable del responsable o tercero siempre que no prevalezca el interés o derechos fundamentales de los titulares (LOPDP, 2021)	Salvaguarda los derechos de la empresa
Gestión comercial	Art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Contrato mercantil
Cotizaciones de producto y servicios para clientes	Art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Propuesta de servicios

Notas de pedido de productos y servicios para clientes	Art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Propuesta de servicios Orden de compra
Envío de información de embarque para transporte de productos	Art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Orden de compra
Gestión de información de formas de pago	art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Contrato mercantil Orden de compra
Negociaciones	Art. 7.5.- Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable, encargado o un tercero legalmente habilitado (LOPDP, 2021)	Orden de compra Facturas
Gestión y elaboración documental	Art. 7.8.- Interés legítimo del responsable del responsable o tercero siempre que no prevalezca el interés o derechos fundamentales de los titulares (LOPDP, 2021)	Contrato mercantil Salvaguarda de derechos de la empresa

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

3.2. Número de sujetos afectados

Tipos de sujetos afectados	Cantidad de sujetos afectados
Potencial cliente persona natural	1-1000
Cliente persona natural	1-1000
Representantes, administradores o puntos de contacto de potencial cliente persona jurídica	1-1000
Representantes, administradores o puntos de contacto de cliente persona jurídica	1-1000
Posible proveedor persona natural	1-1000
Proveedor persona natural	1-1000
Representantes, administradores o puntos de contacto de posible proveedor persona jurídica	1-1000
Representantes, administradores o puntos de contacto de proveedor persona jurídica	1-1000
Accionistas	1-1000
Colaborador	1-1000

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

3.3. Categorías de datos objeto de tratamiento

Tipología de datos personales objeto de tratamiento		Justificación y Detalle
Datos Identificativos	Apellido y nombre	Expediente y Base de datos
	Número de cédula	
	Firma	
	Fecha de nacimiento	
	Lugar de nacimiento	
	Apellido y nombre de padre	
	Apellido y nombre de madre	
	Apellido y nombre de cónyuge	
Datos de Características Personales	Edad	Expediente y Base de datos
	Estado civil	
	Nacionalidad	
	Género	
	Características físicas o antropométricas	

	Fotografía	
	Dirección	
Detalles del empleo	Profesión	Expediente y Base de datos
	Cargo	
	Historial de trabajo	
	Dirección laboral	
	Correo electrónico empresarial	
	Remuneración	
Información comercial	Actividades y negocios	Expediente y Base de datos
	Licencias comerciales	
	RUC	
	Creaciones artísticas	
	Creaciones literarias, científicas o técnicas	
Datos económicos, financieros y seguros	Ingresos	Expediente y Base de datos
	Rentas	
	Inversiones	
	Créditos	

	Préstamos	
	Avales	
	Movimiento de acciones	
	Datos económicos de nómina	
	Deducciones impositivas	
	Historial de créditos	
	Beneficios	
Datos de transacciones, bienes y servicios	Bienes patrimoniales	Expediente y Base de datos
	Garantías	
	Número de cuenta	
Datos de tráfico o localización	Código postal	Expediente y Base de datos
Otros datos	Firma física	Expediente y Base de datos
	Firma electrónica	
	Clave única	

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Tipología de datos personales objeto de tratamiento		Detalle	Justificación del levantamiento de prohibición de tratamiento de datos de categoría especial
Datos sensibles	Datos genéticos	Tipo de sangre	El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
	Datos de salud	Donador de órganos	
	Datos genéticos	Porcentaje de discapacidad	El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del derecho laboral y de la seguridad y protección social.
	Datos de salud	Tipo de discapacidad	
	Datos biométricos	Código dactilar	
	Datos biométricos	Huella dactilar	
	Identidad de género	Sexo	El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

3.4. Temporalidad de conservación de datos en relación con el tratamiento

Extensión del tratamiento	Detalle
Mensual	Cuatrimestral Semestral

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

3.5. Temporalidad de conservación de datos en relación con el tratamiento

Tipo de tratamiento	Tipo de documento	Referencia legal	Borrado	¿Aplicados en este tratamiento?
Digitalización, registro, consulta y conservación	Archivo digital de alta gerencia	Relación entre empresas del grupo multinacional	Plazo de conservación tributario	Si

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

3.6. Extensión geográfica del tratamiento

Extensión geográfica	Detalle
Internacional	República Dominicana Brasil Perú

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

3.7. Información de datos

Especificaciones del tratamiento	Detalle
¿El tratamiento de datos personales tiene la finalidad de vigilar, supervisar o evaluar de forma sistemática al titular de datos personales? (LOPDP, 2021, Norma que regula el tratamiento de datos [NRTD])	No
El tratamiento detecta patrones de comportamiento, elabora perfiles, monitorea a los titulares o a través del tratamiento se permite hacer cualquier tipo de seguimiento al titular (LOPDP, 2021, NRTD)	No
¿El tratamiento se refiere a datos que requieren protección reforzada? (LOPDP, 2021, NRTD)	Si
¿El tratamiento de datos involucra contacto con los titulares que pueda considerarse intrusivo o invasivo? (LOPDP, 2021, NRTD)	No
¿El tratamiento de datos se orienta a la elaboración de perfiles, la categorización o segmentación para la toma de decisiones? (LOPDP, 2021, NRTD)	Si
¿El tratamiento de datos implica la toma de decisiones automatizadas, sin que exista la intervención de personas en la decisión que valora resultados? (LOPDP, 2021, NRTD)	No
La finalidad del tratamiento, ¿corresponde con la finalidad para la que se recogieron los datos? (LOPDP, 2021, NRTD)	Si
¿El tratamiento prevé que un número elevado de personas (más de las necesarias) tenga acceso a los datos personales? (LOPDP, 2021, NRTD)	No
¿Se utilizan datos no anonimizados para fines de estadísticas, históricos o de investigación?	No

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

4. Tecnologías aplicadas para el tratamiento

Tipo de activo		
Tipo de instalación		Detalle y dirección
instalaciones	Local en servidor	Planta central
	almacenamiento en la nube para backup	Amazon S3
	Almacenamiento en servidor local para backup	Planta central
	Archivos físicos	Planta central

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Tipo de dispositivo	
Soportes de Información	Desktop
	Laptop
	Celular

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

Tipo de archivo	
Redes de comunicación	LAN
	WAN

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

5. Intervinientes en el tratamiento

Personas que procesan u operan los activos indicados	Detalle	Número de personas
Representante del área de Finanzas	Gerente financiero	1
Representante del área Comercial	Gerente comercial	1
Accionistas	Grupo Empresarial Multinacional del Sector Industrial	1-25
Trabajadores área comercial	Grupo Empresarial Multinacional del Sector Industrial	1-100

Trabajadores área financiera y contable	Grupo Empresarial Multinacional del Sector Industrial	1-100
--	---	-------

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

6. Sistemas o aplicativos utilizados en el tratamiento

	Nombre de la aplicación/sw	Detalle
Aplicaciones informáticas (software)	S/4 HANA	ERP
	Microsoft 365	Ofimática

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021).

7. Ciclo de vida y operaciones de tratamiento con datos personales

Fase I – Recogida	
Obtención de datos personales	Detalle
Formularios en papel	Órdenes de compra Contratos Documentos personales

Formularios web	Base de datos
-----------------	---------------

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Fase II – Registro	
Almacenamiento de datos personales	Detalle
Almacenamiento	Archivo físico Base de datos
Conservación	7 años en concordancia con la normativa tributaria

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Fase III – Tratamiento / Uso	
Conjunto de operaciones de tratamiento para datos personales	Detalle
Consulta	Base de datos Contratos Mercantiles Documentación financiera

Utilización	Transferencia y Comunicación Gestión Financiera
-------------	--

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Fase IV – Transferencia / Comunicación	
Transferencia o comunicación de datos personales y sus intervinientes	Detalle
Transferencia Internacional	Operaciones financieras y comerciales que incluyen datos personales, transferidas en el Grupo Empresarial Multinacional del Sector Industrial

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

Fase V – Finalización	
Eliminación o conservación de datos personales	Detalle
Conservación	7 años en concordancia con la normativa tributaria

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021).

8. Procedencia de Evaluación de Impacto en protección de datos personales

Análisis de Procedencia EIPD		
Artículo LOPDP	Criterio	
Art. 42 Literal a	El tratamiento consiste en una evaluación sistemática y exhaustiva de aspectos personales basada en un tratamiento automatizado	
	Si	
	No	No se ha establecido un sistema predeterminado, periódico o automatizado para el presente tratamiento
Art. 42 Literal b	El tratamiento a gran escala de categorías especiales de datos	
	Si	
	No	El volumen de datos personales es inferior a 10.000 y no se recogen categorías especiales
Art. 42 Literal b	Tratamiento a gran escala de datos personales relativos a condenas e infracciones penales	
	Si	
	No	No se recogen datos relativos a pasado judicial para el presente tratamiento
Art. 42 Literal c	Observación sistemática a gran escala de una zona de acceso público	
	Si	

No	Grupo Empresarial Multinacional del Sector Industrial se conforma únicamente por empresas privadas
----	--

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

9. Evaluación de Impacto en protección de datos personales

Evaluación de Impacto en Protección de Datos Personales	
Juicio de Idoneidad	
El tratamiento es adecuado para el fin perseguido	
Si	El presente tratamiento es pertinente y no excede los límites de lo necesario para cumplir su finalidad
No	
Juicio de Necesidad	
La finalidad puede alcanzarse de otro modo menos lesivo	
Si	
No	El presente tratamiento se ha limitado al mínimo necesario en la recolección y tratamiento de datos personales, un tratamiento distinto afectaría la calidad, veracidad y confidencialidad de la información

Juicio de Proporcionalidad	
La gravedad del riesgo para los derechos y libertades y su intromisión es adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de la actividad de tratamiento	
Si	Al tratarse de un tratamiento no exhaustivo ni sistemático, la urgencia en que se realiza es adecuada y garantiza en gran medida que los riesgos se mantengan al mínimo
No	
El tratamiento supone una negación al derecho a la protección de datos personales	
Si	
No	El Grupo de empresas pone a disposición diferentes canales de atención para las partes interesadas que desean ejercer sus derechos, así como la designación de un DPD como buena práctica de protección de datos personales

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

10. Análisis de Riesgos en protección de datos personales

Riesgos				
Operaciones relacionadas con los fines de tratamiento	Localización	Identificación unívoca	Decidir sobre el acceso a servicios financieros	Conservación con fines de archivo
	x	X	x	x

Tipos de datos utilizados	Documentos personales	Situación económica	Estado financiero	Datos de medios de pago	Datos y metadatos de las comunicaciones electrónicas y datos inferidos de las comunicaciones electrónicas
	x	X	x	x	x
Extensión y alcance del tratamiento	La duración del tratamiento es elevada			Alcance geográfico elevado	
	X			x	
Categorías de titulares	Empleados				
	x				
Factores técnicos del tratamiento	Servicios web		Aplicaciones móviles		
	X		x		
Efectos colaterales del tratamiento	Podría determinar la situación financiera	Podría determinar la solvencia patrimonial	Pudiera privar a los afectados de sus derechos y libertades		Posible perjuicio económico significativo

	x	X	x	x
Categoría del responsable/encargado	Empleador			
	x			
Brechas de seguridad	Confidencialidad	Disponibilidad		
	X	x		

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021), y, Evaluador de riesgos de la Agencia Española de Protección de Datos Personales (2024).

11. Riesgo Inherente

Riesgo Inherente	
Nivel de riesgo inherente	8
Impacto	Alto
Probabilidad	Alta

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contine la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

12. Medidas de control implementadas

Medida	Naturaleza	Principios y derechos	Referencia
Normas Corporativas Vinculantes	Jurídico/Organizativo	Legitimidad	Normas Corporativas Vinculantes de Grupo Empresarial Multinacional del Sector Industrial ubicado en la página web
		Transparencia	
		Minimización	
		Limitación	
		Seguridad	
		Responsabilidad proactiva	

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).

13. Riesgo Residual

Nivel de Riesgo Residual	
Nivel de riesgo residual	3
Impacto	Menor
Probabilidad	Improbable

Fuente: Elaboración propia a partir de la Ley Orgánica de Protección de Datos Personales que contiene la Norma que regula el tratamiento de datos personales (2021) y el Reglamento a la Ley Orgánica de Protección de Datos Personales (2023).