RESOLUCIÓN Nº SPDP-SPD-2025-0004-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 4 de la LOPDP define al delegado de protección de datos como aquella *"(...) [p]ersona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos (...)"*;

Que el inciso final del artículo 48 de la LOPDP dispone que *"[l]a Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación"*;

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 en la segunda disposición transitoria del Reglamento General de la Ley Orgánica de Protección de Datos Personales ("RGLOPDP") ha previsto que *"[e]n el plazo máximo de un (1) año, contado a partir de la fecha de implementación y funcionamiento de la Superintendencia de Protección de Datos Personales, esta coordinará y llevará a cabo capacitaciones técnicas y cursos de formación dirigidos al público en general, orientados a promover el ejercicio del derecho a la protección de datos personales y a la profesionalización de los delegados de protección de datos personales. Para tal efecto, podrá celebrar alianzas con instituciones de educación superior con experiencia en la materia, así como con organizaciones especializadas que promuevan la 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) 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 el *Reglamento del Programa de Profesionalizante de Delegados de Protección de Datos Personales*;

Que la IRD, a través del informe técnico Nº INF-SPDP-IRD-2025-0008 suscrito el 27 de febrero del 2025, justificó la pertinencia y la necesidad de determinar los lineamientos y criterios para que las personas naturales que desempeñen el cargo de delegados de protección de datos personales tengan, en la materia, conocimientos prácticos, así como en derecho y en sistemas, a fin de ejercer adecuadamente las funciones determinadas en la LOPDP, el RGLOPDP y demás normativa aplicable; informe técnico en cuya parte pertinente se indica que *"[l]a SPDP en ejercicio de sus funciones y atribuciones está facultada de conformidad con el numeral 5 del artículo 76 de la LOPDP para emitir el Proyecto de Resolución que expide el Programa de Profesionalizante de Delegados de Protección de Datos Personales",* a la par que recomendó *"(...) [e]xpedir el Reglamento del Programa de Profesionalizante de Delegados de Protección de Datos Personales, en cumplimiento con la Resolución N° SPDP-SPD-2025-0002-R"*;

Que mediante memorando N° SPDP-IRD-2025-0020-M suscrito el 27 de febrero del 2025, la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ"), el proyecto normativo denominado *Reglamento del Programa de Profesionalizante de Delegados de Protección de Datos Personales* y el informe técnico N° INF-SPDP-IRD-2025-0008, 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, en la parte pertinente de su informe técnico N° INF-SPDP-DAJ-2025-0004 suscrito el 27 de febrero del 2025, determinó que el *Reglamento del Programa de Profesionalizante de Delegados de Protección 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 a través del memorando N° SPDP-DAJ-2025-0018-M suscrito el 27 de febrero del 2025, la DAJ puso en conocimiento de la IRD el informe técnico N° INF-SPDP-DAJ-2025-0004, así como la validación legal del proyecto de resolución que viabilizaría la expedición del *Reglamento del Programa de Profesionalizante de Delegados de Protección 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 el *Reglamento del Programa de Profesionalizante de Delegados de Protección 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 para cumplir con la resolución Nº SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización del *Reglamento del Programa de Profesionalizante de Delegados de Protección de Datos Personales* dentro del término de veinte (20) días, de conformidad con el artículo 12, y se procedió a dar de baja el proyecto normativo el 2 de abril del 2025 de la página web institucional y las redes sociales de la SPDP;

Que a través del informe técnico Nº INF-SPDP-IRD-2025-0019, 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-2025-0066-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:

Art. 1.- Aprobar el *Reglamento del Programa Profesionalizante de Delegados de Protección de Datos Personales,* a fin de garantizar que los profesionales que fueren o se encontraren ya designados por los responsables y encargados del tratamiento, ejecuten las funciones establecidas en la LOPDP de manera proactiva y adecuada en cautela a los principios, derechos y obligaciones establecidos en el ordenamiento jurídico vigente.

Art. 2.- Los delegados de protección de datos personales, para cumplir las funciones que les asigna la LOPDP, deberán contar con cualificaciones en derecho, sistemas y en tecnologías de la información y comunicación, en aras de garantizar la tutela del derecho a la protección de datos personales.

Art. 3.- Las instituciones de educación superior, de conformidad con la Ley Orgánica de Educación Superior y la normativa específica en la materia, son las entidades autorizadas para impartir programas académicos referentes al *Programa Profesionalizante de Delegados de Protección de Datos Personales.* Para ello, las instituciones de educación superior deberán implementar el Anexo I de de esta resolución. Esta disposición es aplicable tanto para programas académicos de tercer nivel o cuarto nivel, como para los sistemas de educación continua.

DISPOSICIÓN GENERAL

Las instituciones de educación superior notificarán a la SPDP los títulos académicos, diplomas o certificados que expidieren, para que sean registrados en la plataforma que se implemente para el efecto una vez que se cumplan los requisitos establecidos.

DISPOSICIONES TRANSITORIAS

Primera.- Las instituciones de educación superior que estuvieren impartiendo programas académicos de profesionalización en protección de datos personales a la fecha de expedición de este reglamento, podrán implementar el *Programa Profesionalizante de Delegados de Protección de Datos Personales* dentro del plazo de seis (6) meses, que empezará a discurrir desde su publicación en el Registro Oficial.

Segunda.- La Unidad de Tecnologías de la Información y Comunicación de la SPDP implementará la plataforma para el registro de títulos académicos, diplomas o certificados dentro del mismo plazo que consta indicado en la disposición precedente.

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.

Firmado electrónicamente por:
FABRIZIO ROBERTO
PERALTA DIAZ
Validar únicamente con FirmaEC

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

ANEXO I

PROGRAMA PROFESIONALIZANTE DE DELEGADOS DE PROTECCIÓN DE DATOS PERSONALES

BLOQUE 1: DERECHO DE PROTECCIÓN DE DATOS PERSONALES

1. Naturaleza jurídica
    a. Derecho de protección de datos: constitución, ley, reglamento, resoluciones
    b. Historia y evolución normativa del derecho a la protección de datos personales.
    c. Modelos de regulación mundial sobre protección de datos personales
    d. Análisis del derecho a la protección de datos personales en el derecho constitucional ecuatoriano.
    e. Ética digital y objetivos de la Ley Orgánica de Protección de Datos Personales.
    f. Conceptos básicos de la Ley Orgánica de Protección de Datos Personales.
        i. Datos personales
        ii. Titular

iii. Tratamiento

iv. Clasificación de los datos

v. Transferencia

2. Ámbito territorial y material de aplicación de la Ley Orgánica de Protección de Datos Personales.

3. Integrantes y roles del sistema de protección de datos personales

a. Titular

b. Responsables

c. Encargados

d. Delegados de protección de datos personales

e. Terceros

f. Autoridad de protección de datos personales

4. Bases legitimadoras de tratamiento

a. Aplicación de cada base dependiente cada caso concreto.

b. Validez de consentimiento Art. 8 Ley Orgánica de Protección de Datos Personales.

5. Principios

a. Interpretación en tratamiento de datos personales

b. Aplicación en el tratamiento de datos personales

c. Responsabilidad proactiva y demostrada

d. Protección de datos personales desde el diseño y por defecto

6. Finalidades del tratamiento

a. Objeto y Fundamentos prácticos

b. Tutela en el tratamiento de datos personales

7. Derechos de los titulares de datos personales

a. Alcance de los derechos (énfasis en casos prácticos de datos sensibles)

b. Excepciones a los derechos

c. Atención a los derechos

d. Canales de atención de derechos

e. Mecanismos de respuesta al ejercicio de derechos

f. Reglamento Denuncias vigente

g. Reglamento Consultas vigente

8. Transferencias internacionales de datos personales

a. Nivel adecuado de protección

b. Garantías adecuadas, tales como: sellos, certificaciones y cláusulas contractuales tipo

c. Normas corporativas vinculantes

d. Autorización para ejecución

e. Excepcionalidades

f. Registro de información de Transferencias Internacionales

9. Obligaciones con la Superintendencia de protección de datos personales de Responsables, Encargados, Terceros y Delegado de protección de datos personales

a. Notificaciones de brechas

b. Registros ante la autoridad

c. Denuncias

d. Ejercicio de derechos

e. Apoderados

10. Régimen sancionador

a. Proceso Administrativo Sancionador

b. Infracciones Leves y Graves

c. Sanciones Leves y Graves

d. Responsabilidad administrativa y aproximación a otras responsabilidades

Tema Optativo:

11. Fenómenos:

a. Cultural: Resaltar cómo la privacidad varía según las culturas y su impacto en las regulaciones locales e internacionales.

b. Analizar cómo la percepción de la privacidad ha evolucionado con la tecnología, desde el uso de redes sociales hasta la economía colaborativa y su relación con los Derechos Humanos.

c. Económico: Explicar cómo los datos personales se han convertido en un recurso estratégico para las empresas, impulsando modelos de negocio basados en *big data* y personalización.

BLOQUE 2: METODOLÓGICO – IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

NORMA OBLIGATORIA: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

1. Aproximación a las normas de mejores prácticas (Ej. *ISO/IEC* 27701, *ISO/IEC* 27001, 27002, 27005, 42001, *COBIT* 19, *OWASP ASVS*, *OWASP Top Ten*, *PCI-DSS, FAIR MODEL*, y entre otras).

2. Inicio de la implementación un sistema de gestión de protección de datos personales

a. Iniciación

b. Análisis de controles existentes de seguridad de la información

c. Alcance

d. Aprobación y coordinación del plan

3. Etapas

a. Definición y establecimiento

i. Políticas de protección de datos personales

ii. Gestión de riesgos para la protección de derechos y libertades

1. Establecimiento del contexto

2. Identificación de riesgos

3. Análisis de riesgos

4. Evaluación de riesgos

5. Tratamiento de riesgos

iii. Evaluación de impacto de tratamiento de datos personales

iv. Declaración de aplicabilidad (Justificar medidas de seguridad)

b. Implementación

i. Gestión de documental

ii. Selección de medidas de seguridad, organizacionales y técnicas

iii. Implementación

iv. Capacitación y comunicación

c. Monitoreo y revisión

i. Análisis y evaluación del rendimiento del sistema

ii. Auditorías internas y/o externas

d. Mantenimiento y mejora continua

i. Tratamiento de no conformidades

ii. Mejora continua e innovación

e. Optativo: Actividades prácticas sobre el contenido de los puntos detallados en el punto 3.

BLOQUE 3: TÉCNICO – CALIBRACIÓN DE RIESGOS Y SEGURIDAD DE DATOS

NORMA OBLIGATORIA: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

1. Establecimiento del Contexto

a. Planificación para la obtención de datos de entrada, elaboración de métricas, diseño de modelos de riesgo

b. Comprensión de los conceptos fundamentales de una gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos

c. Elaboración de criterios de evaluación para la protección de derechos y libertades

d. Determinación de la tolerancia y/o de la capacidad al riesgo.

2. Implementación de la identificación de riesgos

a. Perfilamiento de amenazas

b. Escaneo de vulnerabilidades técnicas y dependencias de software

c. Tipos de ciberataques (Ej. denegación de servicio, malware, entre otras)

3. Análisis cuantitativo de riesgos; ***(escoger cuantitativo y/o cualitativo)***

Se podrá considerar al menos uno de los siguientes métodos recomendados:

a. Probabilidad de ocurrencia

b. Métodos frecuentistas, métodos Bayesianos u otros aplicables

c. Distribuciones de probabilidades (continuas y discretas)

d. Modelos de riesgo (Ej: Modelo *FAIR*)

e. Valor al riesgo en ciberseguridad y en protección de datos

f. Análisis de Monte Carlo y/o Modelos de aprendizaje automático (analítica predictiva aplicada)

g. Métodos de calibración (Ej. *Conformal prediction* u otros aplicables)

4. Análisis cualitativo de riesgos ***(escoger cuantitativo y/o cualitativo)***

Se podrán considerar al menos uno de los siguientes métodos recomendados:

a. Métodos de calibración de opiniones (Ej. *Delphi*, *Lens*, etc.)

b. Técnicas para la elaboración de cuestionarios

c. Análisis argumental

d. Reducción de sesgos y ruido

e. Matrices de riesgos

f. *Rationales* (Justificar los valores de entrada y etiquetas en las matrices de riesgos)

5. Priorización de riesgos

a. Estrategias

b. Ponderación

6. Implementación de medidas de seguridad en protección datos personales

a. Medidas para la prevención de vulneraciones a la seguridad de datos personales

b. Medidas para la detección de vulneraciones a la seguridad de datos personales

c. Medidas para la respuesta a vulneraciones a la seguridad de datos personales

d. Interdependencias entre los controles de riesgos

e. Evaluación del rendimiento de las medidas de seguridad en el tiempo

f. Taxonomías de controles de riesgos (Ej: *ISO/IEC* 27001*, CIS Controls*, entre otras)

g. Recuperación de desastres y continuidad de actividades (*business continuity management*)

h. Respuesta a incidentes

Actividad Práctica optativa: Ejercicios donde los delegados respondan a incidentes simulados como *ransomware* o brechas en sistemas en la nube, u otros

BLOQUE 4: BLOQUE DE CONTENIDOS SUGERIDOS NO OBLIGATORIOS

1. Relación de la tecnología con la protección de datos personales:

Se podrán considerar al menos uno de los siguientes métodos recomendados:

a. *Big Data*,

b. *Analytics*,

c. *Machine Learning*,

d. Entre otras tecnologías

2. Talleres con herramientas y/o metodologías para gestión de riesgos en protección de datos.

3. Protección de Datos y Estrategia Empresarial:

a. Importancia de los datos personales del consumidor/usuario: Análisis del valor estratégico de los datos en la toma de decisiones empresariales y su relación con Derecho Humanos.

b. Tratamiento de datos en análisis de mercado y elaboración de perfiles: Estudio de casos internacionales que muestran cómo las empresas implementan estrategias de personalización respetando la privacidad de los usuarios.

c. Impacto reputacional y económico del cumplimiento normativo: Talleres para evaluar cómo la transparencia y la ética en el manejo de datos pueden convertirse en ventajas competitivas.

d. Gobernanza Corporativa y Compliance: Integración de la protección de datos en programas de cumplimiento y su relación con normas de compliance.

ESTIMACIÓN DE HORAS: mínimo 80.