spdp Superintendencia de Protección de Datos Personales

RESOLUCIÓN N° SPDP-SPD-2026-0039-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 artículo 4 de la LOPDP define a los datos biométricos como un *"[d]ato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros"*;

Que ese mismo artículo caracteriza a los biométricos como datos sensibles, debido a que su indebido tratamiento podría exponer a sus titulares a discriminación, daños potenciales o al menoscabo de sus derechos fundamentales y libertades individuales;

Que la letra a) del artículo 25 de la LOPDP determina que los datos sensibles se consideran categorías especiales de datos personales;

Que el uso creciente de tecnologías biométricas en servicios públicos y privados genera riesgos específicos para los derechos fundamentales y las libertades individuales de las personas, tales como la discriminación algorítmica, la identificación indebida y la reutilización de datos para finalidades incompatibles;

Que resulta necesario establecer criterios específicos para el tratamiento de datos biométricos, atendiendo a su especial naturaleza y a los riesgos asociados a su utilización;

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 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 N° SPDP-SPD-2024-0022-R, publicada en el Registro Oficial N° 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 para establecer los parámetros para el uso de datos biométricos;**

Que la IRD, mediante informe técnico **Nº INF-SPDP-IRD-2026-0020** del **19** de **marzo** del **2026,** justificó la pertinencia de emitir la **Norma General para el Tratamiento de Datos Biométricos,** con el fin de establecer los parámetros técnicos, jurídico-organizativos y de proporcionalidad para el uso de datos biométricos, incluidos los criterios para la evaluación de impacto, los protocolos de consentimiento informado y las medidas de seguridad, por lo que, en su parte pertinente expuso: *"(...) [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 (...) la Norma General para el Tratamiento de Datos Biométricos (...)";* y, por ende recomendó: *"(...) [i]niciar el proceso de socialización del proyecto de Resolución que expide la Norma General Para el Tratamiento de Datos Biométricos, para que en el término de veinte (20) días la ciudadanía pueda avocar conocimiento de la norma"*;

Que mediante memorando **N° SPDP-IRD-2026-0048-M** suscrito el **19** de **marzo** del **2026,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") el proyecto normativo denominado **Norma General para el Tratamiento de Datos Biométricos,** como el informe técnico **N° INF-SPDP-IRD-2026-0020,** 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 a través del informe jurídico **N° INF-SPDP-DAJ-2026-0013,** remitido a la IRD mediante memorando **N° SPDP-DAJ-2025-0044-M** suscrito el **27** de **marzo** del **2026,** la DAJ determinó que el proyecto denominado **Norma General para el Tratamiento de Datos Biométricos** es congruente con los principios de la LOPDP, por cuanto 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-IRD-2026-0057-M** suscrito el **30** de **marzo** 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 **Norma General para el Tratamiento de Datos Biométricos** en la página web institucional y en las redes sociales de la SPDP, para que tal proyecto se encuentre disponible para la ciudadanía, las organizaciones de la sociedad civil o interesados, desde el **31** de **marzo** del **2026** hasta el **28** de **abril** 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 **Norma General para el Tratamiento de Datos Biométricos** dentro del término de veinte (20) días, de conformidad con el artículo 12 de la mencionada resolución;

Que a través del informe técnico **N° INF-SPDP-IRD-2026-0053** suscrito el **20** de **agosto** 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 memorando **N° SPDP-IRD-2026-0147-M** suscrito el **20** 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-2026-166-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 General para el Tratamiento de Datos Biométricos,** 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 GENERAL PARA EL TRATAMIENTO DE DATOS BIOMÉTRICOS

TÍTULO I
NORMAS GENERALES

Art. 1.- Esta norma tiene por objeto regular las condiciones, garantías y límites aplicables al tratamiento de los datos biométricos, así como establecer las reglas necesarias y específicas con el objeto de tratarlos de manera adecuada en procura de la tutela efectiva de los derechos y las libertades de los titulares.

La norma desarrolla los principios y las disposiciones previstos en la LOPDP, atendiendo la naturaleza particular de los datos biométricos, su capacidad de identificación unívoca y los riesgos que su tratamiento podría implicar para la privacidad.

Art. 2.- Las disposiciones de esta norma serán aplicables al tratamiento de datos biométricos con fines identificativos realizado por responsables y encargados de los sectores público y privado, según corresponda, que están sujetos al ámbito de aplicación territorial de la LOPDP.

Esta norma se aplicará a todo tratamiento de datos biométricos efectuado mediante procedimientos automatizados o parcialmente automatizados, así como al tratamiento no automatizado cuando dichos datos formaren parte de sistemas, soportes informáticos o bases de datos estructuradas.

Las disposiciones de esta norma serán de aplicación obligatoria, sin perjuicio de otras regulaciones sectoriales expedidas por autoridad pública competente que establecieren condiciones específicas para el uso de tecnologías biométricas.

Art. 3.- Los datos biométricos, por ser legalmente considerados como sensibles, constituyen una categoría especial de datos personales cuando su tratamiento se realiza a través de medios que permitieren o tuvieren por finalidad identificar de manera unívoca a una persona natural, para lo cual se deberá verificar el cumplimiento de la LOPDP en lo que respecta al tratamiento de datos sensibles.

Siempre que el tratamiento de los datos biométricos no tuviere por finalidad o resultado la identificación unívoca de personas naturales, su tratamiento se regirá por las disposiciones establecidas por la LOPDP, el Reglamento General de la LOPDP (“RGLOPDP”) y la normativa secundaria aplicable, sin perjuicio de implementar las medidas de seguridad correspondientes.

TÍTULO II
DEFINICIONES Y REQUISITOS PARA EL TRATAMIENTO

Art. 4.- Para efectos del tratamiento de datos biométricos, las palabras enlistadas a continuación tendrán los siguientes significados:

4.1. Asimetría significativa: Es una situación en la que existe un desequilibrio de poder, autoridad, dependencia o subordinación entre el responsable del tratamiento y el titular de los datos personales; desequilibrio que puede afectar la capacidad de este último para manifestar una voluntad libre, específica, informada, inequívoca y de

manera explícita, respecto del tratamiento de sus datos biométricos o para ejercer efectivamente sus derechos.

4.2. Dato biométrico bruto: Es la información biométrica capturada directamente de una persona natural, tales como las imágenes faciales, las huellas dactilares, los patrones de voz, los escaneos de iris o cualquier otro rasgo biométrico.

4.3. Decisiones basadas en biometría con intervención humana: Es la participación de una persona natural en un proceso de decisión automatizada basada en biometría, que se limita a confirmar o ejecutar el resultado generado por el sistema, sin efectuar una evaluación independiente y efectiva del caso ni tener capacidad real para modificar la decisión propuesta o tomada.

4.4. Espacio público: Es todo lugar físico al que el público tiene acceso general, independientemente de su titularidad o dominio público o privado, tales como los centros comerciales, las estaciones de transporte, los estadios, las plazas o los parques, entre otros.

4.5. Identificación biométrica: Es la comparación de una muestra biométrica con múltiples registros almacenados en una o varias bases de datos para determinar la identidad de una persona natural.

4.6. Identificación unívoca: Es la capacidad de un sistema biométrico para identificar o verificar la identidad de una persona natural de forma única mediante el tratamiento de sus características físicas, fisiológicas o conductuales.

4.7. Imposibilidad técnica: Es una situación acreditada mediante análisis técnico previo y documentado que demuestra, justifica y prueba fehacientemente que las alternativas razonablemente disponibles de carácter no biométrico resultan insuficientes, inviables o incapaces de cumplir la finalidad perseguida con un nivel equivalente de seguridad, confiabilidad o eficiencia operativa.

4.8. Plantilla biométrica: Es la representación matemática, codificada y derivada del dato biométrico bruto y utilizada para efectuar comparaciones biométricas. El responsable del tratamiento deberá privilegiar, en todo momento, el uso de plantillas biométricas y evitar, salvo estricta necesidad técnica, el almacenamiento de datos biométricos brutos.

4.9. Sistemas biométricos: Es el conjunto de tecnologías, procesos y dispositivos destinados a capturar, procesar, analizar o comparar datos biométricos con el propósito de identificar y/o verificar la identidad de una persona natural. Los sistemas biométricos incluyen, entre otros, aquellos que están basados en el reconocimiento facial, las huellas dactilares, así como reconocimiento de iris, voz, patrones de comportamiento o cualquier otra tecnología que utilizare rasgos biométricos.

4.10. Verificación biométrica: Es la comparación de una muestra biométrica con una plantilla previamente asociada a una identidad declarada, con el fin de confirmar dicha identidad.

Art. 5.- El tratamiento de datos biométricos deberá, en todo momento, estar precedido de un análisis de riesgos y su correspondiente evaluación de impacto, que justifique suficientemente la utilización de sistemas biométricos para la finalidad perseguida; todo ello de acuerdo con la LOPDP, el RGLOPDP y la normativa secundaria aplicable.

La determinación del nivel de riesgo deberá realizarse en cada caso, considerando, entre otros factores, la finalidad, el alcance y el contexto del tratamiento, así como el tipo y el volumen de los datos biométricos objeto de tratamiento. Para ello, se deberán aplicar las medidas de seguridad correspondientes que estuvieren determinadas a partir del análisis de riesgos y su

evaluación de impacto, de conformidad con lo previsto en la normativa aplicable de protección de datos.

Se considerarán de alto riesgo aquellos tratamientos de datos biométricos que:

5.1. Tuvieren como resultado la identificación unívoca de personas naturales;

5.2. Implicaren la evaluación sistemática o exhaustiva de aspectos personales mediante tratamientos automatizados, sobre cuya base se adopten decisiones que produzcan afectación a derechos y libertades fundamentales sobre las personas naturales; o,

5.3. Conllevaren la observación sistemática, a gran escala, de zonas de acceso público.

Art. 6.- El tratamiento de datos biométricos será lícito únicamente cuando exista una base de legitimación válida de conformidad con el tratamiento de datos sensibles contemplado en la LOPDP.

Siempre que, de manera técnica y cabalmente demostrada, los tratamientos de datos biométricos no incluyeren identificación unívoca o verificación biométrica, se los podrá realizar al amparo de las bases de legitimación de la LOPDP.

Art. 7.- Cuando el tratamiento biométrico se basare en el consentimiento, el responsable o encargado, según corresponda, deberá garantizar, en forma obligatoria, que dicho consentimiento sea previo, libre, específico, informado, inequívoco y explícito.

Asimismo, el responsable o encargado, según corresponda, deberá ofrecerle al titular al menos un mecanismo alternativo equivalente que no requiera el uso de biometría. La excepción por imposibilidad técnica solo será aplicable cuando el responsable o encargado, según corresponda, hubiese documentado, acreditado y demostrado, debida y suficientemente en la evaluación de impacto del tratamiento de datos personales (“EIPD”), que ningún mecanismo alternativo permite alcanzar la finalidad legítima con niveles de seguridad equivalentes, o que la finalidad del tratamiento no se pudiese lograr razonablemente por otros medios.

Art. 8.- Cuando el tratamiento de datos biométricos se sustente en el consentimiento, pero en contextos en los que existiere una relación de asimetría significativa entre el responsable o encargado, según corresponda, y el titular de los datos, se deberá garantizar que dicho consentimiento sea explícito y cumpla con todas las condiciones previstas en la LOPDP.

Para los efectos de este artículo, se entenderá que existe asimetría significativa únicamente cuando concurriesen elementos que puedan afectar de manera real la libertad de decisión del titular, tales como:

8.1. La existencia de una relación de subordinación jurídica o dependencia económica directa;

8.2. El condicionamiento del acceso a derechos fundamentales, servicios esenciales o beneficios relevantes; o,

8.3. La ausencia de alternativas reales y razonables para el titular dentro del contexto específico del tratamiento.

En los casos en que se configure una asimetría significativa, el responsable o encargado, según corresponda deberá, como regla general, ofrecerle al titular una alternativa razonable no biométrica, salvo que existiere imposibilidad técnica o fáctica debidamente justificada, una obligación derivada de una norma con rango de ley o una disposición expedida por autoridad pública competente.

Art. 9.- Se entenderá que existe imposibilidad técnica o fáctica cuando:

9.1. No existiesen mecanismos alternativos que garanticen un nivel equivalente de seguridad y eficacia; o,

9.2. Las alternativas disponibles resultaren manifiestamente insuficientes para prevenir riesgos, tales como suplantación de identidad, accesos no autorizados o fraudes, especialmente en contextos de seguridad, infraestructuras críticas o servicios de alto impacto.

Art. 10.- El titular de los datos personales podrá, de todas formas, revocar su consentimiento en cualquier momento, en cuyo caso se deberán implementar los medios o mecanismos para que tal revocatoria se pueda hacer efectiva de manera expedita y célere.

Art. 11.- No se considerará relación de asimetría significativa el uso de biometría para la autenticación en operaciones sujetas a obligaciones de debida diligencia reforzada, de acuerdo con las normativas de prevención de fraude, lavado de activos y financiamiento del terrorismo.

TÍTULO III
PRINCIPIOS DE FINALIDAD, NECESIDAD Y PROPORCIONALIDAD

Art. 12.- Queda prohibida la reutilización de datos biométricos para cualquier finalidad distinta a aquella que legitimó su obtención inicial. Cualquier nuevo tratamiento o finalidad adicional requerirá:

12.1. La obtención de un nuevo consentimiento libre, específico, informado e inequívoco por parte del titular; o,

12.2. En el caso de tratamiento de datos sensibles, verificar que se cumplan las previsiones y requisitos que, al efecto, están contemplados en la LOPDP, el RGLOPDP y la demás normativa aplicable.

Art. 13.- Antes de implementar un sistema biométrico, el responsable o encargado, según corresponda, deberá evaluar si el objetivo perseguido puede alcanzarse mediante mecanismos menos invasivos o riesgosos para la privacidad de las personas.

El uso de biometría solo será admisible cuando resulte estrictamente necesario para alcanzar la finalidad prevista y cuando no existieren otros medios que permitan cumplirla.

TÍTULO IV
DISEÑO, SEGURIDAD Y EVALUACIÓN DE IMPACTO

Art. 14.- Los sistemas biométricos deberán diseñarse e implementarse de conformidad con los principios de protección de datos desde el diseño y por defecto, además de garantizar que el tratamiento de datos biométricos incorpore salvaguardas técnicas y organizativas desde las fases iniciales de concepción del sistema. Para ello, el responsable o encargado, según corresponda, deberá asegurar la minimización de los datos tratados, la limitación estricta de accesos, la seguridad reforzada y la adopción de arquitecturas tecnológicas que reduzcan estructuralmente el riesgo de identificación indebida, reutilización no autorizada o filtración de datos biométricos.

Art. 15.- El responsable o encargado, según corresponda, deberá realizar en forma obligatoria la EIPD antes de implementar cualquier sistema biométrico.

La EIPD deberá identificar, analizar, y evaluar los riesgos para los derechos y libertades de las personas, así como establecer las medidas necesarias para mitigarlos siguiendo los lineamientos del marco normativo aplicable.

La EIPD deberá ser revisada y actualizada cada doce (12) meses y también cuando cambie el nivel de riesgo del tratamiento.

Art. 16.- El tratamiento de datos biométricos requerirá la implementación de medidas de seguridad reforzadas, acordes con los resultados de su análisis de riesgos y la EIPD realizada para cada uno de los tratamientos; ello de acuerdo con la versión que estuviere vigente de la *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales* de la SPDP.

TÍTULO V
TRANSPARENCIA Y DERECHOS DE LOS TITULARES

Art. 17.- El responsable o encargado, según corresponda, deberá cumplir con la obligación de informarle al titular de forma clara, comprensible y accesible sobre todo tratamiento de datos personales biométricos, de conformidad con el artículo 12 de la LOPDP, particularmente en lo que respecta:

17.1. A la obligación de proporcionarle al titular información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas; y,

17.2. A la obligación de transmitirle tal información, en cualquier modo comprobable, en un lenguaje, claro, sencillo y de fácil comprensión.

Art. 18.- Las decisiones que produjeren efectos jurídicos o que afectaren a los derechos y las libertades fundamentales del titular de datos, no podrán basarse exclusivamente en sistemas automatizados de identificación biométrica o en decisiones basadas mayoritariamente en biometría con intervención humana formal o testimonial.

El titular tendrá derecho a solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada.

TÍTULO VI
LIMITACIONES ESPECÍFICAS

Art. 19.- El responsable o encargado, según corresponda, que use tecnologías de reconocimiento facial deberá cumplir con lo establecido en el artículo 26 de la LOPDP, así como realizar el análisis de riesgos, la EIPD e implementar medidas de seguridad reforzadas considerando la naturaleza, las finalidades y los medios utilizados en el tratamiento de datos biométricos.

Además, el responsable o encargado, según corresponda, deberá asegurarse de que estas medidas de seguridad garanticen la protección de los datos biométricos en su ciclo de vida, pero también deberá revisar y actualizar el análisis de riesgos y la EIPD de forma periódica o cuando se actualizare la tecnología empleada.

El uso de tecnologías de reconocimiento facial no constituye, por sí mismo, un tratamiento de datos a gran escala; sin embargo, será obligación del responsable o encargado, según corresponda, verificar lo establecido en el RGLOPDP y en la normativa secundaria específica aplicable.

Art. 20.- Queda prohibido el uso de sistemas biométricos destinados a la identificación masiva e indiscriminada de personas naturales en espacios públicos. Excepcionalmente —y por mandato expreso de una norma con rango de ley— se podrá habilitar su uso, siempre y cuando el responsable o encargado, según corresponda, justifique de manera motivada el tratamiento y garantice el cumplimiento de los principios de la LOPDP, sin contrariar la CRE.

Art. 21.- El tratamiento de datos biométricos de niños, niñas y adolescentes con fines identificativos está prohibido, salvo que no existiesen otros medios menos invasivos o riesgosos para cumplir con la finalidad del tratamiento, y siempre que se cuente el respectivo análisis de riesgos y la EIPD.

La legitimación para el tratamiento de datos biométricos de niños, niñas y adolescentes deberá realizarse mediante el consentimiento explícito otorgado por su representante legal, tutor o curador del niño, niña o adolescente; o, excepcionalmente, cuando dicho tratamiento esté destinado a salvaguardar la vida del titular, bajo el supuesto de que aquel no se encontrare capacitado, física o jurídicamente, para dar su consentimiento; esto último de conformidad con la letra g) del artículo 26 de la LOPDP.

Art. 22.- Los adolescentes con edades comprendidas entre los quince (15) y los diecisiete (17) años podrán otorgar su consentimiento explícito por sí mismos, siempre que la información les fuese proporcionada en un lenguaje sencillo y adaptado a su edad.

Excepcionalmente, el representante legal podrá solicitar la revocación de dicho consentimiento cuando existieren motivos razonables y debidamente fundamentados para considerar que el tratamiento implica un alto riesgo para los derechos y las libertades fundamentales del adolescente o si se comprometiere su interés superior. El responsable o encargado, según corresponda, deberá evaluar la solicitud y adoptar las medidas correspondientes en función del interés superior de niñas, niños y adolescentes.

DISPOSICIÓN TRANSITORIA

Los responsables o encargados del tratamiento que estuvieren utilizando sistemas biométricos al momento de la entrada en vigencia de esta norma, deberán adecuar sus procesos y sistemas dentro del plazo de doce (12) meses contados desde la publicación de esta norma general en el Registro Oficial.

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