RESOLUCIÓN Nº SPDP-SPD-2025-0003-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el numeral 19 del artículo 66 de la Constitución de la República del Ecuador garantiza y reconoce a las personas *"[e]l 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 1 de la Ley Orgánica de Protección de Datos Personales ("LOPDP") declara, como su objetivo y finalidad, *"(...) garantizar el ejercicio del derecho de protección de datos personales, que incluye el acceso y decisión sobre información y datos de ese carácter, así como su correspondiente protección (...)"*;

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

Que el artículo 40 de la LOPDP determina *"(...) [p]ara el análisis de riesgos, (...) el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras: 1) Las particularidades del tratamiento; 2) Las particularidades de las partes involucradas; y, 3) Las categorías y el volumen de datos personales objeto de tratamiento"*;

Que, por un lado, el artículo 42 de la LOPDP exige al responsable del tratamiento de datos realizar *"(...) una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera";* y, por otro, determina que *[l]a evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de: a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales; b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, o c) Observación sistemática a gran escala de una zona de acceso público. (...)"*;

Que el artículo 29 del Reglamento General de la Ley Orgánica de Protección de Datos Personales, (RGLOPDP), respecto a la evaluación de impacto señala que *"(...) consiste en un 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 establecidas en la Ley Orgánica de Protección de Datos Personales, este Reglamento y demás normativa aplicable"*;

Que el artículo 30 del RGLOPDP establece que *"(...) La evaluación de impacto tiene por objeto: 1. Identificar y describir los riesgos potenciales y probables de determinados tratamientos de datos personales;2. Describir las acciones concretas para la gestión de los riesgos identificados; 3. Actuar de forma preventiva en el cumplimiento de las obligaciones establecidas en la Ley, su Reglamento y demás normativa aplicable; y, 4. Propiciar lineamientos para la construcción de una cultura preventiva de la protección de datos personales de la organización"*;

Que el artículo 31 del RGLOPDP señala que *"(...) [l]as evaluaciones de impacto del tratamiento de datos serán obligatorias en los casos establecidos en la Ley y deberán realizarse de forma previa al inicio del tratamiento de datos personales (...)"*;

Que el artículo 32 del RGLOPDP prevé que *"(...) [e]n los casos en que sea obligatoria, la evaluación de impacto será presentada ante la Autoridad de Protección de Datos Personales y contendrá, al menos, lo siguiente: 1. La descripción sistemática de las operaciones de tratamiento y las finalidades de ese tratamiento; 2. La justificación de la necesidad de llevar a cabo esas*

operaciones de tratamiento, así como su proporcionalidad con respecto de la finalidad; 3. La evaluación de riesgos a los derechos y libertades de los titulares; y, 4. Las medidas previstas para hacer frente a los riesgos, las garantías, medidas de seguridad y mecanismos destinados a salvaguardar y demostrar el respeto al derecho de los titulares a la protección de sus datos personales. La información otorgada en virtud de los numerales precedentes debe limitarse a la que sea necesaria para respaldar la evaluación y no incluir detalles potencialmente confidenciales relacionados con las implementaciones de seguridad o la información confidencial";

Que el numeral 5 del artículo 76 de la LOPDP dispone que *"(...) [l]a Autoridad 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 presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades: (...) 5) Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales (...)"*;

Que el numeral 16 del artículo 76 de la LOPDP le confiere a la SPDP funciones, atribuciones y facultades para *"(...) [p]romover e incentivar el ejercicio del derecho a la protección de datos personales, así como la concientización en las personas y la comprensión de los riesgos, normas, garantías y derechos, en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria tales como niñas niños y adolescentes (...)"*;

Que el numeral 7 del artículo 80 del RGLOPDP prescribe que *"(...) [l]a Autoridad de Protección de Datos Personales, además de las* [atribuciones] *señaladas en la Ley de la materia, tendrá las siguientes: (...) 7. Emitir guías de referencias que ayuden a los responsables y encargados del tratamiento de datos en el proceso de adecuación y cumplimiento de la normativa de protección de datos personales (...)"*;

Que mediante resolución Nº SPDP-SPDP-2024-0001-R, publicada en el Tercer Suplemento del Registro Oficial Nº 624 de agosto 19 de 2024, se aprobó el Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la SPDP ("Estatuto SPDP");

Que el artículo 1 del Estatuto SPDP, en su Anexo 1, declara que *"[l]a Superintendencia de Protección de Datos Personales 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 el literal b, numeral 2 del artículo 10 del Estatuto SPDP faculta a la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales ("IIT") a *"(...) [p]roponer y supervisar la implementación de política, lineamientos y mejores prácticas en materia de seguridad de la información y protección de datos personales, en concordancia con los estándares nacionales e internacionales (...)"*;

Que mediante Memorando N° SPDP-IGITS-2024-0013-M de diciembre 18 de 2024, la IIT puso en conocimiento de la Intendencia General de Regulación de Protección de Datos Personales ("IRD"), que la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales* no podría expedida en diciembre del 2024 a pesar de lo dispuesto mediante resolución Nº SPDP-SPDP-2024-0020-R, en razón a los siguientes motivos: *"(...) 1. Si bien el texto ha sido concluido en alrededor de 40 fojas, estamos creando gráficos e ilustraciones en coordinación con relaciones públicas, con la finalidad de que el texto sea más fácil de comprender para responsables y encargados del tratamiento de datos personales. 2. La guía agregará dos tutoriales aplicados de evaluaciones de impacto del tratamiento en el Anexo. 3. Dada la importancia de la guía, mi recomendación es culminar estos últimos hitos y hacer una revisión. Cabe considerar que todas las guías que en adelante desarrollemos acerca de controles de riesgos de protección de datos aplicados, tendrán a esta guía como dependencia"*;

Que el literal b) del numeral 2 del artículo 10 de la antedicha resolución Nº SPDP-SPDP-2024-0001-R, establece las atribuciones y responsabilidades de la Intendencia General de Regulación de Protección de Datos Personales ("IRD"), entre las que consta 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 Superintendencia de Protección de Datos Personales, 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 dicha ley y su reglamento (...)"*;

Que mediante resolución Nº SPDP-SPD-2025-0001-R del 31 de enero del 2025, publicada en Registro Oficial N° 750 del 24 de febrero del 2025, se establecieron las disposiciones, delegaciones de facultades y atribuciones a las autoridades, funcionarios y servidores públicos de la SPDP, en cuyo literal a), artículo 4, se le ha delegado a la IRD, entre otras, la responsabilidad de *"[e]mitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales"*;

Que mediante resolución Nº SPDP-SPDP-2024-0018-R, publicada en el Segundo Suplemento del Registro Oficial Nº 679 del 8 de noviembre del 2024, se expidió el Reglamento para la Elaboración y Aprobación del Plan Regulatorio Institucional de la Superintendencia de Protección de Datos Personales, en cuya disposición transitoria se ha previsto que *"(...) el PRI correspondiente a los años fiscales 2024 y 2025 no seguirá el procedimiento establecido en este reglamento y, por ende, se elaborará únicamente a base de los informes técnicos emitidos por las Unidades Administrativas correspondientes; validados por la IGRPDP; aprobados por el Superintendente o su delegado; y, finalmente, publicado en los portales oficiales de la SPDP cuando estén habilitados"*;

Que la IRD, mediante informe técnico Nº INF-SPDP-IRD-2025-0003 suscrito el 3 de enero del 2025, solicitó al Superintendente de Protección de Datos Personales la aprobación del Plan Regulatorio Institucional ("PRI") del año fiscal 2025, a fin de cumplir con la disposición transitoria de la resolución Nº SPDP-SPDP-2024-0018-R, así como para garantizar la transparencia y eficacia de la SPDP;

Que mediante resolución N° SPDP-SPD-2025-0002-R del 3 de febrero del 2025 se aprobó el PRI del año 2025, dentro del cual se estableció la necesidad de emitir la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales*;

Que la IIT, a través del informe técnico N° SPDP-IGITS-2025-001-I suscrito en el 21 de febrero del 2025, evidenció la necesidad de emitir la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales,* para garantizar los derechos y libertades fundamentales de los titulares y establecer tanto lineamientos obligatorios como optativos para el cumplimiento de los responsables y encargados del tratamiento;

Que mediante memorando N° SPDP-IIT-2025-0017-M suscrito en el 21 de febrero del 2025, la IIT puso en conocimiento de la IRD tanto el proyecto normativo denominado *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales,* como el informe técnico N° SPDP-IGITS-2025-001-I, elaborados por el Intendente General de Innovación Tecnológica y Seguridad de Datos Personales, señor doctor don Luis Enríquez Álvarez;

Que la IRD, en atención al informe técnico N° SPDP-IGITS-2025-001-I, emitió el informe técnico Nº INF-SPDP-IRD-2025-0009, que contiene el análisis de la procedencia del proyecto presentado por la IIT; y, en atención a ello, recomendó continuar con el procedimiento establecido en la resolución Nº SPDP-SPDP-2024-0018-R, publicada en el Segundo Suplemento Registro Oficial Nº 679 del 8 de noviembre del 2024, que contiene el Reglamento para la Elaboración y Aprobación del Plan Regulatorio Institucional de la Superintendencia de Protección de Datos Personales, respecto del proyecto normativo denominado *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales,* de acuerdo con lo establecido en los artículos 40 y 42 de la LODPD, los artículos 29, 30 y 31 del RGLOPDP, así como con el literal b), numeral 2, del

artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R, con el objetivo de garantizar el adecuado tratamiento de los datos personales de los titulares en el análisis de riesgos y la evaluación de impacto;

Que mediante memorando N° SPDP-IRD-2025-0023-M suscrito el 27 de febrero del 2025, la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") tanto la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales,* como el informe técnico N° INF-SPDP-IRD-2025-0009, para que en el término de diez (10) días realice las diligencias pertinentes de conformidad con lo dispuesto en la resolución N° SPDP-SPDP-2024-0022-R;

Que a través del informe técnico N° INF-SPDP-DAJ-2025-0006 suscrito el 27 de febrero del 2025, la DAJ determinó que la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales* es congruente con los principios establecidos en la LOPDP, no transgrede o contradice normas matrices, cumple con el principio de legalidad y, por ello, recomendó que *"(...) [l]a IRD debe disponer a quien corresponda la publicación a través de la página web institucional e informar su publicación a través de las redes sociales institucionales, con la finalidad de que la ciudadanía, las organizaciones de la sociedad civil o interesados en general, de manera motivada, puedan remitir sus observaciones o realizar aportes respecto del contenido (...)"*;

Que mediante memorando N° SPDP-DAJ-2025-0020-M suscrito el 27 de febrero del 2025, la DAJ puso en conocimiento de la IRD el informe técnico N° INF-SPDP-DAJ-2025-0006, así como la validación legal del proyecto de resolución que viabilizaría la expedición de la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales*;

Que en el memorando N° SPDP-IRD-2025-0024-M suscrito el 27 de febrero del 2025, la IRD solicitó a las unidades administrativas de la SPDP que procedan con las acciones pertinentes a fin de que publiquen la *Guía de Gestión de Riesgos y Evaluación de Impacto de Tratamiento de Datos Personales* en la página web institucional y en las redes sociales de la SPDP, para que el proyecto de normativa esté disponible para la ciudadanía, las organizaciones de la sociedad civil o interesados en general desde el 3 de marzo del 2025 hasta el 1 de abril del 2025, con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que a través del informe técnico Nº INF-SPDP-IRD-2025-0018, suscrito el 28 de abril del 2025, la IRD incorporó al informe técnico las observaciones y aportes que se consideraron relevantes y adecuados, previa justificación de las modificaciones realizadas al proyecto normativo;

Que mediante memorando Nº SPDP-IRD-2025-0065-M, suscrito el 28 de abril del 2025, la IRD remitió todo el expediente al suscrito Superintendente de Protección de Datos Personales para que realice las observaciones correspondientes o, en su caso, para que lo apruebe;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias,

RESUELVE:

EXPEDIR LA GUÍA DE GESTIÓN DE RIESGOS Y EVALUACIÓN DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

Art. 1.- Aprobar la *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales,* cuya autoría corresponde al señor doctor don Luis Enríquez Álvarez, Intendente General de Innovación Tecnológica y Seguridad de Datos Personales, en concordancia con lo establecido en los artículos 40 y 42 de la LODPD, los artículos 29, 30, 31 y 32 del RGLOPDP, así como con el literal b), numeral 2, del artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R; ello con el objetivo de precautelar el adecuado tratamiento de los datos personales de los titulares respecto al análisis de riesgos y la evaluación de impacto.

Art. 2.- El capítulo I de la *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales* será de obligatorio cumplimiento para los responsables y encargados del tratamiento de datos personales; el capítulo II tendrá un carácter meramente referencial, por lo que será de carácter optativo u orientativo, y, por ende, la metodología de riesgos en protección de datos personales podrá ser seleccionada al libre arbitrio del responsable y encargado del tratamiento de

datos personales. No obstante, se deja expresamente establecido que el análisis de riesgos y la evaluación de impacto son de obligatorio cumplimiento de conformidad con la LOPDP, el RGLOPDP y demás normativa en la materia.

DISPOSICIÓN GENERAL

En el plazo de un (1) año contado a partir de la publicación de esta resolución en el Registro Oficial, la IIT ejecutará la revisión y evaluación del contenido de la *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales,* con el objeto de garantizar la mejora continua del documento en mención; y, dentro de idéntico lapso, preparará el informe técnico pertinente que deberá poner en conocimiento del Superintendente de Protección de Datos Personales.

DISPOSICIONES TRANSITORIAS

Primera.- De conformidad con la resolución Nº SPDP-SPDP-2024-0020-R y la resolución Nº SPDP-SPDP-2024-0022-R, la SPDP emitirá la normativa técnica en materia de riesgos y evaluación de impacto en protección de datos personales que considere necesaria para precautelar los derechos y libertades fundamentales de los titulares.

Segunda.- La *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales,* de conformidad con las funciones, atribuciones y competencias de la SPDP establecidas en la LOPDP, el RGLOPDP y demás normativa aplicable, podrá reformarse de conformidad con la resolución Nº SPDP-SPDP-2024-0022-R.

DISPOSICIÓN FINAL

Esta resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dada y firmada en Quito, D. M., el 29 de abril del 2025.

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES