

PROYECTO DE LEY No. ____ DE 2026 SENADO DE LA REPÚBLICA

Por medio del cual se establecen los lineamientos normativos éticos y de integridad científica para la gobernanza de sistemas de inteligencia artificial en el sector salud, se garantiza la seguridad del paciente; la protección de los datos de salud, la autonomía profesional y se dictan otras disposiciones.

**EL CONGRESO DE COLOMBIA
DECRETA**

TÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto. Establecer el marco normativo especial para la gobernanza, desarrollo, entrenamiento, validación, importación, comercialización, implementación, uso, actualización, supervisión, vigilancia y retiro de sistemas de inteligencia artificial en salud, con el fin de proteger la vida, la salud, la dignidad humana, la autonomía, la igualdad, la privacidad, la seguridad del paciente y la integridad científica, y promover innovación segura, responsable y sostenible.

Parágrafo. La interpretación y aplicación de la presente ley se realizará conforme al principio de prevalencia del derecho fundamental a la salud y de protección de la dignidad humana.

Artículo 2. Ámbito de aplicación. La presente ley se aplica a las personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras, que desarrollen, entrenen, suministren, importen, distribuyan, integren, implementen, operen o utilicen sistemas de inteligencia artificial en el Sistema General de Seguridad Social en Salud o con finalidad sanitaria en Colombia. También se aplicará cuando el tratamiento de datos, la prestación del servicio o el efecto clínico se produzca en territorio colombiano.

Artículo 3. Finalidades. Son finalidades de la ley: proteger a pacientes y usuarios; garantizar seguridad y calidad; establecer obligaciones por rol; asegurar validación y vigilancia; proteger datos sensibles; prevenir sesgos y discriminación; preservar autonomía profesional; promover investigación e innovación responsables; fortalecer capacidades institucionales y facilitar cooperación internacional.

Artículo 4. Exclusiones. No estarán sometidas a los requisitos sanitarios reforzados las herramientas de propósito general que no hayan sido destinadas, adaptadas o utilizadas para una finalidad clínica o sanitaria de riesgo, los programas basados exclusivamente en reglas determinísticas simples, las calculadoras convencionales y

los sistemas administrativos sin impacto material en derechos o decisiones asistenciales, sin perjuicio de las demás normas aplicables.

Parágrafo. La exclusión cesará cuando la finalidad declarada, el uso real o la integración del sistema produzca impacto clínico o significativo en derechos.

Artículo 5. Interpretación, especialidad y armonización. La presente ley se interpretará sistemáticamente con las normas sobre derecho fundamental a la salud, datos personales, historia clínica, ética médica, telesalud, investigación con seres humanos, dispositivos médicos, seguridad digital, protección al consumidor, propiedad intelectual y responsabilidad. En concurrencia con una ley general de inteligencia artificial, prevalecerá la regla especial sanitaria respecto de la seguridad clínica y del paciente.

Artículo 6. Definiciones. Para efectos de esta ley se entenderá por:

- a. **Contenido sintético clínico:** imagen, audio, video, señal, informe, registro o documento sanitario generado o materialmente modificado mediante inteligencia artificial.
- b. **Deepfake médico:** contenido sintético o manipulado que representa de forma falsa o engañosa a un paciente, profesional, procedimiento, hallazgo, imagen diagnóstica, señal biomédica o evento clínico, con capacidad de inducir error.
- c. **Sistema robótico clínico:** equipo, brazo robotizado, robot o plataforma física controlada o asistida por software o inteligencia artificial, destinado a ejecutar o apoyar procedimientos diagnósticos, intervencionistas, quirúrgicos, rehabilitadores o terapéuticos.
- d. **Sistema de inteligencia artificial en salud:** sistema basado en máquinas que, con distintos niveles de autonomía, infiere a partir de entradas cómo generar predicciones, contenidos, recomendaciones o decisiones para una finalidad sanitaria.
- e. **Proveedor:** quien desarrolla o coloca el sistema en el mercado bajo su nombre.
- f. **Implementador:** quien integra o utiliza el sistema bajo su autoridad.
- g. **Operador clínico:** profesional o equipo que usa sus resultados.
- h. **Validación analítica:** demostración del desempeño técnico.
- i. **Validación clínica:** evidencia de seguridad, desempeño y utilidad en la población y contexto previstos.
- j. **Deriva algorítmica:** deterioro o cambio del desempeño por variaciones en datos, entorno o modelo.
- k. **Sistema adaptativo:** el que modifica su comportamiento después de su puesta en servicio.
- l. **Incidente grave:** evento que cause o pueda causar muerte, deterioro serio de la salud, discriminación grave o afectación masiva de datos.

- m. Modelo de propósito general: modelo capaz de cumplir múltiples tareas y susceptible de integración en diferentes sistemas.
- n. IA generativa: sistema capaz de producir contenido nuevo en texto, audio, imagen, video, código u otras modalidades.

TÍTULO II. PRINCIPIOS Y DERECHOS

Artículo 7. Principios éticos, bioéticos y rectores. El desarrollo y uso de IA en salud se regirá por la dignidad humana, centralidad de la persona, autonomía, beneficencia, no maleficencia, justicia, solidaridad, equidad, no discriminación, precaución proporcional, supervisión humana efectiva, privacidad desde el diseño, confidencialidad, seguridad, ciberresiliencia, calidad de datos, transparencia, explicabilidad proporcional, trazabilidad, responsabilidad, rendición de cuentas, interoperabilidad, accesibilidad, sostenibilidad, integridad científica y neutralidad tecnológica. La aplicación de estos principios deberá atender el contexto clínico, social, territorial, cultural y poblacional.

Artículo 8. Primacía de la persona, autonomía profesional y juicio clínico. Los sistemas de inteligencia artificial en salud tendrán carácter de apoyo y consulta. No sustituirán automáticamente el juicio clínico ni serán de seguimiento obligatorio en decisiones con consecuencias significativas para la vida, la integridad o la salud. El profesional conservará la facultad y el deber de aceptar, controvertir o apartarse de la recomendación algorítmica por razones clínicas, científicas, éticas, bioéticas o contextuales, de conformidad con sus competencias y autonomía profesional. Cuando resulte pertinente para la seguridad del paciente y la trazabilidad de la atención, dejará constancia de los fundamentos de su decisión.

Parágrafo. Ninguna institución, asegurador, proveedor o desarrollador podrá imponer al profesional el seguimiento automático de una recomendación algorítmica ni derivar consecuencias adversas por apartarse de ella cuando exista justificación clínica, científica, ética o bioética.

Artículo 9. Derecho a la información. Toda persona tendrá derecho a conocer, en lenguaje claro y accesible, cuando un sistema de IA intervenga materialmente en su atención, su finalidad general, limitaciones relevantes, grado de participación humana, categorías de datos utilizados cuando proceda y canales de revisión o reclamación.

Artículo 10. Derecho a revisión humana. Ninguna decisión exclusivamente automatizada podrá negar, suspender, priorizar, limitar o modificar el acceso a servicios, tecnologías, medicamentos, procedimientos o prestaciones en salud cuando produzca efectos jurídicos o clínicos significativos. La persona tendrá

derecho a revisión humana oportuna, motivada y realizada por personal competente.

Artículo 11. Consentimiento y autonomía. El uso de IA como parte ordinaria de una tecnología o proceso asistencial autorizado se informará en el consentimiento aplicable. Se requerirá consentimiento específico cuando implique investigación, experimentación, uso secundario no exceptuado de datos identificables, interacción clínica directa con agentes conversacionales o riesgo adicional relevante.

Artículo 12. No discriminación, equidad algorítmica y procedencia de los datos. Los sistemas no podrán generar resultados discriminatorios. Proveedores e implementadores evaluarán el desempeño por subgrupos relevantes, adoptarán medidas de mitigación y documentará las limitaciones identificadas. Las diferencias clínicamente justificadas no constituirán discriminación cuando estén sustentadas en evidencia y sean proporcionales.

