RESOLUCIÓN Nº SPDP-SPD-2026-00[*]-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el numeral 19 del artículo 66 de la Constitución de la República del Ecuador ("CRE") les 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 92 de la CRE consagra el derecho de toda persona a conocer de la existencia de sus datos personales en archivos públicos o privados, así como a solicitar su acceso gratuito, actualización, rectificación, eliminación o anulación, especialmente tratándose de datos sensibles, con la adopción de las medidas de seguridad necesarias;

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 idem, 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 76 idem, el Superintendente de Protección de Datos Personales;

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

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

Que el numeral 4 del artículo 80 del Reglamento General de la LOPDP ("RGLOPDP") le otorga a la SPDP, entre otras atribuciones, la de *"[e]mitir regulaciones para la protección de datos personales"*;

Que el numeral 5 del artículo 83 del RGLOPDP determina que al Superintendente de Protección de Datos Personales le compete *"[a]probar y expedir normas internas resoluciones y manuales que sean necesarios para el buen funcionamiento de la* [Superintendencia] *a su cargo"*;

Que mediante resolución N° SPDP-SPDP-2024-0001-R del 2 de agosto del 2024, publicada en el Tercer Suplemento del Registro Oficial N° 624 del 19 de agosto del 2024, el Superintendente de Protección de Datos Personales aprobó el Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la Superintendencia de Protección de Datos Personales; que fue reformada mediante Resolución No. SPDP-SPDP-2024-0014-R,

publicada el 18 de noviembre de 2024 en el Registro Oficial Año III No. 685, y mediante Resolución N° SPDP-IRD-2025-0028-R, expedida el 30 de julio del 2025, publicada en el Registro Oficial Año I N° 105 del 19 de agosto del 2025;

Que el artículo 1 de la misma resolución Nº SPDP-SPDP-2024-0001-R, en su Anexo 1, ha previsto 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 la letra b), numeral 2 del artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R, establece que a la Intendencia General de Regulación de Protección de Datos Personales ("IRD") le corresponde, entre otras atribuciones y responsabilidades, *"[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 la letra c), numeral 2 del artículo 10 de esa misma resolución N° SPDP-SPDP-2024-0001-R, establece, entre las atribuciones y responsabilidades de la IRD, la 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 letra a) del artículo 4 de la resolución N° SPDP-SPD-2025-0001-R del 31 de enero del 2025, publicada en el Registro Oficial N° 750 del 24 de febrero del 2025, mediante la cual se expidieron las disposiciones, delegaciones de facultades y atribuciones a las autoridades, funcionarios y servidores públicos de la SPDP, se le delegó al Intendente General Regulación de Protección de Datos Personales, 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 a través de la resolución Nº SPDP-SPDP-2024-0022-R del 31 de diciembre del 2024, publicada en el Registro Oficial Nº 734 del 31 de enero del 2025, se expidió el Reglamento para la Creación, Modificación y Derogatoria de la Normativa de la SPDP;

Que el numeral 7 del artículo 47 de la LOPDP indica las *"Obligaciones del responsable y encargado del tratamiento de datos personales.- El responsable del tratamiento de datos personales está obligado a: (...) 7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas; (...)"*

Que el numeral 14 del artículo 76 de la LOPDP dispone como una de las funciones y atribuciones de la SPDP el *"(...) 14) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas; (...)"*

Que el artículo 135 del Código Orgánico Administrativo ("COA") señala que le *"corresponde a la Administración Pública, la dirección del procedimiento administrativo en ejercicio de las competencias que se le atribuyan en el ordenamiento jurídico y en este Código"*;

Que mediante la resolución N° SPDP-SPD-2025-0050-R del 30 de diciembre del 2025 se aprobó el Plan Regulatorio Institucional del año 2026, dentro del cual se ha establecido la necesidad de expedir ***la Normativa Técnica Sobre Notificación de Vulneraciones de Seguridad de Datos Personales,*** aprobado, en su día, mediante la resolución Nº SPDP-SPD-2025-0005-R del 30 de abril del 2025, que se publicó en el Registro Oficial Nº 42 del 20 de mayo del 2025;

Que mediante el memorando **Nº SPDP-IRD-2025-0008-M** suscrito el **3** de **febrero** del **2025,** la IRD solicitó a todas las unidades e intendencias de la SPDP que, hasta el 30 de abril del 2025, establezcan la necesidad de emisión de normativa secundaria para que se la incluya en el Plan Regulatorio Institucional ("PRI") 2026;

Que mediante memorando N° SPDP-IIT-2026-0048-M suscrito el 21 de abril de 2026 la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales ("IIT") puso en conocimiento de la IRD el informe técnico Nº SPDP-IGITS-2026-002-IV junto con el Proyecto Normativo borrador que contiene la Norma Técnica de Notificaciones de Vulneraciones de la Seguridad de Datos.

Que mediante el memorando **N° SPDP-IRD-2026-0078-M** suscrito el 28 de abril del **2026,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") el proyecto normativo denominado ***la Normativa Técnica Sobre Notificación de Vulneraciones de Seguridad de Datos Personales*****,** así como el informe técnico **N° INF-SPDP-IRD-2026-0029,** para que en el 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 la DAJ, mediante el informe técnico **N° INF-SPDP-DAJ-2026-0018** suscrito el 29 de abril del **2026,** determinó *"(...) se concluye que el proyecto de resolución para la emisión de la NORMA TÉCNICA DE NOTIFICACIONES DE VULNERACIONES DE LA SEGURIDAD DE DATOS establece un marco técnico y procedimental claro para la notificación y gestión de vulneraciones de seguridad de datos personales; por lo que en base a los artículos 10 número 10.5, 11 de la Resolución Nro. SPDP-SPDP-2024-0022-R que contiene el Reglamento para la Creación, Codificación y Derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales, el suscrito VALIDA dicho proyecto por cumplir con el principio de legalidad, por no vulnerar ni contradecir las normas matrices, y por coadyuvar al cumplimiento de los objetivos de la Superintendencia de Protección de Datos Personales."*;

Que mediante el memorando **N° SPDP-IRD-2026-0079-M** suscrito el **29 de abril** 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 normativo denominado ***Normativa Técnica Sobre Notificación de Vulneraciones de Seguridad de Datos Personales*** en la página web institucional y en las redes sociales de la SPDP, para que se encuentre disponible para la ciudadanía, las organizaciones de la sociedad civil o interesados desde el **04 de mayo del 2026 hasta el 01 de junio 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 de ***la Normativa Técnica Sobre Notificación de Vulneraciones de***

Seguridad de Datos Personales dentro del término de veinte (20) días, de conformidad con el artículo 12 de la mencionada resolución;

Que, como resultado del proceso descrito previamente, se redefinió la denominación del proyecto como **XXX;**

Que a través del informe técnico **N° INF-SPDP-IRD-2026-00xx** suscrito el **xx** de **xx** del **2026,** la IRD incorporó las observaciones y aportes que se consideraron relevantes y adecuados, todo ello con la justificación de las modificaciones realizadas al proyecto normativo;

Que mediante el memorando **N° SPDP-IRD-2026-00xx-M** suscrito el **x** de xxx 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-2026-00xx-M** del **xx** de **xxx** 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-[*]-M** del **[*]** de **abril** del **2026,** la IRD puso en conocimiento del Superintendente de Protección de Datos Personales el proyecto que contiene la ***Normativa Técnica Sobre Notificación de Vulneraciones de Seguridad de Datos Personales*****,** debidamente subsanado, de conformidad con el artículo 14 del aludido Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias;

RESUELVE:

EMITIR LA NORMA TÉCNICA DE NOTIFICACIONES DE VULNERACIONES DE LA SEGURIDAD DE DATOS

TÍTULO I
OBJETO, DEFINICIONES, ÁMBITO, LINEAMIENTOS

Art 1.- Esta norma técnica tiene por objeto regular el proceso de presentación, así como la gestión de las notificaciones de vulneraciones de seguridad de datos personales para responsables y encargados del tratamiento de datos personales.

Art 2.- El ámbito de aplicación de la presente norma técnica es de conformidad con el artículo 3 de la LOPDP.

Art. 3.- Definiciones: para efectos de la presente norma técnica se deberán considerar las siguientes definiciones:

3.1. Incidente: una situación que afecta la seguridad de un sistema o un proceso de manera general.

3.2 Vulneración: Sin perjuicio de la definición establecida en la LOPDP, se debe entender que toda vulneración es un incidente que afecta los datos personales de los titulares, y constituye una brecha de seguridad.

Art 4.- Las vulneraciones de la seguridad de datos personales son de tres tipos: vulneraciones de confidencialidad, vulneraciones de integridad, y vulneraciones de disponibilidad.

Art 5.- Las vulneraciones tienen las siguientes temporalidades:

5.1. Vulneraciones de integridad y de disponibilidad: pueden ser temporales, siempre y cuando se haya tomado las medidas técnicas y organizacionales tales como: planes de continuidad de actividades de negocios, planes de recuperación de desastres, backups de los datos personales, redundancia en el software, servidores alternos, entre otras.

5.2. Las vulneraciones de confidencialidad: pueden ser irreversibles, sobre todo cuando se trata de datos biométricos, los datos de la salud, y otros datos sensibles o especiales de menores establecidos en la LOPDP.

Art 7.- El objetivo de la notificación a la SPDP es informar a la autoridad acerca de incidentes de seguridad en los que puede existir la probabilidad de vulneraciones a los derechos y libertades de los titulares de datos personales. La Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales gestionará el tratamiento de las notificaciones recibidas de manera confidencial, con fines investigativos, analíticos y estadísticos.

Art 8.- El objetivo de la notificación a los titulares es informarles acerca de una vulneración de seguridad, a fin de respetar sus derechos y libertades.

Art 9.- El responsable del tratamiento debe realizar las notificaciones de vulneración de seguridad de datos personales por medios digitales, a través del Sistema Nacional de Protección de Datos Personales (SISPDP). La ausencia de notificación será considerada como infracción grave en concordancia con el artículo 68 de la LOPDP.

Art 10.- Los lineamientos básicos para las notificaciones a la SPDP de vulneración a la seguridad de datos personales tendrán los siguientes principios:

10.1. Celeridad. Para el tratamiento se utilizará un sistema auxiliar experto confidencial y soberano de inteligencia artificial agéntica (AIxSPDP), con el fin de incrementar la celeridad del proceso, mejorando la escalabilidad del tratamiento de notificaciones, generar métricas y aplicar modelos de riesgo que garanticen la explicabilidad, y que ayuden a estimar de manera objetiva el nivel de riesgo de cada incidente.

10.2. Trazabilidad. El sistema AIxSPDP procesará la información recibida, asignando un número de trámite y permitiendo la trazabilidad integral de todos los trámites y métricas generadas.

10.3. Objetividad. El análisis de datos, métricas y modelos de riesgo que provee el sistema AIxSPDP, es esencial para lograr una mayor objetividad en la toma de decisiones realizada por los funcionarios de la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales.

10.4. Obligatoriedad. La ausencia o falta de notificación a los titulares es una infracción grave, en concordancia con el artículo 68 de la LOPDP.

10.5. Confidencialidad. Las notificaciones serán tratadas de manera general bajo el principio de confidencialidad, con controles estrictos de acceso.

10.6. Interoperabilidad. Las vulneraciones de la seguridad podrán ser tratadas de manera coordinada con otras instituciones, tales como el Arcotel, y los Equipos de respuesta a incidentes de seguridad de la información (CSIRT, CERT). Cuando las vulneraciones de seguridad tengan un alcance internacional, se las podrá tratar en cooperación con autoridades de protección de datos personales de otros países.

Art 11.- Los lineamientos básicos para las notificaciones a titulares son los siguientes:

11.1. Claridad. La notificación a los titulares se realizará con un lenguaje claro, transparente y sencillo.

11.2. Publicidad. Los responsables del tratamiento realizarán la notificación a través de al menos dos medios de comunicación de difusión masiva.

11.3. Obligatoriedad. La ausencia o falta de notificación a los titulares es una infracción grave en concordancia con el artículo 68 de la LOPDP.

Art 12.- La notificación de los encargados deberá realizarse de acuerdo con lo establecido en el artículo 43 de la LOPDP, por ello, la comunicación deberá ser por escrito y enviada por correo electrónico, a menos que el responsable y el encargado del tratamiento hubieran designado otro medio electrónico para tal efecto en el contrato de encargo respectivo.

El responsable del tratamiento una vez recibida la comunicación sobre la vulneración deberá notificar a la SPDP en el término de cinco (5) días de acuerdo con el artículo 43 de la LOPDP.

TÍTULO II
PROCESO DE NOTIFICACIÓN DE VULNERACIONES A LA SPDP

Art 13.- Las notificaciones de una vulneración de seguridad de datos, se deberán realizar a través de un formulario en línea, hospedado en el SISPDP (https://servicios.spdp.gob.ec), estas se deberán realizar el responsable del tratamiento de datos personales.

Art. 14.- Una vez que el formulario sea enviado, se generará un comprobante el cual contendrá la constancia de haber realizado la notificación, éste será emitido de manera automática por el SISPDP, el cual llegará al correo electrónico del que realiza la notificación. El formulario se grabará de manera automática en las bases de datos de la SPDP que hayan sido asignadas.

Art. 15.- Una vez que el formulario conste en las bases de datos de la SPDP, será ingresado al sistema experto auxiliar (AIxSPDP). Este sistema analizará la información recibida con el fin de descartar aquellos formularios que no correspondan a notificaciones de vulneraciones de seguridad de datos personales, así como validará aquellas notificaciones que sí cumplan con los requisitos establecidos en el Reglamento a la LOPDP.

Art. 16.- Una vez filtrados los formularios, se mantendrán solo los que son notificaciones de vulneraciones de seguridad y el sistema AIxSPDP descompondrá los elementos sustanciales del incidente de seguridad, para reducir la incertidumbre en la estimación, los probables niveles de riesgo para los derechos y libertades de los titulares de los datos. Una vez realizado el análisis de datos, éste pasará por revisión y supervisión humana, la cual estará a cargo de la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales donde se analizarán las métricas recibidas y determinarán si el caso amerita pasar a la Intendencia General de Control y Sanción, recomendando el inicio de un proceso de control, a través de un informe debidamente justificado y con firma de responsabilidad.

Art. 17.- Las notificaciones de vulneración de la seguridad de datos personales que no hayan sido enviadas a la Intendencia General de Control y Sanción quedarán archivadas en estado de monitoreo, el cual estará a cargo y se realizará bajo la supervisión de la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales .

El monitoreo se realizará con la finalidad de determinar si el riesgo de vulnerar los derechos y libertades de los titulares de datos puede aumentar en el tiempo, especialmente en las vulneraciones de confidencialidad, cuyo impacto en los derechos y libertades de titulares de datos podría materializarse en el futuro.

DISPOSICIONES GENERALES

Única.- Esta norma técnica podrá ser revisada y actualizada en cualquier momento por la SPDP, en función de los avances tecnológicos, sin limitación alguna.

DISPOSICIÓN TRANSITORIA

Única.- La Unidad de Planificación y Gestión Estratégica contará con un plazo de seis meses (6) meses, contados a partir de la entrada en vigencia de la presente norma técnica, para revisar los manuales de procesos, los cuales deberán ser elaborados por la IIT.

DISPOSICIÓN FINAL

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

Dada y firmada en Quito, D. M., el [*] de abril del 2026.

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES