RESOLUCIÓN Nº SPDP-SPD-2026-0037-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que de acuerdo con el número 8 del artículo 11 de la Constitución de la República del Ecuador ("CRE"), *"[e]l contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas",* a la par que el numeral 9 de este mismo artículo determina que *"*[e]*l más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución"*;

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

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

Que a través de la Ley Orgánica de Protección de Datos Personales ("LOPDP") se creó la Superintendencia de Protección de Datos Personales ("SPDP") como un órgano de control, con potestad sancionatoria, de administración desconcentrada, con personalidad jurídica y autonomía administrativa, técnica, operativa y financiera, cuyo máximo titular es, de acuerdo con el inciso primero del artículo 77 ídem, el Superintendente de Protección de Datos Personales;

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

Que el artículo 3 de la LOPDP establece que *"[s]in perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando: 1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional; 2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional; 3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y, 4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público"*;

Que, además de los principios establecidos en la CRE, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la LOPDP se rige por los de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad del tratamiento, confidencialidad, calidad y exactitud, conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, aplicación favorable al titular e independencia del control, tal cual lo determina el artículo 10 del aquí citado cuerpo legal;

Que el artículo 20 de la LOPDP le reconoce al titular el derecho que tiene para *"(...) no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de*

procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales (...)";

Que el artículo 29 del Reglamento General de la LOPDP ("RGLOPDP") define a la evaluación de impacto como el *"análisis preventivo, de naturaleza técnica, mediante el cual el responsable valora los impactos reales del tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios y el respeto de los derechos y de las obligaciones"* que estuvieren establecidos en la normativa aplicable;

Que el artículo 58 del RGLOPDP le impone al responsable del tratamiento la obligación de *"aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos que realiza es conforme con la normativa",* para lo cual habrá de tener en cuenta la naturaleza, el ámbito, la finalidad del tratamiento y los riesgos;

Que el artículo 59 del RGLOPDP instituye que, en lo tocante a las medidas de protección de datos desde el diseño, el responsable, de manera previa al tratamiento, está obligado a *"establecer las medidas técnicas y organizativas adecuadas para aplicar los principios establecidos en la normativa de forma eficaz, y proteger los derechos de los titulares (...)"*, en cuyo caso habrá de tener en cuenta la naturaleza, ámbito y finalidad del tratamiento, los riesgos de diversa probabilidad y gravedad asociados al tratamiento, el estado de la técnica y el coste de aplicación;

Que el artículo 60 del RGLOPDP, en relación con las medidas de protección por defecto, compele al responsable del tratamiento a adoptar las de carácter técnico y las organizativas que fueren adecuadas *"para garantizar que, mediante ajustes (...), solo puedan tratarse aquellos datos personales cuyo tratamiento sea necesario para la respectiva finalidad específica del tratamiento",* de tal manera que *"los datos no puedan ser accesibles a un número indefinido de personas de forma automatizada" (...)"*;

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

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

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

Que, de igual manera, con ocasión del XVII Encuentro Iberoamericano de la RIPD se aprobaron, el 21 de junio del 2019, las Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial, en las que, al aludir sobre el impacto de la regulación del tratamiento de datos personales en la inteligencia artificial, se declara que tal regulación no debe tener solamente en cuenta *"los intereses del titular del dato",* sino que, también, debe reconocer *"la necesidad de los datos para la realización de diversas actividades lícitas, legítimas y de interés general o particular",* de modo tal que *"la normatividad no se opone al tratamiento, sino que exige que el mismo esté rodeado de garantías adecuadas",* con el objetivo último de *"evitar*

cualquier abuso que pueda generar una amenaza o vulneración de los derechos humanos de los titulares de los datos";

Que la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, con el voto conforme de sus ciento noventa y tres Estados miembros, aprobó, el 23 de noviembre del 2021, la Recomendación sobre la Ética de la Inteligencia Artificial, en la que se consagran los principios de proporcionalidad e inocuidad; de seguridad y protección; de equidad y no discriminación; de sostenibilidad; el del derecho a la intimidad y protección de datos; de supervisión y decisión humanas; de transparencia y explicabilidad; de responsabilidad y rendición de cuentas; de sensibilidad y educación; y, de gobernanza y colaboración adaptativas y de múltiples partes interesadas;

Que mediante acuerdo ministerial N° MINTEL-MINTEL-2025-0030, publicado en el Suplemento del Registro Oficial N° 206 del 19 de enero del 2026, el Ministro de Telecomunicaciones y de la Sociedad de la Información expidió la Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en el Ecuador ("Estrategia IA-MINTEL");

Que de acuerdo con el Índice Latinoamericano de Inteligencia Artificial, citado en la Estrategia IA-MINTEL, el Ecuador *"se encuentra en una posición intermedia-baja en la región en cuanto a preparación para la IA, con desafíos importantes en las tres dimensiones evaluadas"* (p. 23), la de gobernanza entre ellas, por cuanto en lo que atañe al marco regulatorio *"[s]igue sin normativa específica para IA, aunque hay avances en protección de datos personales y ciberseguridad"* (p. 25);

Que, de igual manera, en la Estrategia IA-MINTEL se reconoce expresamente que *"[e]l uso masivo de datos personales en sistemas basados en IA requiere garantías más robustas para proteger la privacidad de los ciudadanos"* (p. 26), ello a pesar de identificar como una fortaleza la existencia de *"[u]n marco legal de protección de datos personales reciente y alineado con estándares internacionales"* (p. 27);

Que, asimismo, en la Estrategia IA-MINTEL se declara, como uno de sus principios rectores, que se respete y promueva *"[l]a privacidad y la protección de datos personales de los usuarios (...) en cumplimiento irrestricto de sus derechos conforme a lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, demás legislación y normativa local y los estándares internacionales vigentes y aplicables"*, para lo cual se deberá asegurar *"que los datos personales sean tratados únicamente para fines legítimos, explícitos y determinados, minimizando su uso al estrictamente necesario y garantizando el consentimiento informado, libre y expreso de los titulares de los datos, salvo las excepciones previstas en la normativa vigente"* (p. 31);

Que es necesario afianzar y coadyuvar a la promoción y el respeto de la privacidad y la protección de los datos personales, que consta establecido como principio rector en la Estrategia IA-MINTEL, y tanto más si, por mandato del artículo 227 de la CRE, la administración pública debe también regirse por el principio de coordinación;

Que los contenidos de las recomendaciones y demás documentos previamente enunciados —sin perjuicio de los mandatos constitucionales, legales y reglamentarios también citados— dotan de coherencia técnica y legitimidad normativa al marco regulatorio nacional, aseguran su compatibilidad con estándares ampliamente aceptados en los ámbitos regional y global, constituyen instrumentos orientadores que facilitan la aplicación de los principios de protección de datos en entornos automatizados y refuerzan la interpretación sistemática de los derechos del titular frente al uso de tecnologías emergentes;

Que la Codificación del Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la SPDP ("Estatuto"), aprobada y expedida mediante resolución Nº SPDP-SPD-0030-R, fue publicada en el Tercer Suplemento del Registro Oficial Nº 339 del 3 de agosto del 2026;

Que en el artículo 1 del Estatuto la SPDP declara que *"se alinea con su misión y define su Estructura Organizacional sustentada en su base normativa y su direccionamiento estratégico institucional, los cuales serán determinados en su Planificación Estratégica Institucional, Modelo de Gestión Institucional y Matriz de Competencias"*;

Que en el apartado 12.1.3.2. del Estatuto se ha previsto, como una de las atribuciones de la Intendencia General de Regulación de Protección de Datos Personales ("IRD"), la de *"[d]irigir y proponer la elaboración de las propuestas o proyectos normativos para crear, reformar o derogar los actos normativos, sean estos políticas, directrices, reglamentos, resoluciones, lineamientos, normas técnicas, oficios circulares, etcétera, necesarios para el ejercicio de todas las competencias y atribuciones propias de la SPDP, con los previos informes técnicos de las unidades administrativas sustantivas y adjetivas relacionadas con el ámbito de aplicación de tales normas; así como, todos aquellos actos normativos relacionados con el ejercicio, tutela y procedimientos administrativos de gestión que garanticen a las personas naturales la plena vigencia de sus derechos y deberes previstos en la LOPDP y su Reglamento General"*;

Que, de igual manera, en el apartado 12.1.3.3. del Estatuto, se le atribuye a la IRD la responsabilidad de *"[d]irigir y proponer la presentación al Superintendente de Protección de Datos Personales de las propuestas de normas, reglamentos, directrices, resoluciones, normas técnicas, oficios circulares, etcétera, vinculados con la regulación de protección de datos personales, para su expedición"*;

Que a través de la resolución Nº SPDP-SPD-2026-0035-R del 20 de agosto del 2026, publicada en el Registro Oficial Nº 363 del 7 de septiembre del 2026, se expidieron las disposiciones y delegaciones de competencias a los servidores públicos de la SPDP;

Que por virtud del apartado 1.1. de la mencionada resolución Nº SPDP-SPD-2026-0035-R, le fueron delegadas al Intendente General de Regulación de Protección de Datos Personales la competencia para *"[p]roponer normativa regulatoria en materia de protección de datos personales para la aprobación, mediante resolución, del Superintendente de Protección de Datos Personales"*;

Que a través de la resolución N° SPDP-SPD-2024-0022-R, publicada en el Registro Oficial N° 734 del 31 de enero del 2025, se expidió el Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la SPDP;

Que mediante resolución Nº SPDP-SPDP-2024-0018-R, publicada en el Registro Oficial Nº 679 del 8 de noviembre del 2024, se expidió el Reglamento para la Elaboración y Aprobación del Plan Regulatorio Institucional ("PRI");

Que mediante la resolución N° SPDP-SPD-2025-0050-R del 30 de diciembre del 2025 se aprobó el PRI 2026;

Que el PRI 2026 fue reformado a través del informe N° SPDP-IRD-2026-0035-R del 22 de mayo del 2026, dentro del cual se ha establecido la necesidad de expedir **la reforma a la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** aprobada, en su día, mediante resolución Nº SPDP-SPD-2026-0009-R del 12 de febrero del 2026, que se publicó en el Registro Oficial N° 240 del 10 de marzo del 2026;

Que la IRD, mediante el informe técnico Nº INF-SPDP-IRD-2026-0038 del **3** de **junio** del **2026,** justificó la pertinencia de **reformar la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** dado que, *"la reforma a la Resolución Nº SPDP-SPD-2026-0009-R resulta pertinente y normativamente necesaria, en tanto contribuye a fortalecer la seguridad jurídica para los sujetos regulados así como para la ciudadanía, ya que asegura la proporcionalidad de las obligaciones regulatorias y garantiza una aplicación razonable y viable de la normativa de protección de datos personales en el uso de sistemas de inteligencia artificial"*;

Que por medio del memorando **N° SPDP-IRD-2026-0102-M,** suscrito el **3** de **junio** del **2026,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") tanto el proyecto normativo denominado **Reforma a la Resolución N° SPDP-SPD-2026-0009-R que Expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** como el informe técnico **N° INF-SPDP- IRD-2026-0038,** para que, dentro del término de diez (10) días, se pronuncie sobre la concordancia con la normativa y la legalidad, de conformidad con lo dispuesto en la resolución N° SPDP-SPDP-2024-0022-R;

Que a través del informe jurídico **N° INF-SPDP-DAJ-2026-0024,** remitido a la IRD mediante memorando **N° SPDP-DAJ-2026-0076-M** del **17** de **junio** del **2026,** la DAJ validó el proyecto normativo denominado **Reforma a la Resolución N° SPDP-SPD-2026-0009-R que Expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** por cuanto cumple con el principio de legalidad, no vulnera ni contradice las normas matrices que integran el ordenamiento jurídico aplicable y coadyuva al cumplimiento de los objetivos y atribuciones de la Superintendencia de Protección de Datos Personales; y, por ello, recomendó *"continuar con el procedimiento previsto en el Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales, a fin de proseguir con las etapas correspondientes para la expedición de la reforma normativa propuesta"*;

Que mediante el memorando **N° SPDP-IRD-2026-0109-M** suscrito el **18** de **junio** del **2026,** la IRD solicitó a las unidades administrativas de la SPDP que procedan con las acciones pertinentes, a fin de que publiquen el proyecto de **Reforma a la Resolución N° SPDP-SPD-2026-0009-R que Expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** en la página web institucional y en las redes sociales de la SPDP, para que esté disponible para la ciudadanía, las organizaciones de la sociedad civil o los interesados en general, desde el **19** de **junio** del **2026** al **16** de **julio** del **2026,** inclusive, con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que, para cumplir con la resolución Nº SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización del proyecto de **Reforma a la Resolución N° SPDP-SPD-2026-0009-R que Expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** dentro del término de veinte (20) días, de conformidad con el artículo 12 de la mencionada resolución;

Que a través del informe técnico **Nº INF-SPDP-IRD-2026-0056,** suscrito el **24** de **agosto** del **2026,** la IRD incorporó las observaciones y aportes que se consideraron relevantes y adecuados, previa justificación de las modificaciones realizadas al proyecto normativo;

Que mediante memorando **N° SPDP-IRD-2026-00150-M** suscrito el **24** de **agosto** del **2026,** notificado al despacho el **24** de **agosto** del **2026,** la IRD remitió todo el expediente al Superintendente de Protección de Datos Personales para que realice las observaciones correspondientes o, en su caso, para que lo apruebe;

Que mediante el memorando **N° SPDP-SPD-2026-0157-M** del **3** de **septiembre** del **2026,** el suscrito Superintendente de Protección de Datos Personales comunicó a la IRD las observaciones que realizó al proyecto; y, además, solicitó que aquellas sean revisadas de conformidad con el artículo 14 del Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

Que mediante el memorando N° **SPDP-IRD-2026-164-M** del **8** de **septiembre** del **2026,** la IRD puso en conocimiento del Superintendente de Protección de Datos Personales el proyecto que contiene la **Reforma a la Resolución N° SPDP-SPD-2026-0009-R que Expide la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial,** debidamente subsanado, de conformidad con el artículo 14

del aludido Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias,

RESUELVE:

REFORMAR LA RESOLUCIÓN N° SPDP-SPD-2026-0009-R, PUBLICADA EN EL REGISTRO OFICIAL N° 240 DEL 10 DE MARZO DEL 2026, QUE EXPIDIÓ LA NORMA GENERAL PARA LA GARANTÍA DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN EL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Art. 1.- El artículo 1 dirá:

*"**Art. 1.-** Esta norma general tiene por objeto garantizar la aplicación de los principios, derechos y obligaciones previstos en la LOPDP, en el RGLOPDP y en la normativa secundaria expedida por la SPDP, que serán de obligatorio cumplimiento para los responsables del tratamiento —así como para los encargados que tuvieren acceso, visibilidad o control efectivo de los datos objeto de tratamiento— siempre y cuando desarrollen, entrenen, implementen, desplieguen y/o provean sistemas de inteligencia artificial que traten datos personales de titulares ecuatorianos, con independencia de la ubicación física del sistema o del proveedor.*

Tales responsables y encargados del tratamiento, en función de los riesgos identificados en el tratamiento de datos que se efectuare, deberán implementar las medidas de seguridad que fueren pertinentes, de conformidad con lo previsto en la LOPDP, el RGLOPDP y la normativa secundaria emitida por la SPDP.

Esta norma general no se aplicará en los sistemas de inteligencia artificial que no procesaren datos personales, considerando el ámbito de aplicación material y territorial establecido en la LOPDP".

Art. 2.- En el artículo 2 agréguense las siguientes definiciones:

*"**2.5. Acceso a datos personales:** Es la posibilidad, directa o indirecta, permanente, temporal u ocasional de conocer, consultar, recibir, recuperar, extraer, utilizar, comunicar, transferir, almacenar o de cualquier otra forma interactuar con datos personales tratados mediante sistemas de inteligencia artificial, independientemente del medio, mecanismo, interfaz, modalidad técnica o nivel de acceso empleado. El acceso podrá producirse con independencia de que los datos personales fuesen tratados de forma individualizada, agregada, seudonimizada, cifrada o mediante cualquier otra modalidad que permitiese, directa o indirectamente, su conocimiento o utilización.*

***2.6. Visibilidad de datos personales:** Es la posibilidad, directa o indirecta de identificar, observar, conocer, inferir, consultar o tener conocimiento de la existencia, contenido, características, estructura, comportamiento, disponibilidad, ubicación, flujo, tratamiento o resultados asociados a datos personales tratados mediante sistemas de inteligencia artificial, aun cuando no existiere la posibilidad de acceder directamente a la totalidad de dichos datos. La visibilidad podrá derivarse de capacidades técnicas, funcionales, contractuales, organizativas o de cualquier otra circunstancia que permitiese conocer o inferir información relativa a los datos personales o a su tratamiento.*

***2.7. Control efectivo de datos personales:** Es la existencia de la capacidad, facultad, posibilidad o influencia, directa o indirecta de carácter técnico, contractual, jurídico, económico u organizativo, para intervenir, determinar, modificar, limitar, autorizar, condicionar, supervisar o influir, total o parcialmente, sobre los datos personales, las operaciones de tratamiento, los sistemas de inteligencia artificial*

utilizados para su tratamiento, o sobre las finalidades, medios o resultados de dicho tratamiento. El control efectivo podrá existir incluso cuando no se ejerciere materialmente la facultad o capacidad de intervención, siendo suficiente la posibilidad real de ejercerla, por sí mismo o a través de terceros".

Art. 3.- El artículo 4 dirá:

***"Art. 4.-** Los responsables del tratamiento, así como los encargados que tuvieren acceso, visibilidad o control efectivo sobre los datos personales objeto de tratamiento, en el marco del uso de sistemas de inteligencia artificial, garantizarán los derechos reconocidos en la LOPDP así como el acceso a los mecanismos para su ejercicio, de conformidad con lo previsto en el RGLOPDP".*

Art. 4.- El inciso primero del artículo 5 dirá:

***"Art. 5.-** Los responsables del tratamiento, así como los encargados que tuvieren acceso, visibilidad o control efectivo sobre los datos personales objeto de tratamiento y que trataren datos personales en sistemas de inteligencia artificial, obligatoriamente: (...)".*

Art. 5.- En el artículo 5 añádase, como inciso final, lo siguiente:

"Cuando el encargado del tratamiento proveyere, desarrollare o mantuviere sistemas de inteligencia artificial, proporcionarán al responsable del tratamiento toda la información suficiente sobre el funcionamiento general del sistema, sus limitaciones relevantes, riesgos previsibles y medidas de control implementadas, en la medida que fuere necesaria para que el responsable pueda cumplir las obligaciones previstas en la normativa de protección de datos personales, sin que esto implique la difusión de los secretos comerciales, industriales o de propiedad intelectual del encargado del tratamiento".

Art. 6.- El artículo 6 dirá:

***"Art. 6.-** Los responsables del tratamiento, así como los encargados que tuvieren acceso, visibilidad o control efectivo sobre los datos personales objeto de tratamiento, de manera previa al desarrollo del sistema de inteligencia artificial y siempre que trataren datos personales, deberán realizar la gestión de riesgos y, cuando correspondiere, la evaluación de impacto del tratamiento de datos personales ("EIPD"), de conformidad con lo establecido en la LOPDP, el RGLOPDP y la normativa secundaria emitida por la SPDP".*

Art. 7.- El primer inciso del artículo 7 dirá:

***"Art. 7.-** Los responsables del tratamiento, así como los encargados que tuvieren acceso, visibilidad o control efectivo sobre los datos personales objeto de tratamiento, deberán, de forma permanente y continua, implementar las medidas de seguridad adecuadas establecidas en la normativa de protección de datos personales para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades en los sistemas de inteligencia artificial. En consecuencia: (...)".*

Art. 8.- El artículo 8 dirá:

***"Art. 8.-** Los responsables del tratamiento, así como los encargados que tuvieren acceso, visibilidad o control efectivo sobre los datos personales objeto de tratamiento, que, mediante el uso de sistemas de inteligencia artificial, incumplieren lo establecido en la LOPDP, el RGLOPDP y esta norma general, serán sancionados de conformidad con el régimen sancionatorio legalmente previsto para el efecto.*

Los encargados que alegaren la inexistencia de acceso, visibilidad o control efectivo sobre los datos personales, deberán implementar y conservar evidencia suficiente que permita acreditar dicha circunstancia ante la SPDP cuando ella así lo requiriese".

Art. 9.- Luego del artículo 10, añádase lo siguiente:

"DISPOSICIONES GENERALES

Primera.- *Las obligaciones, responsabilidades y efectos jurídicos previstos en esta norma general serán exigibles a los encargados del tratamiento únicamente respecto de aquellas operaciones o fases del tratamiento sobre las cuales tuvieren acceso, visibilidad o control efectivo de los datos personales, de conformidad con la naturaleza de los servicios prestados y las instrucciones impartidas por el responsable del tratamiento.*

La presente disposición no constituirá una exoneración general de responsabilidad para los encargados del tratamiento, sino una delimitación funcional y proporcional de las obligaciones derivadas de esta norma general, en observancia de los principios de responsabilidad proactiva, necesidad y proporcionalidad.

Segunda.- *La ausencia de acceso, visibilidad o control efectivo del encargado no le eximirá del cumplimiento de las disposiciones legales, reglamentarias y de normativa secundaria que fuese aplicable".*

DISPOSICIÓN FINAL

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

Dada y firmada en Quito, D. M., el 9 de septiembre del 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FABRIZIO ROBERTO PERALTA DIAZ

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES