RESOLUCIÓN Nº SPDP-SPD-2026-0040-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el número 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 77 idem, el Superintendente de Protección de Datos Personales;

Que el inciso primero del 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 número 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 número 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 número 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 el número 7 del artículo 47 de la LOPDP obliga al responsable del tratamiento a *"[t]omar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas"*;

Que el número 14 del artículo 76 de la LOPDP le atribuye a la SPDP la facultad de *"[l]levar 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") determina 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 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 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 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 por medio de la resolución N° SPDP-SPD-2025-0050-R del 30 de diciembre del 2025 se aprobó el PRI 2026, dentro del cual se ha establecido la necesidad de **expedir la Normativa Técnica sobre Notificación de Vulneraciones de Seguridad de Datos Personales;**

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 PRI 2026;

Que por medio del memorando **N° SPDP-IIT-2026-0048-M** suscrito el **21** de **abril** del **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 borrador que contiene la **Norma Técnica de Notificaciones de Vulneraciones de la Seguridad de Datos.**

Que a través del memorando **N° SPDP-IRD-2026-78-M** suscrito el **28** de **abril** del **2026,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") el proyecto normativo denominado **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-2026-00018** suscrito el **29** de **abril** del **2026,** determinó *"(...)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 por medio del 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 **4** de **mayo** del **2026** hasta el **1** 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 la IIT, en el ámbito de sus competencias, efectuó el análisis y la revisión técnica de las observaciones, comentarios y aportes formulados al proyecto de **Norma Técnica de Notificaciones de Vulneraciones de la Seguridad de Datos Personales,** con el objeto de especificar cuáles eran los que resultaban pertinentes para su incorporación al texto normativo y cuáles los que correspondía desestimar, además de efectuar las modificaciones respectivas en el proyecto, con la correspondiente justificación técnica de los cambios realizados;

Que una vez concluido dicho proceso de análisis y revisión, la IRD recopiló y procesó los resultados remitidos por la IIT, incluidas las observaciones y aportes aceptados, los que fueron rechazados y las respectivas justificaciones, a efectos de consolidar el proceso de participación;

Que a través del informe técnico **N° INF-SPDP-IRD-2026-0054** suscrito el **21** de **agosto** del **2026,** la IRD incorporó las observaciones y aportes que la IIT consideró como relevantes y adecuados, todo ello con la justificación de las modificaciones realizadas al proyecto normativo;

Que mediante memorando **N° SPDP-IRD-2026-0148-M** suscrito el **21** de **agosto** del **2026,** notificado al despacho el **21** 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-2026-167-M** del **8** de **septiembre** del **2026,** la IRD puso en conocimiento del Superintendente de Protección de Datos Personales el proyecto que contiene la **Norma Técnica de Notificaciones de Vulneraciones de la Seguridad de los Datos,** debidamente subsanado, de conformidad con el artículo 14 del aludido Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

EN EJERCICIO de sus atribuciones constitucionales, legales y reglamentarias;

RESUELVE:

EXPEDIR LA NORMA TÉCNICA DE NOTIFICACIONES DE VULNERACIONES DE LA SEGURIDAD DE LOS DATOS PERSONALES

TÍTULO I
OBJETO, DEFINICIONES, ÁMBITO, LINEAMIENTOS

Art. 1.- Esta norma técnica tiene por objeto regular el proceso de notificación de vulneraciones de seguridad de datos personales por parte de los responsables y encargados del tratamiento, así como el proceso de gestión de notificaciones de vulneraciones de seguridad de datos personales que fueren recibidas por parte la SPDP.

Art. 2.- El ámbito de aplicación de la presente norma técnica es el determinado por la LOPDP.

Art. 3.- En esta norma técnica se deberán considerar las siguientes definiciones:

3.1. Incidente de protección de datos personales: Es un evento de seguridad que ha vulnerado o tiene la probabilidad de vulnerar la confidencialidad, integridad o disponibilidad de datos personales.

3.2. AIxSPDP: Es el sistema experto auxiliar de gestión, confidencial y soberano, utilizado para establecer la trazabilidad de cada notificación recibida, la ontologías, la generación de métricas de análisis y de modelos adecuados de riesgo basados en inteligencia artificial agéntica con intervención humana en todas sus instancias. Tal como el sistema experto informativo y analítico, no constituye un sistema de toma automatizada de decisiones. La finalidad del AIxSPDP es reducir la incertidumbre en la toma de decisiones informadas por parte de los funcionarios de la SPDP, con respecto a la probabilidad de ocurrencia y al impacto que podría generar una vulneración de la seguridad de datos personales en los derechos y libertades de los titulares.

3.3. SISPDP: Es el Sistema Nacional de Registro de Datos Personales, por medio del cual se receptan las notificaciones de vulneraciones de seguridad y, además, se ofrecen servicios a los responsables del tratamiento, encargados del tratamiento, delegados de protección de datos personales y a los titulares. Está hospedado en la dirección https://servicios.spdp.gob.ec.

3.4. IIT: Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales.

3.5. ICS: Intendencia General de Control y Sanción.

Art. 4.- Las vulneraciones de la seguridad de datos personales son de tres tipos: vulneraciones de confidencialidad; vulneraciones de integridad; y, vulneraciones de disponibilidad. Un mismo incidente de protección de datos personales puede ocasionar vulneraciones de más de un tipo.

Art. 5.- Las vulneraciones tienen las siguientes dimensiones:

5.1. Vulneraciones de integridad: Serán *temporales* cuando, mediante la aplicación de medidas técnicas y organizativas adecuadas, fuese posible verificar, recuperar y restaurar la integridad de los sistemas de información que realizan tratamiento de datos personales, así como la de sus respaldos y la de los propios datos personales. Serán *permanentes* cuando no fuere posible recuperar la integridad de los datos personales; e *irreversibles* cuando no existiere posibilidad técnica de restablecerlos a su estado íntegro.

5.2. Vulneraciones de disponibilidad: Serán *temporales* cuando, mediante la aplicación de medidas técnicas y organizativas adecuadas orientadas a garantizar la continuidad, recuperación, respaldo y redundancia de los sistemas de información y de los datos personales, fuese posible restablecer su disponibilidad. Serán *permanentes* cuando no fuere posible recuperar los datos personales y, por tanto, restablecer su disponibilidad para el titular; e *irreversibles* cuando no existiere posibilidad técnica de recuperar los datos personales involucrados.

5.3. Vulneraciones de confidencialidad: Son esencialmente *permanentes,* pues una vez que los datos personales han sido accedidos sin la autorización del titular, se los puede utilizar, distribuir o publicar en cualquier momento y con fines ilegítimos. Así también, se considerarán *irreversibles* cuando los datos personales no pudiesen ser cambiados por parte del titular, especialmente cuando se tratare de datos sensibles o de categorías especiales de datos personales, de acuerdo con las definiciones de la LOPDP.

Art. 6.- La notificación tiene por objetivo informarle a la SPDP acerca de la existencia de incidentes de seguridad en los que hubiese riesgo para los derechos y libertades de los titulares. La IIT gestionará el tratamiento de las notificaciones recibidas de manera confidencial, con fines preventivos, investigativos, analíticos y estadísticos.

Art. 7.- La notificación a los titulares tiene por finalidad informarles, de manera clara, oportuna y comprensible, sobre la existencia de una vulneración de seguridad de datos personales que pudiese afectar sus derechos y libertades, a fin de que los responsables puedan adoptar las medidas de prevención, protección o mitigación de riesgos.

Art. 8.- A través del SISPDP y por medios digitales, el responsable del tratamiento deberá notificarle a la SPDP la vulneración de seguridad de datos personales. La ausencia de notificación será considerada como infracción grave, de acuerdo con la LOPDP. De manera excepcional, esto es, únicamente si el sistema AIxSPDP no estuviere disponible o en funcionamiento, la notificación se podrá realizar mediante otros canales o medios oficiales. La SPDP constatará si se verificó tal hecho excepcional para poder convalidar la notificación así realizada.

Art. 9.- Las notificaciones a la SPDP se regirán por los siguientes criterios:

9.1. Celeridad: Para la gestión de las notificaciones de vulneraciones de seguridad de datos personales se utilizará el sistema AIxSPDP con intervención humana en todas sus instancias, con el fin de incrementar la atención pronta del proceso; mejorar la escalabilidad del tratamiento de notificaciones; generar métricas significativas; aplicar modelos de riesgo que garanticen la explicabilidad y que ayuden a los funcionarios de la SPDP a estimar, de manera objetiva, el nivel de riesgo de cada incidente, con la finalidad de reducir la incertidumbre para la toma informada de decisiones por parte de los funcionarios de la SPDP.

9.2. Trazabilidad: El sistema AIxSPDP procesará la información recibida, asignará un número de trámite y permitirá la rastreabilidad integral de todos los trámites y métricas generadas.

9.3. Objetividad: La valoración técnica de las notificaciones se realizará a base de criterios neutrales, a través de la utilización del análisis de datos, las métricas y los

modelos de riesgo que provee el sistema AIxSPDP. Este proceso analítico permite la toma de decisiones informadas por parte de los funcionarios de la SPDP.

9.4. Obligatoriedad: La ausencia o falta de notificación a los titulares es una infracción grave, de acuerdo con la LOPDP.

9.5. Confidencialidad: Las notificaciones serán tratadas de manera general bajo el principio de confidencialidad, con controles estrictos de acceso y la implementación de medidas de seguridad proporcionales a cada escenario de riesgo.

9.6. Interoperabilidad: Las vulneraciones de seguridad de datos personales podrán ser tratadas de manera coordinada con otras instituciones, tal como la ARCOTEL y los equipos de respuesta a incidentes de seguridad de la información (CSIRT, CERT). La interoperabilidad con otras instituciones se realizará con observancia de los principios de necesidad, proporcionalidad y seguridad.

9.7. Cooperación internacional: Cuando las vulneraciones de seguridad de datos personales tuvieren un alcance internacional, se las podrá tratar en cooperación con autoridades de protección de datos personales de otros países. La interoperabilidad con otras instituciones y la cooperación internacional se realizarán mediante el cumplimiento de los principios de necesidad, proporcionalidad y seguridad.

Art. 10.- Los requisitos mínimos para las notificaciones a los titulares son los siguientes:

10.1. Claridad: La notificación a los titulares se realizará con un lenguaje claro, accesible, transparente y sencillo. Deberá contener, al menos, la naturaleza de la vulneración; la fecha de detección o el período estimado del evento, cuando fuere posible; las medidas adoptadas por el responsable del tratamiento; y las recomendaciones para los titulares.

10.2. Publicidad: Los responsables del tratamiento realizarán la notificación a los titulares a través de los canales habituales de comunicación que tuviesen establecidos para el efecto, así como a través de anuncios en sus páginas web, por correo electrónico o cualquier otro mecanismo de comunicación directa con el titular. El responsable del tratamiento deberá realizar una publicación en un medio de difusión masiva únicamente cuando no tuviese un canal oficial de comunicación preestablecido con los titulares. La notificación pública deberá cumplir con los principios de minimización y pertinencia.

Art. 11.- De acuerdo con la LOPDP, la obligación de notificación de los encargados a los responsables deberá realizarse en el plazo máximo de dos días. De igual manera, se deberá enviar la información especificada en el RGLOPDP. La comunicación deberá remitirse por correo electrónico, a menos que el responsable y el encargado del tratamiento hubieren 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 de seguridad de datos personales, deberá notificarle a la SPDP en el término de cinco (5) días, de acuerdo con la LOPDP.

TÍTULO II
PROCESO DE NOTIFICACIÓN DE VULNERACIONES A LA SPDP

Art. 12.- Los responsables del tratamiento deberán realizar las notificaciones de vulneraciones de seguridad de datos personales a través del link o enlace https://servicios.spdp.gob.ec).

Art. 13.- Una vez que el formulario se envíe, el SISPDP generará automáticamente una constancia de recepción de la notificación que, a su vez, será remitida a la dirección de correo

electrónico desde la cual se cursó la notificación de vulneración. El formulario se grabará de manera automática en las bases de datos del SISPDP que se hubiesen asignado.

Art. 14.- El sistema AIxSPDP recuperará la información de las bases de datos y analizará la información recibida, con el fin de alertar a los funcionarios de la SPDP sobre aquellos formularios que no correspondan a notificaciones de vulneraciones de seguridad de datos personales. De igual manera, validará aquellas notificaciones que sí cumplan con los requisitos establecidos en el RGLOPDP.

Art. 15.- Una vez filtrados los formularios, solamente se gestionarán los que propiamente tuviesen la calidad de notificaciones de vulneraciones de seguridad. El sistema AIxSPDP descompondrá los elementos sustanciales del incidente de protección de datos personales, para reducir la incertidumbre en la estimación de los probables niveles de riesgo para los derechos y libertades de los titulares.

Realizado el análisis de datos, se lo pasará al análisis, revisión y supervisión humanos a cargo de la IIT. Se analizarán las particularidades del caso y se determinará si es preciso remitirlo a la ICS, en cuyo caso se recomendará el inicio de un proceso de control a través de un informe debidamente justificado y con firma de responsabilidad.

Art. 16.- Las notificaciones de vulneración de la seguridad de datos personales que no hubiesen sido enviadas a la ICS quedarán almacenadas en estado de monitoreo, el cual estará a cargo y se realizará bajo la supervisión de la IIT.

El monitoreo se realizará con la finalidad de estimar si el riesgo de vulnerar los derechos y libertades de los titulares de datos pudiese aumentar con el decurso del 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

Primera.- Esta norma técnica podrá ser revisada y actualizada en cualquier momento por la SPDP en función de los avances tecnológicos, previo informe técnico de la IIT.

Segunda.- La SPDP publicará en su portal web los modelos de riesgo y ontologías de agentes de inteligencia artificial utilizados en el sistema AIxSPDP en el plazo de seis meses, contados a partir de la entrada en vigor de esta norma técnica.

Tercera.- La SPDP publicará las actualizaciones que los modelos de riesgo y ontologías tuviesen en función de las auditorías internas y de los procesos de mejora continua establecidos por el sistema de gestión de protección de datos personales (PIMS), y por el sistema de gestión de seguridad de la información (SGSI) de la SPDP.

DISPOSICIÓN TRANSITORIA

La Unidad de Planificación y Gestión Estratégica contará con un plazo de seis 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 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