Parágrafo 1º. Los proveedores deberán documentar la procedencia geográfica, demográfica, clínica y temporal de los datos utilizados para entrenar, validar y probar el sistema, así como su grado de representatividad frente a la población colombiana y a la población objetivo.

Parágrafo 2º. Cuando los algoritmos o conjuntos de datos provengan de poblaciones, sistemas de salud o contextos sustancialmente diferentes a los colombianos, deberá realizarse validación contextual y evaluación específica de sesgos antes de su implementación.

Artículo 13º. Protección reforzada. Los sistemas destinados o aplicados a niños, niñas y adolescentes, personas con discapacidad, adultos mayores, grupos étnicos, población rural, personas con enfermedades raras o en situación de vulnerabilidad incorporarán salvaguardas reforzadas, accesibilidad, evaluación diferencial de sesgos y mecanismos adecuados de información y representación.

Artículo 14º. Derecho a queja, corrección y reporte. Pacientes, cuidadores y profesionales podrán solicitar corrección de datos, reportar fallas o incidentes, controvertir resultados y recibir respuesta dentro de los términos legales. Los canales deberán ser accesibles y no podrán condicionar la continuidad de la atención.

TÍTULO III. CLASIFICACIÓN POR RIESGO Y PRÁCTICAS PROHIBIDAS

Artículo 15. Clasificación por riesgo. Los sistemas se clasificarán como riesgo mínimo, limitado, alto o crítico según finalidad, autonomía, población, contexto, severidad del daño, reversibilidad, escala, dependencia del usuario y capacidad de

supervisión. El Gobierno Nacional a través de Ministerio de Salud y Protección Social reglamentará criterios, ejemplos y procedimientos de clasificación.

Artículo 16. Riesgo mínimo. Los sistemas de riesgo mínimo estarán sujetos a deberes generales de seguridad, calidad, privacidad y uso leal. Sus proveedores e implementadores deberán evitar representaciones engañosas sobre capacidades o beneficios.

Artículo 17. Riesgo limitado. Los sistemas de riesgo limitado cumplirán, además, obligaciones de transparencia, documentación básica, identificación de interacción automatizada o contenido sintético cuando corresponda, supervisión del implementador y canales de reporte.

Artículo 18. Alto riesgo. Se consideran de alto riesgo, entre otros, los sistemas que apoyen diagnóstico, pronóstico, tratamiento, dosificación, triage o priorización; determinen acceso o cobertura; funcionen como dispositivo médico o componente de seguridad; procesen datos genéticos o biométricos con finalidad clínica; controlen equipos terapéuticos o apoyen sistemas robóticos clínicos sin contacto autónomo directo con el paciente; o puedan producir impacto significativo en salud o derechos.

Artículo 19. Riesgo crítico. Serán de riesgo crítico los sistemas cuyo fallo o uso indebido pueda causar muerte, daño grave o afectación masiva, y aquellos con autonomía elevada en decisiones terapéuticas de alta severidad, así como los sistemas robóticos que ejecuten movimientos, energía, incisiones, resecciones, suturas, implantaciones u otras acciones físicas invasivas sobre el cuerpo humano. Solo podrán implementarse con evidencia robusta, control humano efectivo, contingencia, vigilancia intensificada y autorización sanitaria expresa.

Artículo 20. Prácticas prohibidas. Se prohíbe:

1. adoptar decisiones clínicas o de acceso exclusivamente automatizadas sin revisión humana;
2. Manipular subliminalmente o explotar vulnerabilidades para inducir conductas perjudiciales;
3. Establecer puntajes sociales sanitarios discriminatorios;
4. Inferir emociones para negar servicios o derechos;
5. Discriminar por categorías protegidas;
6. Reutilizar datos de salud para publicidad conductual incompatible o fijación individual discriminatoria de precios;
7. Presentar contenido generado por inteligencia artificial como consejo de un profesional real sin advertencia;
8. Usar sistemas no autorizados cuando la autorización sea exigible;
9. ocultar incidentes o alterar registros de trazabilidad;
10. Utilizar sistemas de inteligencia artificial para realizar publicidad, promoción o recomendación encubierta de medicamentos, dispositivos

médicos, tecnologías, procedimientos o servicios de salud, cuando exista conflicto de interés, patrocinio no revelado, ausencia de evidencia suficiente o riesgo de inducir decisiones clínicas o de consumo contrarias al interés del paciente.;

11. Crear, alterar, falsificar, distribuir o utilizar deepfakes médicos, imágenes radiológicas falsas, señales biomédicas manipuladas, informes clínicos sintéticos engañosos o cualquier contenido que suplante, distorsione u oculte información sanitaria con potencial de afectar la atención, la investigación, la vigilancia, la prueba o los derechos de las personas;

12. Permitir que brazos robotizados o robots ejecuten de manera autónoma procedimientos diagnósticos invasivos, intervencionistas, quirúrgicos o terapéuticos sobre seres humanos sin supervisión directa y continua de un médico especialista competente y sin capacidad de intervención o detención inmediata.

Parágrafo. Toda recomendación automatizada que incluya productos, tecnologías o servicios deberá identificar de manera clara cualquier patrocinio, vínculo económico o interés comercial y diferenciar la información científica de la publicidad.

Artículo 21. Reclasificación y modificación sustancial. La autoridad podrá reclasificar un sistema cuando cambie su finalidad, población, entorno, autonomía, desempeño o evidencia de riesgo. La modificación sustancial de sistemas de alto o crítico riesgo requerirá evaluación previa o un plan de control de cambios aprobado.

TÍTULO IV.

EVALUACIÓN, VALIDACIÓN, AUTORIZACIÓN Y CICLO DE VIDA

Artículo 22. Requisitos generales de alto y crítico riesgo. Antes de su implementación deberán existir: gestión de riesgos; documentación técnica; gobernanza de datos; validación analítica y clínica; evaluación de sesgos; ciberseguridad; supervisión humana; instrucciones de uso; trazabilidad; plan de monitoreo; gestión de incidentes; continuidad operativa y retiro seguro; filtros de seguridad para contenido sintético; mecanismos de autenticidad, procedencia y detección de manipulaciones; y, tratándose de sistemas robóticos clínicos, validación preclínica anatómica, simulación, límites de autonomía, parada de emergencia y control humano directo.

Artículo 23. Validación clínica contextual. La evidencia deberá demostrar asociación clínica válida, desempeño técnico y utilidad clínica en la población, entorno y finalidad previstos. Cuando los datos no representen adecuadamente a la población colombiana, se exigirá validación local o evidencia equivalente.

Parágrafo. Los sistemas robóticos clínicos deberán demostrar, antes de su uso en seres humanos, desempeño y seguridad mediante entrenamiento, simulación y pruebas preclínicas sobre modelos anatómicos, componentes anatómicos, simuladores, fantasmas, especímenes u otros medios equivalentes científicamente aceptados. La autoridad sanitaria determinará los requisitos según la finalidad, invasividad y riesgo.

Artículo 24. Evaluación integral de impacto algorítmico y bioético. Antes del despliegue de sistemas de alto o crítico riesgo, el implementador elaborará una evaluación documentada que abarque riesgos clínicos, éticos, bioéticos, jurídicos, de datos, equidad, discriminación, seguridad digital, interoperabilidad, organización del trabajo, relación profesional-paciente, continuidad asistencial, sostenibilidad e impacto territorial. Deberá identificar beneficios esperados, alternativas disponibles, poblaciones afectadas, medidas de mitigación, riesgos residuales, responsables y criterios de suspensión; riesgos de falsificación o manipulación de contenido clínico; y, en sistemas robóticos, autonomía física, interacción humano-máquina, entrenamiento del especialista, plan de conversión manual y mecanismos de detención segura. Se actualizará ante cambios sustanciales o evidencia nueva.

Artículo 25. Autorización y control sanitario. Los sistemas que constituyan dispositivo médico, software como dispositivo médico, componente de seguridad o tecnología sanitaria sujeta a control requerirán autorización, permiso o registro ante el INVIMA conforme al nivel de riesgo. El Gobierno reglamentará procedimientos proporcionales, equivalencias y confianza regulatoria internacional.

Para tal efecto, el INVIMA podrá administrar los procedimientos de autorización, permiso o registro sanitario; realizar actividades de inspección; emitir alertas; adoptar medidas sanitarias de seguridad; coordinar la vigilancia posmercado y la cooperación regulatoria; y expedir o adoptar guías técnicas sustentadas en estándares nacionales o internacionales reconocidos, de conformidad con la legislación aplicable.

Tratándose de sistemas de inteligencia artificial que generen, reconstruyan o modifiquen contenido clínico sintético, el INVIMA podrá exigir mecanismos proporcionales de autenticidad, procedencia, trazabilidad, conservación del original, detección de manipulación y control de falsificaciones. En los sistemas robóticos o brazos robotizados destinados a procedimientos diagnósticos invasivos, intervencionistas, quirúrgicos o terapéuticos, podrá exigir, según su naturaleza y nivel de riesgo, validación anatómica preclínica, simulación, documentación del entrenamiento del operador, mecanismos de parada de emergencia, límites de autonomía, conversión a control manual y supervisión directa y continua por un médico especialista competente.

Artículo 26. Registro Nacional de Sistemas de Inteligencia Artificial en Salud. Créase el Registro Nacional de Sistemas de Inteligencia Artificial en Salud, como instrumento público de información, seguimiento, vigilancia y gestión regulatoria de los sistemas de inteligencia artificial utilizados en el sector salud, administrado por el Ministerio de Salud y Protección Social o por la entidad que éste designe.

Deberán inscribirse obligatoriamente en el Registro los sistemas de inteligencia artificial clasificados como de alto o crítico riesgo, de conformidad con las categorías, criterios y procedimientos establecidos en la presente ley y su reglamentación. El Gobierno Nacional podrá establecer mecanismos simplificados de identificación, información o reporte para sistemas clasificados como de riesgo limitado cuando, por su finalidad, escala de utilización, población involucrada o contexto de implementación, puedan generar una incidencia relevante en la prestación de servicios de salud o en los derechos de pacientes y usuarios. En ningún caso dichos mecanismos implicarán extender a los sistemas de riesgo mínimo o limitado las obligaciones regulatorias propias de los sistemas de alto o crítico riesgo, salvo que sean reclasificados de conformidad con la presente ley.

El Registro contendrá, como mínimo, la identificación del proveedor y del implementador cuando corresponda; la finalidad y uso previsto del sistema; su clasificación de riesgo; versión o versiones autorizadas; estado regulatorio; población objetivo; institución o instituciones en las cuales se implemente, cuando resulte aplicable; incidentes relevantes conocidos; alertas de seguridad; modificaciones sustanciales y medidas de mitigación adoptadas. La obligación de registro estará a cargo del proveedor y, cuando corresponda según la naturaleza de la implementación, del implementador del sistema, quienes serán responsables de suministrar información veraz, completa, suficiente y actualizada.

Parágrafo 1º. La información contenida en el Registro será tratada de conformidad con las disposiciones sobre protección de datos personales, historia clínica, secreto profesional, propiedad intelectual, secretos empresariales, seguridad digital y demás normas aplicables. El Ministerio de Salud y Protección Social adoptará las medidas necesarias para garantizar que la información publicada o puesta a disposición del público no permita acceder a datos personales sensibles, secretos empresariales, información técnica protegida, vulnerabilidades de seguridad o información cuya divulgación pueda comprometer la seguridad de los pacientes, de las instituciones o de los propios sistemas.

La información sometida a reserva o confidencialidad estará disponible únicamente para las autoridades competentes, dentro del ámbito de sus funciones de inspección, vigilancia, control, evaluación o investigación.

Parágrafo 2º. Los sistemas de inteligencia artificial de alto o crítico riesgo que se encuentren en uso a la entrada en vigencia de la presente ley deberán ser inscritos

en el Registro. Los responsables de dichos sistemas dispondrán de un plazo máximo de dieciocho (18) meses, contado a partir de la reglamentación correspondiente, para acreditar progresivamente el cumplimiento de los requisitos y obligaciones establecidos en la presente ley, sin perjuicio de que la autoridad competente pueda establecer plazos inferiores cuando exista riesgo grave o inminente para la vida, la salud o la seguridad de las personas.

La inscripción en el Registro no sustituye las autorizaciones, permisos, certificaciones, registros sanitarios, evaluaciones de conformidad, requisitos de habilitación ni demás obligaciones regulatorias que resulten exigibles de acuerdo con la naturaleza, finalidad y nivel de riesgo del sistema.

Parágrafo 3º. El Ministerio de Salud y Protección Social reglamentará el funcionamiento, administración, interoperabilidad, actualización, mecanismos de inscripción, modificación y retiro, condiciones de acceso, intercambio de información entre autoridades y demás aspectos necesarios para la operación del Registro, dentro de los doce (12) meses siguientes a la entrada en vigencia de la presente ley. La reglamentación deberá garantizar proporcionalidad regulatoria, interoperabilidad, neutralidad tecnológica, seguridad de la información, protección de datos y ausencia de cargas administrativas injustificadas para sistemas de menor riesgo.

Artículo 27. Evaluación institucional previa. Las Entidades Administradoras de Plan de Beneficios (EAPB), las Instituciones Prestadoras de servicios de Salud (IPS) o la entidad que haga sus veces, las entidades territoriales y demás implementadores verificarán pertinencia, autorización, evidencia, capacidad operativa, interoperabilidad, capacitación, ciberseguridad y plan de contingencia antes de adquirir o usar sistemas de alto o crítico riesgo.

Artículo 28. Gestión de cambios y sistemas adaptativos. Los proveedores definirán límites de modificación, métricas, datos autorizados, criterios de actualización, pruebas, reversión y comunicación. Los cambios que excedan el plan aprobado requerirán nueva evaluación.

Parágrafo. Los sistemas de inteligencia artificial en salud clasificados como de alto o crítico riesgo deberán contar con un historial técnico íntegro, cronológico, verificable e inalterable de todas las modificaciones efectuadas durante su ciclo de vida. Dicho historial deberá contener, como mínimo, la identificación de cada versión del sistema, modelo o componente; la fecha, finalidad, alcance y responsable de la modificación; los conjuntos o fuentes de datos utilizados para entrenamiento, ajuste, reentrenamiento, validación o prueba; las métricas de desempeño anteriores y posteriores; las pruebas técnicas, clínicas, de interoperabilidad, sesgo y ciberseguridad realizadas; los incidentes, alertas, desviaciones y medidas correctivas asociadas; las decisiones de aprobación, rechazo, suspensión, reversión

o retiro; y la comunicación de los cambios a los implementadores, operadores clínicos y autoridades competentes, cuando corresponda.

El historial técnico deberá estar disponible para las autoridades competentes y, de acuerdo con sus funciones, responsabilidades y niveles de acceso, para los implementadores, auditores y operadores clínicos. La información deberá conservarse durante toda la vida útil del sistema y por el término adicional previsto en las normas sanitarias, de historia clínica, de protección de datos personales, de responsabilidad, de archivo y de vigilancia aplicables.

Artículo 29. Vigilancia posmercado y desempeño real. Proveedores e implementadores monitorearán falsos positivos y negativos, sesgos, deriva, fallos, ciberincidentes, uso fuera de indicación, contenido sintético fraudulento, fallas de autenticidad o procedencia, movimientos robóticos no previstos, activaciones indebidas, fallas de parada de emergencia y efectos adversos. Los incidentes graves se reportará inmediatamente y dentro de los plazos reglamentarios.

Artículo 30. Suspensión, retiro y alertas. El Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA) y las autoridades competentes podrán ordenar medidas preventivas, actualización, restricción, suspensión, retiro, alerta o cese de uso cuando exista riesgo no aceptable, incumplimiento o evidencia insuficiente. Las instituciones mantendrán planes de continuidad asistencial.

Artículo 31. Etiquetado e instrucciones de uso. Los sistemas de alto o crítico riesgo deberán identificar finalidad, población, condiciones de uso, contraindicaciones, limitaciones, métricas relevantes, requisitos de supervisión, versión, actualizaciones y canales de soporte y reporte.

TÍTULO V.

GOBERNANZA DE DATOS, INTEROPERABILIDAD Y CIBERSEGURIDAD

Artículo 32. Gobernanza de datos. El tratamiento de datos para IA en salud deberá tener finalidad legítima, base jurídica, minimización, calidad, exactitud, temporalidad, seguridad, trazabilidad y controles de acceso. Se documentarán procedencia, representatividad, etiquetado, transformaciones y limitaciones.

Artículo 33. Datos sensibles, uso secundario e investigación con seres humanos. El uso secundario de datos de salud para entrenamiento, validación o investigación se ajustará al régimen de protección de datos personales contenidos en la Ley 1581 de 2012 o la disposición que haga sus veces, las normas de ética de la investigación y a los principios de integridad científica. La anonimización o seudonimización no exime del análisis del riesgo de reidentificación.

El Gobierno Nacional en cabeza del Ministerio de Salud y Protección Social reglamentará entornos seguros de procesamiento y mecanismos de acceso controlado.

Parágrafo 1. Cuando el desarrollo, entrenamiento, validación o evaluación de un sistema implique investigación en seres humanos, intervención sobre personas, uso de muestras biológicas o tratamiento de información identificable o reidentificable, deberá cumplirse la normativa nacional aplicable y obtenerse la evaluación y aprobación previa de un comité de ética en investigación debidamente constituido, salvo las excepciones expresamente previstas en la ley.

Parágrafo 2. La aprobación ética no sustituye las autorizaciones sanitarias, de protección de datos o institucionales exigibles.

Artículo 34. Conjuntos de datos y prevención de sesgos. Los conjuntos de entrenamiento, validación y prueba deberán ser pertinentes, suficientemente representativos y examinados por subgrupos. Proveedores e implementadores identificarán, medirán, mitigarán y monitorearán sesgos que puedan producir resultados inequitativos.

Artículo 35. Calidad e integridad de datos clínicos. Los datos usados para fines clínicos deberán cumplir criterios de completitud, consistencia, actualidad, pertinencia y trazabilidad. La información sintética podrá utilizarse cuando su metodología, limitaciones y riesgo de distorsión estén documentados.

Artículo 36. Interoperabilidad y portabilidad. Los sistemas favorecerán estándares abiertos, continuidad clínica, portabilidad e integración segura con la historia clínica electrónica interoperable. No podrán crear barreras injustificadas de dependencia tecnológica ni impedir el acceso a información necesaria para la atención.

Parágrafo. Los sistemas de inteligencia artificial en salud que requieran intercambiar información con historias clínicas electrónicas, dispositivos médicos, plataformas institucionales, sistemas de salud pública u otras infraestructuras digitales deberán disponer, cuando resulte técnica y funcionalmente procedente, de interfaces de programación de aplicaciones – API – documentadas, interoperables y seguras.

Las interfaces deberán incorporar mecanismos de autenticación robusta; autorización basada en roles y niveles de acceso; cifrado de las comunicaciones y de los datos intercambiados; validación de entradas y salidas; control y monitoreo de solicitudes; registro de accesos, transacciones, eventos y errores; gestión de versiones; revocación de credenciales; pruebas periódicas de seguridad e interoperabilidad; y mecanismos de continuidad, contingencia, reversibilidad y recuperación.

La obligación de interoperabilidad no implicará la divulgación del código fuente, de secretos empresariales, de información reservada ni de elementos cuya revelación pueda comprometer la seguridad del sistema, la protección de los datos personales o los derechos de propiedad intelectual.

El Gobierno Nacional en cabeza del Ministerio de Salud y Protección Social reglamentará los estándares técnicos aplicables, con observancia de los principios de neutralidad tecnológica, seguridad, competencia, portabilidad y prevención de dependencias injustificadas frente a proveedores.

Artículo 37. Ciberseguridad. Los actores aplicarán seguridad desde el diseño, gestión de vulnerabilidades, autenticación, privilegios mínimos, cifrado, registro de eventos, pruebas periódicas, respuesta a incidentes y recuperación. Los ciberincidentes con impacto clínico o de datos se reportarán a las autoridades.

Artículo 38. Conservación y trazabilidad. Las decisiones, recomendaciones, versiones, entradas relevantes, intervenciones humanas y cambios se conservarán por el término necesario para auditoría, continuidad y responsabilidad, conforme a la regulación de historia clínica y datos personales.

Artículo 39. Transferencias y servicios en nube. La contratación de infraestructura o servicios en nube deberá asegurar localización o transferencia lícita, continuidad, reversibilidad, disponibilidad, auditoría, gestión de sub encargados y devolución o eliminación segura de datos.

TÍTULO VI.

IA GENERATIVA, AGENTES CONVERSACIONALES Y MODELOS DE PROPÓSITO GENERAL

Artículo 40. Uso clínico de IA generativa. Los modelos generativos o multimodales utilizados para resumir historias, redactar notas, apoyar diagnóstico, responder consultas o producir recomendaciones estarán sujetos a verificación humana, límites de uso, evaluación de alucinaciones, control de fuentes, protección frente a inyección de instrucciones y registro de versiones.

Artículo 41. Agentes conversacionales. Los chatbots o agentes que interactúen con pacientes se identificarán inequívocamente como automatizados, informarán sus limitaciones, no simularán identidad profesional y activarán escalamiento humano ante urgencia, incertidumbre, riesgo o solicitud del usuario.

Artículo 42. Contenido sintético, filtros de seguridad, conservación del original y trazabilidad. Las imágenes, audios, videos, señales, informes o documentos clínicos generados o materialmente modificados por inteligencia artificial deberán

incorporar salvaguardas proporcionales para prevenir, detectar y bloquear su falsificación, uso engañoso o circulación no autorizada. Tales salvaguardas incluirán, según el riesgo, verificación de autenticidad y procedencia, marcas de agua o credenciales digitales, metadatos de origen, control de acceso, firma o sello de integridad, detección de manipulaciones, registro inalterable de cambios y alertas frente a posibles deep fakes médicos o falsificación de imágenes radiológicas.

Parágrafo 1. Cuando la omisión de una marca visible pueda inducir a error, el contenido sintético o modificado deberá identificarse claramente. Podrá omitirse una marca visible si afecta la utilidad clínica, siempre que existan mecanismos internos verificables de autenticidad, procedencia y trazabilidad.

Parágrafo 2. La institución deberá conservar de manera íntegra, segura, inalterada y accesible la versión original de los exámenes, imágenes, señales, registros o documentos antes de cualquier modificación, reconstrucción, mejora o interpretación realizada mediante inteligencia artificial.

Parágrafo 3. El profesional autorizado deberá poder comparar en todo momento la versión original con la versión modificada o generada por inteligencia artificial. El sistema registrará la naturaleza, fecha, autor o proceso, versión, finalidad y alcance de cada modificación.

Parágrafo 4. Todo contenido sintético clínico detectado como fraudulento, no autorizado o potencialmente perjudicial deberá aislarse, conservarse como evidencia, reportarse conforme a los protocolos de incidentes y excluirse de decisiones clínicas hasta su verificación humana.

Artículo 43. