RESOLUCIÓN Nº SPDP-SPD-2025-0005-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") reconoce y garantiza a 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. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*;

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 el artículo 135 del Código Orgánico Administrativo ("COA") determina que *"(...) 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 el artículo 136 del COA estatuye que *"[l]as administraciones públicas pueden establecer formularios de uso obligatorio y determinar los modelos de solicitudes, reclamos, recursos y, en general, de cualquier tipo de petición que se le dirija. Los formularios y modelos estarán a disposición de las personas en las dependencias administrativas y se publicarán a través de los medios de difusión institucional. La persona interesada puede acompañar los elementos que estime convenientes para precisar o completar los datos del formulario o modelo, los cuales no podrán ser inadmitidos y serán valorados por el órgano al momento de resolver (...)"*;

Que el artículo 1 de la Ley Orgánica de Protección de Datos Personales ("LOPDP") declara que aquella tiene por objeto 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 técnico de control, con potestad sancionatoria, de administración desconcentrada, con personalidad jurídica y autonomía administrativa, técnica, operativa y financiera;

Que el numeral 4 del artículo 76 de la LOPDP le atribuye a la SPDP funciones, atribuciones y facultades para *"[r]ealizar o delegar auditorías técnicas al tratamiento de datos personales (...)"*;

Que el artículo 81 del Reglamento General de la Ley Orgánica de Protección de Datos Personales ("RGLOPDP" estatuye que *"las actividades de control se realizarán de acuerdo con el plan anual aprobado por la máxima autoridad, el cual será elaborado considerando la naturaleza de las organizaciones controladas, el volumen y la sensibilidad de los datos personales sujetos a tratamiento, la aplicación de los diferentes procedimientos de control y la disponibilidad presupuestaria. Se podrán ejecutar procedimientos de control no considerados dentro de los planes anuales si la situación lo amerita, basados en criterios de criticidad, oportunidad y posibles lesiones al derecho a la protección de datos personales de uno o más titulares de datos personales (...)"*;

Que mediante resolución Nº SPDP-SPDP-2024-0001-R, publicada en el Tercer Suplemento del Registro Oficial Nº 624 de 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 ("Estatuto SPDP"), en virtud del cual se le atribuyó a la Intendencia General de Control y Sanción (ICS"), entre otras atribuciones y responsabilidades, la de *"dirigir y proponer el Plan Anual de Auditorías de Control de Protección de Datos Personales a base de los indicadores de riesgo suministrados por la unidad administrativa técnica (...)"*;

Que el numeral 9, artículo 10, del Anexo I del Estatuto SPDP establece, como uno de los entregables de la ICS, el Plan Anual de Auditorías;

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 d), artículo 5, se le ha delegado a la ICS, entre otras, la responsabilidad de *"[r]ealizar y/o delegar las auditorías técnicas a los sujetos que traten datos personales o que aparentaren tratarlos por cuenta de los sujetos regulados (...)"*;

Que mediante memorando Nº SPDP-IGCS-2025-0003-M suscrito el 20 de enero del 2025, la ICS remitió el informe técnico Nº SPDP-ICS-2025-001-I, que expresa la necesidad de expedir el *Reglamento de la Elaboración y Aprobación del Plan Anual de Auditorías de la Superintendencia de Protección de Datos Personales,* así como los motivos asociados a la demora en su presentación a la Intendencia General de Regulación de Protección de Datos Personales ("IRD");

Que a través del memorando Nº SPDP-IRD-2025-0013-M suscrito el 13 de febrero del 2025, la IRD remitió sus observaciones al proyecto normativo previamente enunciado, para lo cual concedió el término diez (10) días con el objeto de *"(...) subsanar las observaciones señaladas o, en su caso, modificar su propuesta inicial (...)"*;

Que por medio del memorando Nº SPDP-ICS-2025-0012-M, suscrito y notificado el 25 de febrero del 2025, la ICS subsanó las observaciones realizadas por la IRD;

Que mediante memorando N° SPDP-IRD-2025-0022-M del 27 de febrero del 2025 se remitió el expediente a la Dirección de Asesoría Jurídica ("DAJ");

Que a través del memorando Nº SPDP-DAJ-2025-0017-M del 27 de febrero del 2025, el Director de Asesoría Jurídica remitió, a la IRD, el informe N° INF-SPDP-DAJ-2025-0003, en el cual confirmó que la propuesta del *Reglamento de la Elaboración y Aprobación del Plan Anual de Auditorías de la Superintendencia de Protección de Datos Personales* cumple con el principio de legalidad, que no vulnera ni contradice las normas matrices y que aporta al cumplimiento de los objetivos de la SPDP;

Que mediante el informe técnico Nº INF-SPDP-IRD-2025-0017, 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-2025-0064-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 EL REGLAMENTO PARA LA ELABORACIÓN Y APROBACIÓN DEL

PLAN ANUAL DE AUDITORÍAS DE LA SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I
NORMAS GENERALES

CAPÍTULO ÚNICO
OBJETO, ÁMBITO DE APLICACIÓN, DEFINICIONES, PRINCIPIOS Y VALORES

Art. 1.- Este reglamento tiene por objeto determinar los lineamientos y procedimientos para la elaboración y aprobación del Plan Anual de Auditorías ("PAA"), que la SPDP habrá de realizarle a los administrados.

Art. 2.- El reglamento será de cumplimiento obligatorio para la ICS de la SPDP, en atención a sus atribuciones y facultades de control y supervisión debidamente delegadas mediante el acto administrativo respectivo.

Art. 3.- Las palabras, siglas y acrónimos enlistados a continuación tendrán los significados asociados a los mismos:

3.1. Auditoría: Proceso técnico y jurídico, sistemático y documentado, mediante el cual se evalúa el grado de cumplimiento de un administrado con relación a las disposiciones establecidas en la LOPDP, el RGLOPDP y demás normativa emitida por la SPDP.

3.2. Boletín Informativo de Auditorías Anuales: Documento que contiene el extracto relevante del PAA, que será publicado en la página web institucional de la SPDP.

3.3. Delegado: El funcionario a quien, de conformidad con la resolución Nº SPDP-SPD-2025-0001-R del 31 de enero del 2025, se le ha encargado la gestión del respectivo proceso sustantivo que es objeto de delegación.

3.4. ICS: La Intendencia General de Control y Sanción o, según el contexto, el Intendente General de Control y Sanción.

3.5. LOPDP: Ley Orgánica de Protección de Datos Personales.

3.6. PAA: Plan Anual de Auditoría.

3.7. RGLOPDP: Reglamento General a la Ley Orgánica de Protección de Datos Personales.

3.8. SPDP: La Superintendencia de Protección de Datos Personales.

3.9. Superintendente: El Superintendente de Protección de Datos Personales.

Art. 4.- Para la elaboración del PAA se deberán aplicar, en todo momento, los derechos y principios establecidos en la Constitución de la República del Ecuador; los tratados y convenios internacionales en materia de protección y privacidad de datos personales; la LOPDP; el RGLOPDP y, en general, cualquier norma jurídica que, expedida de conformidad con la Constitución de la República, tenga o pudiere tener, como ámbito de aplicación material, el tratamiento de datos personales.

TÍTULO II
DEL PROCEDIMIENTO DE APROBACIÓN Y ELABORACIÓN DEL PAA

CAPÍTULO I
RESPONSABILIDAD Y PROCESO

Art. 5.- La ICS llevará a cabo el proceso de elaboración y aprobación del PAA durante el ejercicio económico inmediatamente anterior a su ejecución, el cual iniciará el primer día laborable de cada junio.

Art. 6.- El PAA, además de hallarse debidamente justificado, deberá estar provisto del siguiente contenido:

6.1. Datos generales:

6.1.1. Número de informe;

6.1.2. Nombre de la autoridad competente;

6.1.3. Nombre de la Intendencia encargada de la elaboración del PAA;

6.1.4. Ejercicio fiscal dentro del cual será aplicable el PAA;

6.1.5. Nombre del responsable de quien ha elaborado, revisado y aprobado el PAA;

6.1.6. Correo electrónico del responsable de la elaboración del PAA; y,

6.1.7. Fecha de aprobación y actualización del PAA.

6.2. Introducción:

6.2.1. Antecedentes;

6.2.2. Marco legal;

6.2.3. Alineación con la planificación estratégica institucional:

6.2.3.1. Misión institucional;

6.2.3.2. Visión institucional; y,

6.2.3.3. Objetivo estratégico institucional.

6.3. Desarrollo:

6.3.1. Alcance;

6.3.2. Metodologías utilizadas;

6.3.3. Objetivos:

6.3.3.1. Objetivo general; y,

6.3.3.2. Objetivos específicos.

6.3.4. Criterios de auditoría;

6.3.5. Programación de actividades;

6.3.6. Recursos para la ejecución del PAA; y,

6.3.7. Indicadores de medición.

6.4. Conclusiones.

6.5. Recomendaciones.

6.6. Anexos.

Art. 7.- La ICS deberá remitir la propuesta de PAA al Superintendente o su delegado para su consideración hasta el último día laborable de cada agosto, quien, a su vez, deberá emitir sus observaciones, en caso de haberlas, o aprobarlo hasta la finalización de la segunda semana de cada septiembre.

Art. 8.- En caso de existir observaciones o modificaciones, el borrador del PAA será devuelto al ICS, quien deberá subsanar los reparos o absolver las dudas en un término máximo de quince (15) días. Posteriormente, se lo deberá remitir al Superintendente o su delegado para la aprobación y suscripción.

Art. 9.- El PAA, debidamente suscrito por el Superintendente de Protección de Datos Personales, tendrá carácter reservado para el público en general y para los funcionarios de la SPDP, salvo para los de la ICS y el Superintendente o su delegado.

CAPÍTULO II
DE LOS CRITERIOS EMPLEADOS PARA LA SELECCIÓN DEL (DE LOS) SECTORES Y SUJETOS AUDITADOS

Art. 10.- La selección del (de los) sector(es) y sujetos auditados que realicen actividades de tratamiento se basará en criterios objetivos.

Hecha la selección, se definirá la cantidad de inspecciones a efectuar sobre la base de los criterios que se establecen seguidamente y sin perjuicio de otros que pudieren corresponder:

10.1. Alcance del tratamiento en el derecho a la protección de datos personales de los titulares;

10.2. Impacto y riesgo del tratamiento en el derecho a la protección de datos personales de los titulares;

10.3. Volumen, sensibilidad o categoría especial de los datos personales;

10.4. Vulnerabilidad de los titulares de datos personales;

10.5. Cantidad de denuncias recibidas;

10.6. Criticidad de las denuncias recibidas;

10.7. Actualizaciones significativas en las regulaciones sectoriales de los sujetos que realizan actividades de tratamiento;

10.8. Uso de innovación tecnológica en las actividades de tratamiento;

10.9. Aplicación de procedimientos de control;

10.10. Disponibilidad de recursos (humanos, financieros, técnicos); y,

10.11. Cantidad y gravedad de las vulneraciones de seguridad de datos personales reportadas.

CAPÍTULO III
DEL BOLETÍN INFORMATIVO DE AUDITORÍAS ANUALES

Art. 11.- El Boletín Informativo de Auditorías Anuales (“Boletín”) es el mecanismo que se utilizará para dar publicidad a la gestión de la SPDP y cumplir el principio de transparencia previsto en la LOPDP.

Art 12.- El Boletín deberá contener la siguiente información:

12.1. Nombre de la autoridad competente;

12.2. Nombre de la Intendencia encargada de la elaboración del PAA;

12.3. Ejercicio fiscal dentro del cual será aplicable el PAA;

12.4. Fecha de aprobación del PAA; y,

12.5. Sector(es) auditado(s).

Art 13.- Una vez aprobado y suscrito el PAA por el Superintendente o su delegado, la ICS elaborará el Boletín y lo remitirá al Superintendente o su delegado para su aprobación.

En caso de que el Boletín fuere observado por el Superintendente o su delegado, será devuelto a la ICS para que realice los cambios necesarios dentro del término de cinco (5) días. En el decurso de dicho término, será enviado al Superintendente o su delegado para la aprobación final.

Una vez aprobado por el Superintendente o su delegado, será devuelto a la ICS que, a su vez, solicitará a la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales ("IIT") la publicación del Boletín en la página web institucional para conocimiento de la ciudadanía. Dicho Boletín deberá permanecer publicado durante todo el ejercicio fiscal al que haga referencia.

De igual manera, la página web institucional tendrá un apartado histórico dentro del cual se podrán verificar las publicaciones del Boletín de cada ejercicio fiscal.

Art. 14.- En caso de que el Superintendente, su delegado o la ICS identificaren la necesidad de incluir o excluir procesos de auditoría en la planificación, se deberá realizar un informe de necesidad para explicar las razones por las cuales se modificará el PAA y de qué forma esto garantiza el derecho de protección de datos personales.

El informe será realizado por la ICS y será remitido al Superintendente o su delegado junto con el PAA modificado y el Boletín actualizado para su revisión y aprobación.

Art. 15.- Si las modificaciones realizadas al PAA hicieren referencia al ejercicio fiscal aplicable o al (a los) sector(es) auditado(s), se publicará un Boletín actualizado que deberá contener lo siguiente:

15.1. Actualización al ejercicio fiscal aplicable:

15.1.1. Nombre de la autoridad competente;

15.1.2. Nombre de la intendencia encargada de la elaboración del PAA;

15.1.3. Fecha de aprobación del PAA original;

15.1.4. Fecha de aprobación de la actualización del PAA;

15.1.5. Ejercicio fiscal dentro del cual iba a ser aplicable el PAA;

15.1.6. Actualización del ejercicio fiscal dentro del cual será aplicable el PAA; y,

15.1.7. Exposición de argumentos respecto de la procedencia de la modificación.

15.2. Sector(es) auditado(s):

15.2.1. Actualización al (a los) sector(es) auditado(s);

15.2.2. Nombre de la autoridad competente;

15.2.3. Nombre de la intendencia encargada de la elaboración del PAA;

15.2.4. Fecha de aprobación del PAA original;

15.2.5. Fecha de aprobación de la actualización del PAA;

15.2.6. Ejercicio fiscal dentro del cual será aplicable el PAA;

15.2.7. Sector(es) auditado(s) inicialmente seleccionado(s) dentro del PAA original;

15.2.8. Sector(es) auditado(s) modificado(s) PAA; y,

15.2.9. Exposición de argumentos respecto de la procedencia de la modificación.

DISPOSICIONES GENERALES

Primera.- En el marco de las competencias asignadas a la SPDP, la ICS incorporará, dentro del Plan Regulatorio Institucional correspondiente al ejercicio fiscal 2026, la elaboración de un reglamento específico que regule el procedimiento de auditoría.

Segunda.- En el reglamento que regule el procedimiento específico de auditoría, se incorporarán mecanismos de retroalimentación institucional que permitan evaluar la eficacia, eficiencia y pertinencia del proceso de auditoría, con el propósito de identificar oportunidades de mejora y optimización continua. La retroalimentación recibida será objeto de análisis, a fin de introducir los ajustes y actualizaciones necesarias en el procedimiento, para así garantizar su evolución constante y su adecuación a las mejores prácticas en materia de control y supervisión de la protección de datos personales.

DISPOSICIÓN TRANSITORIA

Por cuanto la SPDP inició sus actividades en la segunda quincena de septiembre del 2024, el PAA correspondiente al año fiscal 2025 no seguirá el procedimiento establecido en este Reglamento y, por ende, será elaborado únicamente a base del informe técnico emitido por la ICS, aprobado por el Superintendente o su delegado y, posteriormente, publicado a través del Boletín en el portal institucional.

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 30 de abril del 2025.

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES