

RESOLUCIÓN N°
EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES
CONSIDERANDO:

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 ídem, detentan “personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa (...)”.

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

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

Que, el artículo 4 de la LOPD incluye dentro de los datos sensibles a los datos de salud los cuales constituyen información particularmente sensible debido a que su información es respecto a la esfera más íntima de una persona natural y tiene capacidad de identificar de manera única a las mismas.

Que, el artículo 25 de la LOPDP establece como categorías especiales a los datos de salud y adicionalmente a los datos sensibles, por lo que se evidencia que hay un doble nivel de especialidad.

Que, el artículo 26 de la LOPDP menciona que todo tratamiento de datos sensibles está prohibido a no ser que concurra una de las siguientes excepciones: “a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines. b) El tratamiento es necesario para el

cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social. c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento. d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos. e) El tratamiento se lo realiza por orden de autoridad judicial. f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente Ley”.

Que, en este mismo sentido el artículo 30 de la LOPDP menciona que *“Las instituciones que conforman el Sistema Nacional de Salud y los profesionales de la salud pueden recolectar y tratar los datos relativos a la salud de sus pacientes que estén o hubiesen estado bajo tratamiento de aquellos, de acuerdo a lo previsto en la presente Ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales en coordinación con la autoridad sanitaria nacional. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas. Esta obligación será complementaria del secreto profesional de conformidad con cada caso. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento, No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular; Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional”.*

Que, el artículo 31 de la LOPDP indica que *“Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto: 1. Los datos relativos a la salud generados en establecimientos de salud públicos o privados, serán tratados cumpliendo los principios de confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo conforme lo determina esta Ley, salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para*

finde de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria, y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad. 2. Los datos relativos a la salud que se traten, siempre que sea posible, deberán ser previamente anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos. 3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para obtener la autorización mencionada, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos y el informe previo favorable emitido por la Autoridad Sanitaria”.

Que, el artículo 32 de la LOPDP establece que “Los datos relativos a salud que consten en las instituciones que conforman el Sistema Nacional de Salud, podrán ser tratados por personas naturales y jurídicas privadas y públicas con fines de investigación científica, siempre que según el caso encuentren anonimizados, o dicho tratamiento sea autorizado por la Autoridad de Protección de Datos Personales, previo informe de la Autoridad Sanitaria Nacional”.

Que, en concordancia con los artículos previamente citados, el numeral 2 del artículo 4 del RGLOPDP menciona que “La definición de datos de salud establecida en la Ley comprende la información relativa a todos los aspectos de salud, tanto físicos como psíquicos, de la persona. Se incluyen todos los datos relativos al estado de salud del titular que dan información sobre su estado de salud física o mental pasado, presente o futuro. Así también contiene la información sobre la persona natural recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o dato asignado a una persona natural que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del titular, independientemente de su fuente”.

Que, el artículo 11 del RGLOPDP indica que “Finalizado el plazo de conservación de los datos, el responsable del tratamiento de datos deberá proceder a la eliminación segura de los mismos. La eliminación de datos personales no aplicará cuando el tratamiento sea necesario en los siguientes supuestos: 1. Por razones de interés público en el ámbito de la salud pública y privada, así como en materia estatal, seguridad, laboral y educación; 2. Para la formulación, el ejercicio o la defensa de reclamaciones. La Autoridad de Protección de Datos Personales podrá requerir información cuando lo considere necesario. Para el efecto, ajustará los requerimientos a normas, lineamientos sobre plazo de conservación y estándares internacionales sobre la eliminación de datos”.

Que, mediante resolución N° SPDP-SPD-2026-0030-R del 22 de julio del 2026, publicada en el Tercer Suplemento del Registro Oficial N° 339 del 3 de agosto del 2026, el Superintendente de Protección de Datos Personales aprobó y expidió la Codificación del Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la Superintendencia de Protección de Datos Personales (“Codificación”).

Que, en el artículo 1 de la Codificación 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 número 12.1.3.2. de la Codificación 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, en el número 12.1.3.3. de esa misma Codificación, 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 N° SPDP-SPD-2026-0035-R del 20 de agosto del 2026, publicada en el Registro Oficial N° 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 N° 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, mediante resolución N° SPDP-SPDP-2024-0018-R, publicada en el Registro Oficial N° 679 del 8 de noviembre del 2024, se expidió el Reglamento para la Elaboración y Aprobación del Plan Regulatorio Institucional y se estableció el procedimiento para el procedimiento de aprobación y elaboración del Plan Regulatorio Institucional.

Que, mediante resolución N° SPDP-SPD-2025-0050-R, expedida el 30 de diciembre de 2025, en la cual se aprobó el PRI 2026, se determinó la necesidad de emitir la normativa donde se regule el tratamiento de datos personales relativos a la salud.

Que la IRD, mediante informe técnico N° INF-SPDP-IRD-2026-0059 del 11 de septiembre del 2026, justificó la pertinencia de emitir la **Norma General para el Tratamiento de Datos Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado**, con el fin de establecer los lineamientos para el tratamiento de datos personales de salud, incluidos los criterios para el 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 Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado”; y, por ende recomendó: “(...) a iniciar con el proceso de socialización del proyecto de “Norma General Para el Tratamiento de Datos Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado”, en cumplimiento con lo dispuesto por la resolución N° SPDP-SPDP-2024-0022-R para que en el término de veinte (20) días la ciudadanía pueda avocar conocimiento de la norma”;

Que mediante memorando N° SPDP-IRD-2026-00xx-M suscrito el 11 de septiembre 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 Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado**, como el informe técnico N° INF-SPDP-IRD-2026-00xx, 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-2026-00xx, remitido a la IRD mediante memorando N° SPDP-DAJ-2025-00xx-M suscrito el xx de septiembre del 2026, la DAJ determinó que el proyecto denominado **Norma General para el Tratamiento de Datos Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado** 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-2026-00xx-M suscrito el xx de septiembre 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 Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado** 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 xx de septiembre del 2026 hasta el xx de octubre del 2026, inclusive, con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que, para cumplir con la resolución N° SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización de la **Norma General para el Tratamiento de Datos Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado** 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-2026-00xx suscrito el xx de xxxx 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-2026-0xxx-M** suscrito el **xx de xxx del 2026**, notificado al despacho el **xx de xxxx 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-2026-0xxx-M** del **xx de xxxxx del 2026**, el suscrito Superintendente de Protección de Datos Personales comunicó a la IRD las observaciones que realizó al proyecto; y, además, solicitó que aquellas sean revisadas de conformidad con el artículo 14 del Reglamento para la Creación, Modificación y derogatoria de la Normativa de la Superintendencia de Protección de Datos Personales;

Que mediante el memorando N° **SPDP-IRD-2026-[*]-M** del **[*] de [*] 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 Personales Relativos a la Salud y su Ciclo de Vida en los Sectores Público y Privado**, 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 PERSONALES RELATIVOS A LA SALUD Y SU CICLO DE VIDA EN LOS SECTORES PÚBLICO Y PRIVADO

TÍTULO I DISPOSICIONES GENERALES

Art 1.- La presente Norma tiene por objeto regular el tratamiento de datos personales relativos a la salud durante todo su ciclo de vida, de conformidad con la Constitución de la República (“CRE”), la Ley Orgánica de Protección de Datos Personales (RGLOPDP), su Reglamento General (“RGLOPDP”) y demás normativa aplicable. Su aplicación se realizará de manera complementaria con la Ley Orgánica de Salud y la normativa emitida por la Autoridad Sanitaria Nacional, en ejercicio de sus competencias de rectoría, regulación y control del Sistema Nacional de Salud.

La aplicación de esta Norma se realizará en concordancia con los estándares internacionales aplicables al tratamiento de datos personales relativos a la salud, así como, para las entidades del sector público y con el Esquema Gubernamental de Seguridad de la Información vigente.

Art 2.- Se sujetan a esta norma todas las personas naturales y jurídicas, nacionales o extranjeras, del sector público y privado, que realicen tratamiento de datos personales relativos a la salud en el territorio ecuatoriano o respecto de titulares residentes en el Ecuador, dentro del ámbito de aplicación material y territorial previstos en los artículos 2 y 3 de la LOPDP. Incluyendo, pero sin limitarse a:

- a) Las instituciones que conforman el Sistema Nacional de Salud;
- b) Los profesionales, tecnólogos, técnicos y auxiliares de la salud en ejercicio de sus funciones asistenciales, de investigación o docencia;

- c) Las compañías de salud prepagada y de asistencia médica;
- d) Las compañías de seguros que administren ramos de salud y vida;
- e) Los laboratorios clínicos, centros de imagenología y demás servicios de apoyo diagnóstico;
- f) Las entidades que desarrollen tecnologías de salud digital, telemedicina y telesalud;
- g) Las personas naturales y jurídicas que realicen investigación científica con datos de salud;
- h) Los proveedores de tecnologías neuronales relacionados con la salud mental y dispositivos de interfaz cerebro-computadora que traten datos neuronales que identifiquen o puedan hacer identificable a una persona;
- i) Farmacéuticas en el ejercicio de ensayos médicos y las demás actividades donde pueda haber tratamiento de datos personales de salud relacionados con productos de uso y consumo humano; y,
- j) Cualquier otra persona que realice tratamiento de datos relativos a la salud en el territorio nacional.

La presente Norma se aplicará sin perjuicio de las competencias de la Autoridad Sanitaria Nacional para establecer, mediante la normativa sectorial correspondiente, las condiciones, procedimientos y requisitos aplicables al tratamiento de información necesaria para el funcionamiento y cumplimiento de las finalidades del Sistema Nacional de Salud.

Art 3.- Para efectos de la presente norma, además de las definiciones contenidas en la LOPDP, su RGLOPDP y, por ser la SPDP parte de la Red Iberoamericana de Protección de Datos Personales, se establecen las siguientes:

3.1. Neurodatos: Datos personales obtenidos a partir de un tratamiento técnico específico (de manera directa, indirecta o inferida), en relación con las características anatómicas, fisiológicas, funcionales o conductuales de una persona física relativos a su actividad cerebral y de su sistema nervioso”.

3.2. Neuroderechos: Categoría de derechos humanos que busca garantizar la dignidad y los derechos fundamentales y libertades individuales en el marco de las neurotecnologías.

3.3. Protocolo técnico de anonimización: Documento que describe los métodos, técnicas y parámetros utilizados para impedir la identificación o reidentificación del titular de datos de salud.

3.4. Investigación secundaria con datos de salud: Uso de datos de salud previamente recolectados para una finalidad asistencial, que se destinan a una nueva finalidad de investigación científica.

3.5. Sistema de información de salud: Conjunto organizado de aplicaciones, infraestructura tecnológica, dispositivos, repositorios de datos, comunicaciones y

procedimientos utilizados para el tratamiento de datos personales relativos a la salud en la prestación, administración o gestión de servicios de salud.

3.6. Dispositivo de salud conectado: Equipo, sensor, dispositivo médico o sistema embebido que recolecte, genere, almacene, procese o transmita datos personales relativos a la salud y se comuniquen con otros dispositivos, aplicaciones, sistemas o redes.

3.7. Telesalud: Prestación de servicios de salud a distancia mediante tecnologías de la información y comunicación que implique el tratamiento de datos personales relativos a la salud.

3.8. ICS: Intendencia General de Control y Sanción

3.9. IIT: Intendencia General de Innovación Tecnológica

3.10. IRD: Intendencia General de Regulación de Protección de Datos Personales

Art 4.- Además de los principios establecidos en la LOPDP, el tratamiento de datos de salud observará las siguientes directrices específicas:

4.1. Interés superior del paciente: El tratamiento de datos de salud deberá orientarse en todo momento a la protección de la salud e integridad del titular;

4.2. Secreto profesional reforzado: Los profesionales de la salud, y todas las personas que intervengan en cualquier fase del tratamiento, estarán sujetos al principio de confidencialidad de manera complementaria al secreto profesional;

4.3. Minimización: Tratándose de datos de categoría especial, la minimización de datos deberá ser particularmente estricta y obligatoria, limitándose al mínimo indispensable para la finalidad específica del tratamiento;

4.4. Preferencia por la anonimización: Siempre que sea posible cumplir la finalidad del tratamiento con datos anonimizados, se preferirá la anonimización; cuando la finalidad exija conservar la posibilidad de reidentificación del titular, se aplicará la seudonimización, sin que ello exima bajo ningún concepto el cumplimiento íntegro de la LOPDP. El tratamiento con datos identificados procederá únicamente cuando ninguna de las modalidades anteriores permita alcanzar la finalidad.;

4.5. Integridad neurocognitiva: El tratamiento de neurodatos deberá respetar la integridad mental, la libertad cognitiva y la privacidad mental del titular, evitando cualquier forma de manipulación, discriminación o injerencia arbitraria basada en dichos datos.

TÍTULO II

DERECHOS DE LOS TITULARES EN EL SECTOR SALUD

Art. xx.- Sin perjuicio de los derechos reconocidos en la LOPDP y demás leyes y normas sectoriales, los titulares de datos de salud podrán ejercer sus derechos de conformidad con las disposiciones previstas en el ordenamiento jurídico vigente y la presente norma.

Art. xx.- Sin perjuicio de los demás contenidos, garantías y mecanismos previstos en la LOPDP y el RGLOPDP, el derecho a la información respecto del tratamiento de datos de salud comprenderá el derecho del titular a:

- a) Recibir información clara, accesible, precisa y comprensible sobre el tratamiento de sus datos de salud y su historia clínica, considerando en todo momento su nivel de comprensión y condición particular;
- b) Derecho a que se le comuniquen, en lenguaje claro y comprensible, quiénes tendrán acceso o han accedido a sus datos de salud y con qué finalidad;
- c) Conocer las finalidades específicas para las cuales serán tratados sus datos de salud, así como las consecuencias previsibles de dicho tratamiento;
- d) Ser informado, de manera previa a la obtención de su consentimiento cuando este constituya la base de legitimación aplicable o previo al inicio del tratamiento en los demás casos, sobre la utilización de tecnologías, sistemas automatizados, algoritmos y/o sistemas de inteligencia artificial que intervengan en el tratamiento de sus datos de salud; y,
- e) Conocer la existencia de inferencias, perfiles o predicciones tales como puntuaciones o recomendaciones automatizadas, etcétera, que puedan generarse a partir de sus datos de salud, cuando dichas operaciones produzcan efectos jurídicos o impactos significativos sobre su atención, acceso a servicios o condiciones de tratamiento.

Art. xx.- En ejercicio del derecho de acceso, a más de lo establecido en la LOPDP y el RGLOPDP, el titular tendrá derecho a:

- a) Obtener confirmación sobre si se están tratando o no datos de salud que le conciernen;
- b) Acceder a su historia clínica y demás registros que contengan datos de salud que le correspondan, en formatos accesibles, comprensibles y técnicamente disponibles;
- c) Conocer los accesos realizados a su información de salud cuando estos registros existan y deban mantenerse conforme con la normativa aplicable, incluyendo la identificación de la institución, del usuario o de la categoría de usuario que accedió a la información, la fecha y hora del acceso y la finalidad que lo justificó;
- d) Conocer los accesos realizados a su información de salud cuando estos registros existan y deban mantenerse conforme con la normativa aplicable, incluyendo la identificación de la institución o la categoría de usuario que accedió a la información y la finalidad que justificó dicho acceso.

Art. xx.- En ejercicio del derecho de oposición, a más de lo establecido en la LOPDP y el RGLOPDP, el titular podrá:

- a) Oponerse al tratamiento de sus datos de salud cuando concurren los supuestos previstos en la LOPDP;
- b) Solicitar restricciones específicas de acceso a determinada información de salud por parte de profesionales, unidades o establecimientos de salud o cualquiera de las personas naturales y jurídicas previstas en el artículo de esta normativa, siempre que ello no comprometa la adecuada prestación de los servicios

sanitarios, la seguridad del paciente o la atención de situaciones de emergencia vital;

- c) Oponerse al tratamiento de sus datos de salud con fines distintos de aquellos necesarios para la prestación de servicios de salud, cuando exista una base jurídica que habilite dicho ejercicio.

Las solicitudes de oposición o restricción previstas en este artículo no podrán impedir, limitar o retrasar el tratamiento que resulte necesario para la prestación de servicios de salud, la continuidad de la atención, la protección de la vida o integridad del titular o de terceros, la atención de emergencias, la vigilancia y control de la salud pública, el cumplimiento de obligaciones legales, el ejercicio de competencias de la Autoridad Sanitaria Nacional o cualquier otro tratamiento legítimo establecido en la normativa aplicable.

Los responsables y encargados del tratamiento deberán implementar mecanismos técnicos y organizativos que permitan gestionar las solicitudes de oposición, control o restricción de acceso, garantizando la trazabilidad de los accesos y evitando que dichas solicitudes generen barreras injustificadas para la atención sanitaria o el cumplimiento de las obligaciones legales y sanitarias

Art. xx.- En ejercicio del derecho a la portabilidad, a más de lo establecido en la LOPDP y el RGLOPDP, el titular podrá:

- a) Solicitar la transferencia o comunicación de sus datos de salud entre responsables del tratamiento, cuando ello sea técnicamente posible y proceda de conformidad con la LOPDP;
- b) Recibir sus datos de salud, contenidos o no en su historia clínica, en un formato estructurado, de uso común, y lectura clara que facilite su reutilización y transferencia o comunicación;
- c) Solicitar que la transferencia o comunicación de sus datos de salud se realice de forma segura, íntegra y sin alteraciones que comprometan su calidad o exactitud.

Art. xx.- Los titulares tendrán derecho a que sus datos de salud sean tratados exclusivamente para las finalidades para las cuales fueron recabados de manera explícita y legítima, salvo que se vaya a destinar a una nueva finalidad del tratamiento para la cual exista alguna de las bases de legitimación previstas en la LOPDP que habiliten un tratamiento posterior compatible. En este caso, previo a realizar el tratamiento de datos personales de salud, el responsable del tratamiento deberá cumplir con el deber de informar al titular de datos personales, así como legitimar de manera adecuada el tratamiento a efectuarse.

Art. xx.- El tratamiento de datos personales relativos a la salud de niñas, niños y adolescentes se regirá por el principio de interés superior y por lo dispuesto en la LOPDP y en el RGLOPDP.

La información dirigida a niñas, niños y adolescentes se proporcionará en lenguaje adaptado a su edad y grado de madurez.

Art. xx.- El acceso a los datos personales relativos a la salud de personas fallecidas se regirá por el artículo 27 de la LOPDP y por el artículo 17 del RGLOPDP, cuando la información solicitada contenga datos relevantes de salud que puedan comprometer el estado de los familiares consanguíneos sobre la voluntad manifestada en vida del causante.

TÍTULO III

BASES DE LICITUD PARA EL TRATAMIENTO DE DATOS DE SALUD

CAPÍTULO I

DEL CONSENTIMIENTO

Art xx.- Para el tratamiento de datos relativos a la salud se requerirá el consentimiento previo y explícito del titular, salvo en los casos de excepción previstos en el artículo 31 de la LOPDP. El consentimiento deberá ser libre, específico, informado e inequívoco, y deberá constar la especificación clara de las finalidades del tratamiento.

Art xx.- El consentimiento para el tratamiento de datos de salud deberá cumplir, además de los requisitos generales establecidos de la Ley, los siguientes:

- 6.1.** Ser diferenciado del consentimiento para la intervención médica, quirúrgica, ensayo clínico o de cualquier otra actividad o procedimiento médico;
- 6.2.** Especificar las categorías de datos que se tratarán;
- 6.3** Identificar los posibles destinatarios o categorías de destinatarios de los datos;
- 6.4.** Informar sobre la posibilidad de transferencia nacional o internacional de los datos;
- 6.5.** Ser renovado cuando exista un cambio sustancial en la finalidad del tratamiento;
- 6.6.** Para el tratamiento de datos personales relativos a la salud con fines de investigación, docencia o fines estadísticos se realizará de conformidad con la LOPDP y la normativa sanitaria vigente, priorizando el uso de datos anonimizados o disociados. Se prohíbe la transferencia de datos personales con otros fines distintos para los que fueron recolectados.
- 6.7.** Constar en soporte que permita acreditar su otorgamiento, la fecha, la identidad del titular o titulares y el contenido de la información suministrada; y,
- 6.8.** Ser recabado en condiciones que garanticen su libertad, sin que pueda obtenerse durante la sedación, la anestesia, la urgencia médica o cualquier otra situación que menoscabe la capacidad de decisión del titular, salvo que la propia situación configure un supuesto de exención.

Art xx.- No se requerirá el consentimiento del titular para el tratamiento de datos de salud en los siguientes supuestos, de conformidad con la Ley:

7.1. Cuando sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento;

7.2. Cuando sea necesario para fines de medicina preventiva, laboral u ocupacional, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social;

7.3. Cuando sea necesario por razones de interés público esencial en el ámbito de la salud pública, siendo proporcional al objetivo perseguido y estableciendo medidas de seguridad adecuadas y específicas para proteger los derechos del titular;

7.4. Cuando sea necesario por razones de interés público en el ámbito de la salud pública, como amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios;

7.5. Cuando se pretenda el uso de datos para investigación científica, siempre que se encuentren debidamente anonimizados de acuerdo con el proceso establecido en la presente norma.

En todos los casos de excepción, se deberán establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular, incluyendo especialmente el secreto profesional. Y, en caso de duda en los tratamientos se deberá aplicar el principio en pro del titular de datos personales.

Art. xx.- El titular podrá retirar o revocar en cualquier momento el consentimiento otorgado para el tratamiento de sus datos personales relativos a la salud, sin que ello afecte la licitud del tratamiento realizado con anterioridad. La revocatoria no impedirá la conservación o el tratamiento de los datos cuando exista otra base de legitimación prevista en la LOPDP que lo permita o cuando sea necesario para el cumplimiento de obligaciones legales, la continuidad de la atención sanitaria, la defensa de reclamaciones o la protección de intereses vitales.

CAPÍTULO II

DE LAS BASES DE LEGITIMACIÓN EN EL ÁMBITO ASEGURADOR

Art xx.- Las compañías de seguros y reaseguros que administren ramos de salud y vida, los asesores productores de seguros, intermediarios en colocación de seguros (*brokers*), así como las compañías de salud de medicina prepagada y de asistencia médica, podrán tratar datos personales de salud de sus solicitantes, potenciales asegurados, asegurados, afiliados, beneficiarios o cualquier otra persona cuyos datos resulten necesarios dentro de los procesos precontractuales o contractuales propios de dichas actividades, únicamente cuando cumplan con lo siguiente:

8.1. El tratamiento cuente con el consentimiento previo y explícito del titular en los términos del artículo 26 de la LOPDP, o con otra base de legitimación de las previstas en dicho artículo;

8.2. Los datos se limiten estrictamente a los necesarios para la solicitud y elaboración de cotizaciones, la evaluación, calificación, selección o gestión del riesgo, la determinación de primas y condiciones de aseguramiento, la suscripción del contrato o póliza, gestión de siniestros, prestación de servicios médicos o el cumplimiento de obligaciones derivadas de la póliza o contrato, según corresponda;

8.3. Se informe al titular de manera previa, clara, accesible y comprensible sobre el tratamiento, conforme con los requisitos del artículo 12 de la LOPDP; y,

8.4. Se usen los datos personales solicitados estrictamente para las finalidades para las cuales fueron recabadas y para las que fueron informadas, quedando prohibida cualquier otra finalidad distinta al del ámbito de tratamiento.

8.5. Se implementen medidas de seguridad reforzadas, acordes al nivel de riesgo de los datos objeto del tratamiento.

Art xx.- Se prohíbe a las compañías de seguros y reaseguros, medicina prepagada y asistencia médica:

9.1. El uso de datos genéticos o neurodatos con la finalidad de determinar primas, establecer exclusiones, imponer restricciones de cobertura, rechazar solicitudes de aseguramiento o adoptar condiciones contractuales desfavorables, aun cuando el titular hubiere otorgado su consentimiento para dicho tratamiento. Esta prohibición tendrá carácter de orden público y no podrá ser exceptuada ni dejada sin efecto mediante consentimiento, autorización o acuerdo contractual;

9.2. La elaboración de perfiles basados en datos de salud que resulten en discriminación para el acceso, la fijación de primas o el establecimiento de condiciones contractuales más graves en servicios de salud o seguros, sin que puedan adoptarse decisiones basadas únicamente en tratamiento automatizado sin intervención humana significativa;

9.3. Mantener en los perfiles realizados, donde consten preexistencias a enfermedades sobre las cuales una persona no ha tenido una recaída desde hace 5 años continuos;

9.4. La comunicación de datos de salud a terceros no vinculados al objeto del contrato sin consentimiento explícito del titular, salvo cuando exista mandato legal expreso, incluidos los reportes obligatorios al ente rector de salud para fines de vigilancia epidemiológica, salud pública o emergencia sanitaria, los cuales no requerirán dicho consentimiento;

9.5. La conservación de datos de salud por plazos superiores a los estrictamente necesarios conforme con la normativa sectorial aplicable; y,

9.6. La cesión onerosa o gratuita de bases de datos, sin contar con el consentimiento previo, expreso e independiente por parte de cada uno de los titulares de datos personales donde se demuestre que el mismo fue otorgado de manera libre, específico, informado, e inequívoco.

9.7. Exigir la realización de pruebas genéticas o predictivas como condición para la suscripción, renovación o modificación del contrato.

Art. xx.- Los asesores productores de seguros, intermediarios, compañías de seguros y reaseguros, empresas de medicina prepagada y de asistencia médica deberán garantizar el derecho de eliminación respecto de los perfilamientos efectuados con base en datos personales relativos a la salud de los titulares.

En consecuencia, no podrán conservar, utilizar, reutilizar, comunicar o incorporar en procesos de análisis de riesgo, segmentación, perfilamiento, cotización, suscripción, renovación o modificación contractual, información relacionada con enfermedades, patologías, condiciones médicas o antecedentes clínicos respecto de los cuales el titular no haya presentado recaídas, complicaciones o manifestaciones activas durante un período continuo de cinco (5) años contados desde la finalización del tratamiento o la estabilización de su condición médica.

Cuando la enfermedad o condición médica hubiere sido diagnosticada antes de los dieciocho (18) años, el plazo aplicable será de tres (3) años desde la finalización del tratamiento o la estabilización de la condición médica, siempre que no exista recaída posterior.

Cumplidos los plazos previstos en los incisos anteriores, los responsables y los encargados del tratamiento deberán eliminar o anonimizar los datos utilizados para perfilamientos vinculados a antecedentes de salud. En ningún caso dicha información podrá ser utilizada para establecer exclusiones, restricciones, condiciones más onerosas, incrementos desproporcionados, decisiones automatizadas discriminatorias o limitaciones en el acceso a productos o servicios aseguradores o de medicina prepagada.

El titular podrá ejercer en cualquier momento los derechos de eliminación, oposición y suspensión del tratamiento respecto de perfilamientos realizados sobre datos relativos a su salud, de conformidad con la LOPDP, el RGLOPDP y la presente norma.

TÍTULO IV CICLO DE VIDA DE LOS DATOS DE SALUD

CAPÍTULO I RECOLECCIÓN

Art xx.- La recolección y tratamiento de datos personales relativos a la salud se sujetarán a los principios y demás disposiciones establecidas en la LOPDP y a la normativa emitida por la Autoridad Sanitaria Nacional, en el ámbito de sus competencias. Los responsables del tratamiento deberán documentar la base de legitimación que sustenta la recolección y asegurar que los datos recolectados sean adecuados, pertinentes y no excesivos en relación con la finalidad declarada.

Art xx.- Los responsables que recolecten datos personales de salud en el marco de la atención sanitaria deberán:

- 11.1. Registrar los datos conforme a los formularios de la historia clínica única y demás instrumentos aprobados por la Autoridad Sanitaria Nacional, sin que la urgencia o gravedad de la atención pueda limitarse por consideraciones de protección de datos cuando esté en riesgo la vida o integridad del paciente;

11.2. Garantizar que la recolección sea simultánea a la atención siempre que sea posible;

11.3 Informar al paciente, en lenguaje claro y comprensible, la finalidad del tratamiento y sus derechos sobre los datos, en la medida en que las condiciones clínicas lo permitan;

11.4. Reutilizar los datos registrados en la historia clínica para fines secundarios, investigación, docencia o estadística únicamente cuando dicha reutilización sea compatible con la finalidad original, se sustente en las bases de legitimación de la LOPDP y, tratándose de fines de interés público en salud, se ajuste a los lineamientos que emita la Autoridad Sanitaria Nacional, aplicando anonimización o seudonimización cuando sea posible;

11.5. Registrar los datos observando los estándares de identificación unívoca del paciente y las terminologías clínicas adoptadas por la Autoridad Sanitaria Nacional, de modo que se garantice la exactitud, integridad y trazabilidad de la información clínica; y,

11.6. Abstenerse de condicionar la prestación del servicio de salud al otorgamiento de consentimientos para finalidades distintas de la atención sanitaria.

Art xx.- El tratamiento de datos personales mediante plataformas de telesalud o telemedicina deberá garantizar, además de las medidas previstas en el capítulo de seguridad de la presente Norma:

- a) La verificación adecuada de la identidad del profesional de la salud y del paciente;
- b) La confidencialidad e integridad de las comunicaciones, así como la protección de los datos durante su transmisión y almacenamiento;
- c) La autenticación y autorización de los participantes y el registro de los consentimientos que resulten legalmente exigibles;
- d) La incorporación íntegra y segura de la información pertinente a la historia clínica y el registro de los accesos y operaciones relevantes;
- e) La continuidad de la atención ante fallos tecnológicos y la adopción de procedimientos para situaciones de emergencia; y,
- f) El cumplimiento de los estándares de interoperabilidad establecidos por la Autoridad Sanitaria Nacional.

Las grabaciones o transcripciones solo podrán realizarse cuando sean necesarias para una finalidad legítima, exista una base de legitimación aplicable y el titular haya sido informado de manera previa y haya dado su consentimiento.

La utilización de plataformas de telesalud o telemedicina que impliquen la transferencia internacional de datos personales relativos a la salud, incluidas las que operen mediante servicios de computación en la nube ubicados fuera del territorio nacional, se sujetará al Capítulo IV del presente Título y la LOPDP, RGLOPDP y normativa secundaria emitida por la SPDP en lo que respecta a transferencias internacionales. En ningún caso se emplearán, para la comunicación de datos clínicos, servicios de mensajería o videoconferencia de uso general que no garanticen cifrado en tránsito y reposo, control de acceso y trazabilidad, salvo situaciones de emergencia debidamente documentadas.

CAPÍTULO II

ALMACENAMIENTO Y CONSERVACIÓN

Art xx.- Los datos personales de salud se conservarán por los plazos establecidos en la normativa sectorial aplicable. A falta de norma específica, se observarán los siguientes plazos mínimos:

13.1. Historia clínica: conforme con lo establecido por la Autoridad Sanitaria Nacional para el archivo activo y pasivo;

13.2. Datos para fines de seguros: por el plazo de vigencia del contrato y un período adicional conforme con la normativa del sector financiero y de seguros;

Vencidos los plazos de conservación, el responsable deberá proceder con la eliminación segura, bloqueo o anonimización de los datos según corresponda.

Art xx.- El almacenamiento de datos de salud se sujetará a las medidas mínimas y reforzadas previstas en el capítulo de seguridad de la presente Norma, en coordinación y sin duplicidad con el Esquema Gubernamental de Seguridad de la Información y con los lineamientos técnicos que emita la Autoridad Sanitaria Nacional para los sistemas del Sistema Nacional de Salud.

El responsable garantizará, en particular:

- a) Protección criptográfica de los datos y sus respaldos;
- b) Control de accesos basado en roles y perfiles, que asegure la disponibilidad inmediata de la información al personal de salud en el momento de la atención, incluida la atención de urgencia o emergencia;
- c) Registro de modificaciones y trazabilidad de accesos;
- d) Recuperación segura de la información; y,
- e) Separación lógica de los datos identificativos respecto de la información clínica, únicamente cuando dicha separación sea compatible con los estándares de interoperabilidad y con los tiempos de acceso que exija la continuidad de la atención en salud, conforme a los lineamientos que para tal efecto emita la Autoridad Sanitaria Nacional.

Los plazos de conservación son mínimos y garantizan la continuidad asistencial, la seguridad del paciente y el derecho de acceso del titular. Vencidos estos, la conservación ulterior procederá solo mientras subsista una finalidad legítima, sin exceder el plazo máximo que la Autoridad Sanitaria Nacional determine por categoría, con acompañamiento técnico de la SPDP limitado a verificar su compatibilidad con la LOPDP.

CAPÍTULO III

USO Y TRATAMIENTO

Art xx.- Los datos de salud recolectados para una finalidad determinada no podrán ser tratados posteriormente para fines distintos, salvo que:

15.1. El titular otorgue su consentimiento explícito para la nueva finalidad del tratamiento;

15.2. El tratamiento ulterior sea compatible con la finalidad inicial, de conformidad con los criterios de la Ley;

15.3. Se trate de un supuesto de excepción previsto en la Ley; o,

15.4. Los datos hayan sido debidamente anonimizados.

Art xx.- La elaboración de perfiles basada en datos de salud estará sujeta a las siguientes condiciones:

xx.1. Deberá contar con una base de legitimación prevista en la LOPDP;

xx.2. Se prohíbe la toma de decisiones automatizadas que produzcan efectos jurídicos o afecten directamente a los derechos y libertades del titular cuando se basen exclusivamente en datos de salud, con excepción de la utilización de herramientas de triage o priorización asistida por algoritmos deberá estar sujeta al criterio claro de intervención humana efectiva y, demás que se encuentren previstas en la Ley;

xx.3. El titular deberá ser informado sobre la existencia de elaboración de perfiles y sus consecuencias; y,

xx.4. Se garantizará el derecho del titular a solicitar intervención humana, expresar su punto de vista y, a impugnar la decisión.

CAPÍTULO IV COMUNICACIÓN Y TRANSFERENCIA

Art xx.- La comunicación de datos de salud entre prestadores de servicios del Sistema Nacional de Salud será lícita cuando:

xx.1. Sea necesaria para la continuidad de la atención del paciente, en el marco del sistema de referencia y contrarreferencia, incluyendo la derivación, transferencia, interconsulta o retorno del paciente entre niveles de atención, establecimientos o especialidades, sin que la finalidad asistencial pueda verse retrasada o condicionada por trámites ajenos a la urgencia o gravedad del caso;

xx.2. Se realice a través de los mecanismos de interoperabilidad establecidos por la Autoridad Sanitaria Nacional, obligación aplicable a todos los prestadores del Sistema Nacional de Salud, sean públicos o privados, sin que la naturaleza jurídica del prestador exima del uso de dichos mecanismos ni habilite el uso de canales alternativos no autorizados por el ente rector;

xx.3. Se limite a los datos estrictamente necesarios para la finalidad de la comunicación, conforme al motivo de la referencia, interconsulta o derivación, y a los campos que para tal efecto determinen los formularios o protocolos de referencia y contrarreferencia aprobados por la Autoridad Sanitaria Nacional, evitando la transmisión de información clínica no relacionada con dicho motivo, salvo que resulte necesaria para la seguridad del paciente, tal como antecedentes de alergias, medicación en curso o condiciones clínicas que puedan afectar la atención;

xx.4. Se garantice la trazabilidad de la comunicación, mediante el registro de la fecha, el emisor, el receptor, los datos transmitidos y la finalidad de cada comunicación, de forma que sea posible auditar posteriormente el flujo de información entre prestadores;

xx.5. Se establezcan las medidas de seguridad más altas para los datos en tránsito, incluyendo cifrado extremo a extremo, autenticación de los prestadores emisor y receptor, y control de integridad de la información transmitida, conforme al capítulo de seguridad de la presente Norma y a los lineamientos técnicos que emita la Autoridad Sanitaria Nacional; y,

xx.6. Se cuente con una base de legitimación conforme a la LOPDP, el RGLOPDP y la normativa específica de transferencias, la cual se entenderá cumplida cuando la comunicación se efectúe en el marco de protocolos de referencia y contrarreferencia u otros mecanismos de interoperabilidad definidos por la Autoridad Sanitaria Nacional en ejercicio de su rectoría, sin que se requiera consentimiento adicional del titular cuando dicha comunicación resulte necesaria para su atención.

Art xx.- La transferencia internacional de datos de salud se sujetará a lo previsto en la LOPDP y su RGLOPDP y la resolución de la SPDP correspondiente, con las siguientes condiciones adicionales:

xx.1. Se deberá informar al titular de las finalidades de la transferencia o comunicación y su destinatario.

xx.2. Se requerirá evaluación de impacto en protección de datos en todos los casos en los que se vayan a transferir datos de salud;

xx.3. El instrumento jurídico que sustente la transferencia o comunicación deberá contener cláusulas específicas sobre confidencialidad médica y secreto profesional; y,

xx.4. Se informará al titular sobre los posibles riesgos y vulnerabilidades específicas derivadas de la transferencia internacional de sus datos de salud.

CAPÍTULO V

ELIMINACIÓN Y ANONIMIZACIÓN

Art xx.- La eliminación de datos de salud deberá realizarse mediante procedimientos que garanticen que no podrán ser recuperados. El responsable del tratamiento deberá documentar los procedimientos de eliminación segura y conservará evidencia del cumplimiento de esta obligación.

Art xx.- Se entenderá por anonimización el proceso irreversible mediante el cual los datos de salud dejan de estar vinculados o ser vinculables, directa o indirectamente, a su titular, conforme a la definición establecida en la Ley Orgánica de Protección de Datos Personales. Los responsables que pretendan anonimizar datos de salud deberán observar lo siguiente:

- a) Se efectuará mediante técnicas, metodologías, estándares y buenas prácticas nacionales o internacionales reconocidas, que, conforme al estado de la técnica,

- reduzcan el riesgo de reidentificación a un nivel que no resulte razonablemente atribuible al titular. Podrán emplearse, entre otras, técnicas de generalización, supresión, agregación, perturbación, k-anonimato y privacidad diferencial.
- b) Diferenciar expresamente los procesos de anonimización de los de seudonimización, dado que únicamente los datos efectivamente anonimizados quedan fuera del ámbito de aplicación de la normativa de protección de datos personales;
 - c) Considerar los riesgos de reidentificación derivados de la singularidad inherente a determinados datos de salud;
 - d) Documentar el proceso de anonimización en un protocolo técnico, validado por la unidad o responsable de seguridad de la información y protección de datos de la institución;
 - e) Realizar evaluaciones periódicas del riesgo de reidentificación, con una periodicidad mínima anual o cuando se modifique la finalidad de uso del conjunto de datos o se identifiquen nuevas técnicas de reidentificación; y,
 - f) Suspender el tratamiento del conjunto de datos como anónimo y aplicar las obligaciones correspondientes a datos personales, en caso de que la evaluación periódica determine un riesgo real de reidentificación.

TÍTULO V

DE LA AUTORIZACIÓN PARA TRATAMIENTO DE DATOS DE SALUD ANONIMIZADOS Y NO ANONIMIZADOS

CAPÍTULO I

PROCEDIMIENTO DE AUTORIZACIÓN DE ANONIMIZACIÓN

Art xx.- De conformidad con el numeral 3 del artículo 31 de la LOPDP, todo tratamiento de datos personales de salud que se busque realizar de manera anonimizada deberá ser autorizado previamente por esta autoridad. Para obtener la autorización, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos, las directrices establecidas en la normativa de anonimización, y el informe previo favorable emitido por la Autoridad Sanitaria Nacional.

Art. xx.- El informe previo favorable emitido por la Autoridad Sanitaria Nacional constituirá un requisito habilitante para la autorización prevista en el presente Capítulo.

El informe deberá contener, al menos:

- a) La identificación de la finalidad sanitaria que motiva el tratamiento de los datos personales de salud anonimizados.
- b) Los datos personales relativos a la salud que serán objeto del proceso de anonimización.
- c) La identificación de la entidad responsable del tratamiento y, cuando corresponda, de las demás entidades que participarán en el tratamiento.
- d) Recomendación técnica sobre la idoneidad de las medidas propuestas para preservar la utilidad sanitaria de los datos y su compatibilidad con la finalidad del tratamiento.
- e) El pronunciamiento sobre la conformidad del tratamiento con la normativa sanitaria aplicable.
- f) Conclusiones que motiven la condición de favorable del informe.

- g) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

La evaluación de la suficiencia de las técnicas de anonimización, del riesgo de reidentificación y del cumplimiento de la LOPDP corresponderá exclusivamente a la SPDP.

El informe previo favorable emitido por la Autoridad Sanitaria Nacional será habilitante para la presentación de la solicitud ante la SPDP.

Art xx. - La solicitud de autorización se presentará ante la SPDP a través de su portal institucional con firma electrónica válida y, de manera excepcional a través de ventanilla física de la institución. La solicitud deberá contener al menos lo siguiente:

- a) Identificación completa del solicitante (responsable del tratamiento);
- b) Declaración juramentada de obtención legítima de los datos personales;
- c) Descripción detallada de la finalidad para la cual se busca destinar los datos personales de salud anonimizados;
- d) Datos de salud objeto de anonimización;
- e) Volumen estimado de datos personales anonimizados;
- f) Protocolo técnico de anonimización;
- g) Informe previo favorable de la Autoridad Sanitaria Nacional;
- h) Análisis de riesgos en protección de datos personales;
- i) Evaluación de impacto del tratamiento, cuando corresponda;
- j) Plazo estimado de tratamiento y destino final de los datos; y,
- k) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

Art xx.- El contenido del Protocolo Técnico De Anonimización (“PTA”) deberá contener al menos lo siguiente:

- a) Descripción de las técnicas aplicadas para la anonimización;
- b) Evaluación de riesgo de reidentificación;
- c) Medidas para mitigar el riesgo residual;
- d) Mecanismos de verificación de la efectividad de la anonimización; y,
- e) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

Art xx.- El procedimiento para la autorización del proceso de anonimización de datos personales de salud se sujetará a las siguientes reglas:

1. La solicitud se presentará a través del portal institucional con firma electrónica válida y, de manera excepcional por medios físicos en la ventanilla de las instalaciones de la SPDP;
2. Recibida la solicitud, la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales (“IIT”) verificará el cumplimiento de los requisitos en el término de cinco (5) días. De encontrarse incompleta, se requerirá al solicitante la subsanación en el término de diez (10) días;
3. Una vez aceptado a trámite la solicitud, la IIT verificará el contenido del PTA y elaborará un informe sobre la idoneidad del protocolo de anonimización, el cual en caso de ser favorable deberá ser comunicado al Superintendente de Protección

de Datos Personales o su delegado, en el término de treinta (30) días, para su aprobación;

4. En caso de que informe de IIT identifique que el PTA no es idóneo para las finalidades a las cuales se busca alcanzar o que las medidas y procesos establecidos no son los adecuados o suficientes, la IIT devolverá al solicitante para que este adecúe el protocolo correspondiente de acuerdo con los parámetros indicados por la IIT. Para dicho efecto, la IIT establecerá el término necesario acorde a las medidas específicas que se deban incluir, modificar o subsanar.

Una vez que el solicitante reingrese el protocolo técnico adaptado, el proceso volverá a la etapa mencionada en el numeral 3 del presente artículo; sin embargo, si es que no se ha cumplido en debida manera con lo señalado, la IIT deberá archivar la solicitud justificándolo motivadamente, sin perjuicio de que se pueda a volver a ingresar la solicitud después del término de 30 días.

5. En caso de haber un informe favorable por parte de la IIT, este deberá ser puesto en conocimiento por el Superintendente de Protección de Datos Personales o su delegado, quien lo aprobará o no en un término no mayor de diez (10) días dentro de los cuales se emitirá la resolución de autorización de anonimización.

En caso de que el Superintendente de Protección de Datos Personales o su delegado emita observaciones al informe de idoneidad, dentro del término de diez (10) días antes señalado, se devolverá lo actuado a la IIT, y el proceso volverá a la etapa descrita en el numeral 3 del presente artículo.

6. La resolución de autorización podrá ser revocada si se verifica el incumplimiento del protocolo.

CAPÍTULO II

PROCEDIMIENTO DE AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES DE SALUD NO ANONIMIZADOS

Art xx.- De conformidad con el artículo 32 de la LOPDP, los datos relativos a la salud que consten en las instituciones del Sistema Nacional de Salud podrán ser tratados con fines de investigación científica, siempre que cuenten con uno de los siguientes dos procesos establecidos en la norma:

1. Se encuentre debidamente anonimizados de conformidad con el procedimiento establecido en la presente norma para su anonimización y, con la debida autorización de la SPDP; o,
2. Se solicite autorización a la SPDP para realizar tratamiento de datos personales de salud sin anonimización.

Art. xx.- El informe previo de autorización emitido por la Autoridad Sanitaria Nacional constituirá un requisito habilitante para la autorización de la SPDP prevista en el presente Capítulo.

El informe deberá contener, al menos:

- a) La identificación de la finalidad sanitaria que motiva el tratamiento de los datos personales anonimizados.

- b) Los datos personales relativos a la salud que serán objeto del proceso de anonimización.
- c) La identificación de la entidad responsable del tratamiento y, cuando corresponda, de las demás entidades que participarán en el tratamiento.
- d) Recomendación técnica sobre la idoneidad de las medidas de seguridad propuestas para preservar la utilidad sanitaria de los datos y su compatibilidad con la finalidad del tratamiento.
- e) El pronunciamiento sobre la conformidad del tratamiento con la normativa sanitaria aplicable.
- f) Conclusiones que motiven la condición de favorable del informe.
- g) Idoneidad del tratamiento, y la proporcionalidad del mismo para el cumplimiento de los fines que se buscan alcanzar.
- h) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

La evaluación de la suficiencia de las medidas técnicas y del cumplimiento de la LOPDP corresponderá exclusivamente a la SPDP.

El informe previo favorable emitido por la Autoridad Sanitaria Nacional será habilitante para la presentación de la solicitud ante la SPDP.

Art xx. - La solicitud de autorización para tratar datos personales de salud sin anonimización se presentará ante la SPDP a través de su portal institucional, con firma electrónica válida y, de manera excepcional a través de ventanilla física de la institución.

La solicitud deberá contener, al menos, los siguientes requisitos:

- a) Identificación completa del solicitante (responsable del tratamiento);
- b) Identificación completa de todos los intervinientes en la investigación, esto incluye, pero no limita a, datos de contacto principales y secundarios de:
 - a. Teléfonos móviles
 - b. Teléfonos fijos
 - c. Correo electrónico
 - d. Dirección física
- c) El protocolo de investigación aprobado por un Comité de Ética de Investigación en Seres Humanos debidamente registrado;
- d) Identificación de los tipos de datos de salud;
- e) Identificación de transferencias o comunicaciones internacionales de los datos personales de salud cuando sea pertinente para el objeto de la investigación. En caso de existir transferencias o comunicaciones se deberá identificar cual es el proceso de legitimación de transferencias o comunicaciones que se aplicará de acuerdo con la resolución correspondiente;
- f) Consentimiento de todos los titulares de datos personales que vayan a ser objeto de la investigación;
- g) Finalidades de tratamiento de la investigación;
- h) Justificación de por qué no es posible cumplir la finalidad investigativa exclusivamente con datos anonimizados;
- i) El análisis de riesgos en protección de datos personales;
- j) Las medidas de seudonimización que se aplicarán;
- k) Protocolo técnico de parámetros de protección de datos personales;

- l) Informe previo autorizado de la Autoridad Sanitaria Nacional;
- m) Evaluación de impacto en protección de datos del tratamiento a ejecutar;
- n) Plazo de conservación y destino final de los datos; y,
- o) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

Art xx.- El contenido del Protocolo Técnico de Parámetros de Protección de Datos Personales (“PTP”) deberá contener, al menos, lo siguiente:

- a) Descripción y detalle de las medidas de seguridad implementadas para los datos personales en almacenamiento y en tránsito;
- b) Análisis de riesgos;
- c) Evaluación de impacto;
- d) Mecanismos de verificación de la efectividad de las medidas de seguridad implementadas; y,
- e) Plan de verificación continua de seguridad.
- f) Cualquier otra información de cualquier naturaleza o cualquier otro documento que se considere necesaria o de relevancia para la SPDP.

Art xx.- El procedimiento para autorizar el tratamiento de datos personales de salud sin anonimización se sujetará a las siguientes reglas:

1. La solicitud se presentará principalmente a través del portal institucional con firma electrónica válida y, de manera excepcional por medios físicos en la ventanilla de las instalaciones de la SPDP;
2. Recibida la solicitud, la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales (“IIT”) verificará el cumplimiento de los requisitos en el término de cinco (5) días. De encontrarse incompleta, se requerirá al solicitante la subsanación en el término de diez (10) días;
3. Una vez aceptado a trámite la solicitud, la IIT verificará el contenido del PTP y elaborará un informe sobre la idoneidad del protocolo, el cual en caso de ser favorable deberá ser comunicado al Superintendente de Protección de Datos Personales o su delegado, en el término no mayor de treinta (30) días, para su aprobación;
4. En caso de que informe de IIT identifique que el PTP no es idóneo para las finalidades a las cuales se busca alcanzar o que las medidas y procesos establecidos no son los adecuados o suficientes, la IIT devolverá al solicitante el requerimiento para que este adecúe el protocolo correspondiente, de acuerdo con los parámetros indicados por la IIT, para lo cual la IIT establecerá el termino necesario acorde a las medidas específicas que se deban incluir, modificar o subsanar.

Una vez que el solicitante reingrese el protocolo técnico adaptado o corregido, el proceso volverá a la etapa establecida en el numeral 3 del presente artículo; sin embargo, si es que el solicitante no ha cumplido en debida manera con lo requerido, la IIT deberá archivar la solicitud justificando motivadamente tal decisión, sin perjuicio de que se pueda a volver a ingresar la solicitud después del término de 30 días.

5. En caso de haber un informe favorable por parte de la IIT, este deberá ser notificado al Superintendente de Protección de Datos Personales o su delegado y,

quien aprobará o negará en un término no mayor de diez (10) días, dentro de los cuales se emitirá la resolución respectiva.

En caso de que el Superintendente de Protección de Datos Personales o su delegado emita observaciones al informe de idoneidad, dentro del término de diez (10) días deberá devolver a la IIT el expediente, y el proceso volverá a la etapa descrita en el numeral 3 del presente artículo.

6. La resolución de autorización será revocable si se verifica el incumplimiento de las condiciones bajo las cuales fue otorgada.

TÍTULO VI NEURODATOS

CAPÍTULO I PROTECCIÓN DE NEURODERECHOS

Art xx. La presente norma reconoce y protege los neuroderechos como una dimensión del derecho a la protección de datos personales, específicamente los de salud, en concordancia con los numerales 3 y 19 del artículo 66 de la Constitución de la República, la protección reforzada que la LOPDP otorga a los datos sensibles y datos relativos a la salud y, en concordancia con el reconocimiento que se les da a los mismos en la Red Iberoamericana de Protección de Datos Personales. El alcance de la privacidad de los neurodatos comprende el siguiente alcance a la luz de los principios y derechos reconocidos en la LOPDP:

- a) Privacidad mental: El derecho de toda persona a que sus datos neuronales no sean accedidos, recolectados o utilizados sin su consentimiento explícito e informado de acuerdo con el artículo 31 de la LOPDP;
- b) Integridad mental: El derecho a no ser sometido a manipulación neurocognitiva mediante neurotecnología, preservando la autonomía del pensamiento, al amparo de derecho de información y de la obligación de solicitar el consentimiento libre, específico, informado e inequívoco;
- c) Identidad personal neurocognitiva: El derecho a que el uso de neurotecnología no altere de manera no consentida el sentido de identidad de la persona; y
- d) No discriminación neurocognitiva: El titular de datos personales tiene derecho a no ser discriminado con base en datos obtenidos del registro o análisis de la actividad cerebral.

Art xx.- Los neurodatos se consideran datos personales relativos a la salud y, datos sensibles, por lo que, su tratamiento estará sujeto a las mayores garantías previstas en la LOPDP, además de las disposiciones específicas de la presente Norma.

Art xx.- El consentimiento para el tratamiento de neurodatos, además de lo establecido en el artículo 8 de la LOPDP, deberá verificar lo siguiente:

- a) Explícito y por escrito o por medio electrónico verificable;
- b) Granular, permitiendo al titular distinguir entre las diversas finalidades del tratamiento;
- c) Informado con particular detalle sobre los tipos de inferencias que pueden realizarse a partir de los datos cerebrales;

- d) Revocable en cualquier momento con efectos inmediatos sobre la continuidad de la recolección; y,
- e) Renovable periódicamente, con un máximo de vigencia de un (1) año cuando se trate de tratamientos continuos.

Art xx.- Se prohíbe el tratamiento de neurodatos en los siguientes casos:

- a) Para fines de vigilancia, control conductual o manipulación del pensamiento;
- b) La comercialización de neurodatos identificativos sin consentimiento explícito y renovable del titular;
- c) La utilización de neurodatos para elaboración de perfiles con fines discriminatorios;
- d) El uso de neurodatos para actividades de mercadotecnia directa;
- e) El uso de neurotecnología invasiva para recolección de datos sin consentimiento explícito o sin supervisión de un profesional de la salud; y,
- f) La transferencia internacional de neurodatos identificados se sujetará al régimen de transferencia o comunicaciones internacionales previsto en los artículos 55 a 60 de la LOPDP, su RGLOPDP y la resolución de la SPDP correspondiente, debiendo el responsable garantizar la protección de los neuroderechos del titular.

CAPÍTULO II

OBLIGACIONES DE LOS RESPONSABLES DEL TRATAMIENTO QUE TRATEN NEURODATOS

Art xx. Todo tratamiento de neurodatos requerirá una evaluación de impacto previa en forma obligatoria, conforme con lo previsto en el artículo 42 de la LOPDP, la cual deberá incluir una sección específica sobre los riesgos para los neuroderechos del titular.

Art xx.- Los responsables del tratamiento que traten o traten neurodatos, deberán cumplir con las siguientes obligaciones a más de las ya establecidas en la LOPDP y el RGLOPDP y demás normativa secundaria expedida por la SPDP:

- a) Implementar medidas criptográficas y controles de acceso reforzados, apropiados a la sensibilidad, finalidad, contexto del tratamiento y estado de la técnica;
- b) Establecer protocolos de borrado seguro de neurodatos en bruto una vez cumplida la finalidad del tratamiento; y,
- c) Abstenerse de inferir información más allá de la finalidad declarada y consentida.

TÍTULO VII

TRATAMIENTO DE DATOS PERSONALES RELATIVOS A LA SALUD EN ENSAYOS CLÍNICOS

Art xx.- Las disposiciones del presente capítulo serán aplicables a los tratamientos de datos personales relativos a la salud realizados en el marco de ensayos clínicos reguladas por la Autoridad Sanitaria Nacional.

Estarán sujetos a las disposiciones de este capítulo principalmente los siguientes: patrocinadores, investigadores principales, centros de investigación, establecimientos de salud, organizaciones de investigación por contrato, monitores, auditores, laboratorios farmacéuticos, comités de ética de investigación en seres humanos y cualquier otra

persona natural o jurídica que participe en el tratamiento de datos personales durante el desarrollo de ensayos clínicos.

Art xx.- Antes del inicio del ensayo clínico, las partes involucradas deberán documentar expresamente sus respectivos roles como responsables, corresponsables o encargados del tratamiento, así como las obligaciones que asume cada uno respecto del cumplimiento de la LOPDP.

Art xx.- El acceso a datos personales relativos a la salud por parte encargados del tratamiento y terceros autorizados únicamente podrá realizarse cuando resulte estrictamente necesario para verificar:

- a) La seguridad de los participantes;
- b) La calidad e integridad del ensayo;
- c) El cumplimiento de obligaciones regulatorias;
- d) La validez científica de la información.

En todos los casos, el acceso deberá limitarse al mínimo necesario y quedar sujeto a obligaciones de confidencialidad y secreto profesional.

TITULO VIII

TRATAMIENTO DE DATOS PERSONALES RELATIVOS A LA SALUD MEDIANTE TECNOLOGÍAS DIGITALES DE SALUD

Art. xx.- Tendrán la consideración de datos personales relativos a la salud aquellos obtenidos, registrados, generados, inferidos o analizados mediante tecnologías digitales que permitan revelar o describir, directa o indirectamente, a la situación, condición o información relacionada con la salud de una persona natural.

Comprenderá, entre otras, las aplicaciones móviles de salud, plataformas digitales, sistemas informáticos, programas o aplicaciones de software, tecnologías de monitoreo remoto, dispositivos médicos conectados, dispositivos portátiles o vestibles (*wearables*), sensores biométricos y asistentes digitales o de cualquier otra naturaleza.

Cuando la tecnología digital de salud constituya dispositivo médico o software como dispositivo médico conforme a la normativa sanitaria, la aplicación de esta Norma se entenderá sin perjuicio de las competencias de la Agencia Nacional de Regulación, Control y Vigilancia Sanitaria. Las tecnologías de bienestar que no constituyan dispositivo médico quedan igualmente sujetas a la presente Norma cuando traten datos personales relativos a la salud.

Art. xx.- Tendrán la consideración de datos personales relativos a la salud aquellos obtenidos, registrados, generados, inferidos o analizados mediante tecnologías digitales que permitan revelar o describir, directa o indirectamente, el estado de salud físico o mental de una persona natural.

Art. xx.- Además del deber de información previsto en la LOPDP, los proveedores de tecnologías digitales de salud deberán cumplir con la obligación de información prevista en la LOPDP, de manera previa, clara, accesible y fácilmente comprensible, especialmente se deberá informar sobre:

- a) Las funcionalidades de la tecnología que impliquen tratamiento de datos personales de salud;
- b) La utilización de algoritmos, procesos automatizados o sistemas de inteligencia artificial que intervengan en el tratamiento de los datos;
- c) La existencia de elaboración de perfiles, inferencias o predicciones relacionadas con el estado de salud del titular.

Art xx.- Se prohíbe a los proveedores de tecnologías digitales de salud:

- a) Comercializar datos personales relativos a la salud para fines incompatibles con aquellos que justificaron su recopilación;
- b) Utilizar datos personales relativos a la salud para publicidad comportamental sin una base de legitimación conforme a la LOPDP;
- c) Reutilizar datos personales relativos a la salud para finalidades incompatibles de las que fundamentaron su recopilación;
- d) Implementar funcionalidades que amplíen sustancialmente el tratamiento de datos sin actualizar el deber de información y verificar la base de legitimación correspondiente. Entendiéndose tales ampliaciones, pero sin limitarse, a las siguientes: aquellas que impliquen la recolección de nuevas categorías de datos de salud, inferencia o perfilamiento de datos, nuevas finalidades de tratamiento o la incorporación de nuevos destinatarios no informados previamente

Art xx.- Cuando las tecnologías digitales permitan el intercambio de datos personales relativos a la salud con otros sistemas, plataformas, dispositivos de cualquier naturaleza o prestadores de servicios, el responsable deberá garantizar que:

- a) Los encargos de tratamiento o, transferencias/comunicaciones, según corresponda, cumplan con lo previsto en la LOPDP y normativa específica emitida por la SPDP;
- b) Se compartan únicamente los datos estrictamente necesarios;
- c) Se implementen mecanismos de autenticación, autorización y trazabilidad de los accesos.
- d) Se preserve la integridad, disponibilidad y confidencialidad de la información durante todo el proceso de intercambio.

TÍTULO IX OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS

CAPÍTULO I OBLIGACIONES GENERALES

Art xx.- Los responsables del tratamiento de datos de salud deberán cumplir con las siguientes obligaciones a más de las ya establecidas en la LOPDP y en su RGLOPDP:

- a) Implementar protocolo de detección y actuación frente a brechas de seguridad;
- b) Designar un delegado de protección de datos;
- c) Llevar un registro de actividades de tratamiento;
- d) Realiza el análisis de riesgos en protección de datos personales;
- e) Realizar evaluaciones de impacto en protección de datos;
- f) Registrar y mantener actualizada la información en el Registro Nacional de Protección de Datos Personales;

- g) Capacitar periódicamente a su personal sobre protección de datos personales de salud y secreto profesional; e,
- h) Implementar medidas de seguridad de datos desde el diseño y por defecto en sus sistemas de información de salud.

Art xx. El encargado del tratamiento de datos de salud deberá:

- a) Implementar medidas de seguridad equivalentes a las del responsable;
- b) Devolver y eliminar los datos de salud una vez culminado el encargo; y,
- c) Permitir y colaborar con las auditorías e inspecciones que realice el responsable o esta Autoridad.

CAPÍTULO II

SEGURIDAD DE LOS DATOS Y SISTEMAS DE INFORMACIÓN DE SALUD

Art xx.- Deber reforzado de seguridad: Los responsables y encargados deberán implementar y mantener medidas técnicas, organizativas, administrativas, legales y físicas destinadas a proteger los datos personales relativos a la salud y los sistemas de información que intervengan en su tratamiento.

Las medidas deberán preservar la confidencialidad, integridad, disponibilidad, autenticidad, resiliencia y recuperación segura de los datos y servicios, y prevenir su acceso, utilización, alteración, comunicación, pérdida, destrucción o indisponibilidad no autorizados.

La seguridad deberá aplicarse durante todo el ciclo de vida del tratamiento y de los componentes tecnológicos utilizados, desde su diseño, adquisición o desarrollo hasta su actualización, sustitución, retiro o eliminación.

Las medidas deberán ser compatibles con la seguridad del paciente, la continuidad asistencial y el funcionamiento seguro de los servicios y dispositivos de salud. La evaluación de riesgos determinará las medidas adicionales y no podrá justificar la exclusión de los mínimos establecidos en esta Norma.

Art xx.- Los responsables y encargados del tratamiento de datos personales de salud deberán aplicar las medidas de seguridad establecidas en el Esquema Gubernamental de Seguridad de la Información (EGSI), cuando les resulte aplicable, y demás normativa técnica vigente, incorporando las medidas adicionales que correspondan según la naturaleza, finalidad, contexto y resultados del análisis del riesgo en el tratamiento. En particular, deberán garantizar:

- a) Control del entorno tecnológico: identificación y mantenimiento actualizado de los sistemas, dispositivos, bases de datos, integraciones, versiones, componentes, proveedores y flujos de información que intervengan en el tratamiento;
- b) Gestión de identidades y accesos: identificación individual de usuarios y dispositivos; autenticación adecuada; asignación de permisos conforme a las funciones autorizadas; mínimo privilegio; segregación de funciones; revisión periódica de accesos; y control reforzado de cuentas privilegiadas, accesos remotos y accesos de emergencia;
- c) Protección de datos y comunicaciones: mecanismos criptográficos apropiados para los datos almacenados, transmitidos y respaldados; gestión segura de claves,

- credenciales y secretos; y medidas para prevenir la copia, exportación, comunicación o extracción no autorizada;
- d) Operación y mantenimiento seguro: configuración segura de sistemas y dispositivos; gestión de cambios, vulnerabilidades, actualizaciones y parches; restricción de servicios e interfaces innecesarias; control del soporte remoto; y gestión de componentes obsoletos o sin soporte;
 - e) Registro, monitoreo y auditoría: conservación protegida de registros que permitan identificar los accesos y operaciones relevantes; monitoreo de eventos anómalos; revisión de actividades privilegiadas; protección de los registros frente a alteración o eliminación; y preservación de evidencia cuando corresponda; y,
 - f) Continuidad, recuperación y respuesta: copias de respaldo protegidas; pruebas de restauración; mecanismos de continuidad operativa y asistencial; detección, contención y recuperación frente a incidentes; y procedimientos de notificación de vulneraciones conforme a la normativa aplicable.

Art xx.- Sistemas conectados, embebidos y prestación remota: Cuando el tratamiento se realice mediante dispositivos de salud conectados, sistemas embebidos, plataformas de telemedicina, mecanismos de interoperabilidad, aplicaciones móviles, monitoreo remoto o servicios en nube, las medidas mínimas comprenderán, además:

- a) La criticidad del uso del dispositivo, sistema o servicio y su impacto en la seguridad del paciente, la continuidad asistencial y los derechos de los titulares;
- b) Los riesgos derivados de la interconexión, interoperabilidad, administración remota, dependencia de terceros y exposición de interfaces o servicios;
- c) Las condiciones técnicas, de soporte, actualización y ciclo de vida establecidas por el fabricante o proveedor;
- d) La integridad y trazabilidad de la información intercambiada o incorporada a los sistemas de salud; y,
- e) La disponibilidad de mecanismos de continuidad y recuperación ante fallos de conectividad, componentes o servicios críticos.
- f) La integración del paradigma de protección de datos personales por diseño y por defecto dentro del ciclo de desarrollo.

Cuando una medida de seguridad no pueda implementarse por razones técnicas, clínicas, de compatibilidad o relacionadas con el ciclo de vida del componente, el responsable deberá documentar la situación, evaluar el riesgo y adoptar medidas compensatorias o un plan de mitigación, sustitución o retiro, según corresponda.

Art. xx.- Cuando se permita a los titulares o a terceros autorizados acceder a resultados de exámenes, imágenes diagnósticas, historias clínicas, informes médicos u otros datos personales relativos a la salud mediante enlaces, códigos, portales de descarga o mecanismos equivalentes, el responsable deberá implementar medidas que impidan su acceso indiscriminado o no autorizado.

Estos mecanismos deberán considerar, de acuerdo con el riesgo, la naturaleza de la información y las consecuencias de un acceso indebido, al menos lo siguiente medidas de seguridad:

- a) La verificación de la identidad o legitimación de la persona que solicita el acceso;

- b) La utilización de enlaces individualizados, no predecibles, con vigencia limitada y susceptibles de revocación;
- c) La aplicación de mecanismos de autenticación independientes del mero conocimiento o posesión del enlace, tales como credenciales personales, códigos de un solo uso, autenticación de múltiples factores u otros mecanismos equivalentes, cuando el riesgo lo requiera;
- d) La limitación del número de accesos, dispositivos, sesiones o descargas, cuando resulte proporcional a la finalidad;
- e) El registro de la generación, envío, apertura, autenticación, consulta, descarga, intento fallido, expiración y revocación del mecanismo de acceso, en cuanto resulte técnicamente aplicable;
- f) La protección de los documentos frente a su indexación pública, acceso automatizado, modificación, sustitución o exposición mediante direcciones permanentes;
- g) La disponibilidad de mecanismos para revocar el acceso, reportar su envío a un destinatario incorrecto o solicitar la emisión de un nuevo enlace; y,
- h) La información clara al titular sobre la vigencia del acceso, las medidas de seguridad aplicables y los riesgos derivados de compartir el enlace, las credenciales o los documentos descargados.

La entrega o utilización de un mecanismo de acceso no trasladará al titular la responsabilidad derivada de las deficiencias de seguridad atribuibles al responsable o encargado del tratamiento. Cuando el titular requiera compartir la información con un profesional de la salud u otro tercero, el responsable procurará habilitar mecanismos de acceso delegado, temporal y trazable, sin perjuicio del derecho del titular a obtener y comunicar sus propios datos.

Los mecanismos de acceso público, permanentes, reutilizables o que permitan consultar datos de salud únicamente mediante su posesión se considerarán insuficientes, salvo que el responsable demuestre, mediante una evaluación documentada de riesgos, que la naturaleza de la información y los controles compensatorios aplicados ofrecen un nivel de seguridad adecuada.

Los mecanismos de acceso a datos personales relativos a la salud deberán responder a una evaluación documentada de riesgos y no podrán basarse exclusivamente en la posesión de un enlace, código o mecanismo equivalente cuando ello resulte insuficiente para garantizar la seguridad de la información.

Art xx.- Verificación de la efectividad: Los responsables y encargados verificarán, de manera planificada y documentada, la implementación y efectividad de las medidas mediante revisiones técnicas, evaluaciones de vulnerabilidades, pruebas de recuperación y, cuando corresponda, pruebas de penetración.

La verificación se realizará con una periodicidad acorde con la criticidad del sistema y, adicionalmente, antes de la puesta en producción de sistemas de alto impacto, después de cambios sustanciales, ante vulnerabilidades relevantes o luego de incidentes que comprometan la seguridad o la continuidad asistencial.

Las vulneraciones de seguridad de datos personales se notificarán a la SPDP y a los titulares cuando corresponda, de conformidad con la LOPDP y su Reglamento. Los

incidentes de ciberseguridad se reportarán a las autoridades o equipos competentes únicamente en los supuestos previstos en la normativa específica.

CAPÍTULO III

CASOS DE SEGURIDAD REFORZADA

Art xx. El tratamiento de datos personales de personas con discapacidad o de grupos vulnerables, relativos a su condición de salud o discapacidad, gozará de protección reforzada. Los responsables deberán:

- a) Garantizar la accesibilidad de los mecanismos para el ejercicio de derechos;
- b) Proporcionar información en formatos accesibles y comprensibles según el tipo de discapacidad o enfermedad;
- c) Obtener el consentimiento de manera adaptada a las capacidades del titular, conforme la normativa específica; y,
- d) Abstenerse de utilizar los datos relativos a la discapacidad o de grupos vulnerables para fines discriminatorios.

Art xx. Los datos relativos a la salud mental gozan de una protección reforzada en atención a su naturaleza sensible y al impacto que su divulgación puede tener en la dignidad, autonomía e integridad del titular. Los responsables y encargados del tratamiento deberán:

- a) Aplicar medidas de seguridad reforzadas para datos de diagnóstico, tratamiento y evolución en salud mental;
- b) Garantizar el secreto profesional y la confidencialidad en todas las modalidades de atención, sean presenciales, virtuales o telemáticas;
- c) Abstenerse de comunicar datos de salud mental a terceros sin consentimiento explícito del titular, salvo los supuestos legales de excepción; e,
- d) Implementar protocolos específicos de acceso restringido a datos de salud mental dentro de los sistemas de información clínica.

TÍTULO X

PROCESOS INTERNOS DE LA AUTORIDAD

CAPÍTULO I

SUPERVISIÓN Y CONTROL

Art xx.- La SPDP realizará supervisiones aleatorias a los responsables del tratamiento autorizados, a tratar datos personales de salud que no hayan sido anonimizados, así como los tratamientos autorizados que se encuentran anonimizados, para verificar:

- a) El cumplimiento de protocolos;
- b) La efectividad de las medidas de seguridad implementadas;
- c) La no reidentificación de los titulares; y,
- d) El cumplimiento de las condiciones de la autorización.

Art xx.- Las causales de revocatoria son las siguientes:

- a) Se detecte incumplimiento del protocolo aprobado;
- b) Se verifique la reidentificación de titulares;

- c) Se modifiquen sustancialmente las condiciones bajo las cuales se otorgó la autorización sin solicitar nueva autorización; o,
- d) Se determine que las técnicas de anonimización aplicadas resultan insuficientes conforme el estado de la técnica.

Art xx.- El procedimiento para la revisión o revocatoria de cualquiera de las autorizaciones otorgadas, se cumplirá el siguiente procedimiento:

xx.1. Inicio del procedimiento: La ICS podrá iniciar, de oficio o a petición de parte interesada, el procedimiento de revisión y posible revocatoria cuando existieren indicios razonables de incumplimiento, de los requisitos establecidos en la presente norma bajo los cuales fue otorgada la autorización.

Sobre la base de tales indicios, la ICS deberá verificar la existencia del incumplimiento mediante el inicio de una actuación previa. Concluido dicho proceso, y de verificarse que el responsable del tratamiento este incurso en alguna causal de revocatoria o hubiere incumplido la normativa de protección de datos personales, se remitirá a la IIT un informe técnico en el que evidenciará cuál ha sido el incumplimiento constatado.

Si el incumplimiento fuere de aquellos constitutivos de infracción de acuerdo con la LOPDP, la ICS podrá continuar con la actuación previa; y, eventualmente, disponer que se implementen medidas correctivas.

xx.2. Informe técnico: Una vez que la IIT reciba el informe técnico emitido por la ICS, comenzará a discurrir el plazo de dos (2) meses para la emisión del informe correspondiente de hallazgos técnicos, en el cual se deberá determinar en forma motivada si hay un incumplimiento técnico y, como consecuencia de ello un riesgo viable.

Luego de que la IIT tenga la información, el informe de la IIT deberá recomendar que se rectifique la autorización, que se dispongan modificaciones o, en su caso, que la autorización sea revocada.

xx.3. Modificación: En caso de que se concluyere la necesidad de modificar los elementos de la autorización, el responsable del tratamiento deberá modificarlas en un término no mayor de treinta (30) días. Al efecto, se cumplirá el mismo procedimiento establecido para la autorización.

xx.4. Resolución: La IIT notificará al Superintendente con el informe técnico que recomiende la revocatoria o la rectificación junto con todo el expediente recibido de la ICS, el Superintendente de Protección de Datos Personales tendrá el término de diez (10) días para expedir una resolución motivada en virtud de la cual podrá:

xx.4.1. Ratificar la autorización;

xx.4.2. Revocar la aprobación del tratamiento autorizado de datos de salud.

xx.5. Efectos de la revocatoria: Expedida la resolución de revocatoria, el responsable del tratamiento deberá cesar inmediatamente, sin dilación alguna, el tratamiento correspondiente.

xx.6. Registro y publicidad: La resolución de revocatoria será publicada en el portal institucional de la SPDP, con el objeto de facilitar su acceso y conocimiento público y evitar que se produzcan vulneraciones a los derechos de los titulares de datos personales.

Art. xx.- A través de la ICS, y mientras se lleve a cabo el proceso de revisión o revocatoria, la SPDP podrá disponer la suspensión temporal del tratamiento previamente autorizado, siempre y cuando existieren indicios razonables de vulneraciones a los derechos de los titulares de datos personales y de incumplimiento a la normativa de protección de datos personales.

La suspensión tendrá carácter preventivo y se mantendrá vigente hasta la conclusión del procedimiento de revisión o revocatoria correspondiente.

El tratamiento de datos personales de salud previamente realizado con la autorización inicial dada será objeto de un control posterior o *ex post*.

CAPÍTULO II COORDINACIÓN INTERINSTITUCIONAL

Art xx. La SPDP mantendrá mecanismos permanentes de coordinación con la Autoridad Sanitaria Nacional para:

- a) La recepción de informes previos para la autorización de tratamientos de datos de salud anonimizados;
- b) El intercambio de información sobre vulneraciones de seguridad que afecten datos de salud;
- c) La capacitación conjunta a los actores del Sistema Nacional de Salud; y,
- d) La supervisión coordinada del cumplimiento normativo.

CAPÍTULO III REGISTRO Y PUBLICIDAD

Art xx.- Esta autoridad, a través de la IIT mantendrá, a más de los expedientes de todo el proceso, un registro interno de las autorizaciones otorgadas para el tratamiento de datos de salud, el cual contendrá:

- a) Identificación del responsable autorizado;
- b) Tipo de autorización otorgada, esto es anonimizada o no;
- c) Finalidades del tratamiento autorizadas;
- d) Fecha de otorgamiento;
- e) Condiciones especiales impuestas, siempre que existieran; y,
- f) Estado de la autorización (vigente, revocada, vencida).

Art xx.- La SPDP emitirá lineamientos y directrices orientadoras para facilitar el cumplimiento de la presente Norma por parte de los administrados, las cuales podrán abordar, entre otros temas:

- a) Técnicas de anonimización y seudonimización recomendadas para datos de salud;
- b) Modelos de consentimiento informado para el sector salud;

- c) Estándares de seguridad para datos de salud;
- d) Orientaciones para la protección de neuroderechos.

CAPÍTULO IV

REMISIÓN AL RÉGIMEN SANCIONATORIO

Art xx.- El incumplimiento de las disposiciones contenidas en la presente norma se sujetará al régimen de infracciones, medidas correctivas y sanciones establecido en la LOPDP y su Reglamento General. La SPDP aplicará las medidas correctivas y, de ser el caso, iniciará los procedimientos administrativos sancionatorios correspondientes, de conformidad con lo previsto en los artículos 65 al 74 de la LOPDP, el Capítulo XIV de su Reglamento General y el Código Orgánico Administrativo respecto al proceso administrativo sancionador.

DISPOSICIONES GENERALES

ÚNICA.- La presente Norma será revisada y actualizada por esta Autoridad cuando los avances tecnológicos, particularmente en materia de neurotecnologías, inteligencia artificial aplicada a la salud o técnicas de reidentificación, lo hagan necesario para mantener un nivel adecuado de protección.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Los responsables y encargados del tratamiento de datos de salud dispondrán del plazo de un (1) año contado a partir de la publicación de la presente norma en el Registro Oficial, para adecuar sus procesos, sistemas y documentación al contenido de la misma.

SEGUNDA.- Las solicitudes de autorización para tratamiento de datos de salud anonimizados que se encuentren en trámite a la fecha de entrada en vigencia de la presente Norma, se resolverán conforme con el procedimiento aquí establecido.

TERCERA.- En el plazo de seis meses (6) contados a partir de la publicación de la presente norma, la Superintendencia de Protección de Datos Personales habilitará el sistema electrónico para la recepción de solicitudes de autorización.

CUARTA.- La IIT deberá crear el registro interno de aprobaciones anonimizadas y no anonimizadas en un plazo de nueve meses a partir de la publicación de la presente norma en el Registro Oficial.

DISPOSICIÓN FINAL

La presente Norma Técnica entrará en vigencia a partir de su publicación en el Registro Oficial.

Comuníquese y publíquese.

Dado en el Distrito Metropolitano de Quito, a los [día] días del mes de [mes] de 2026.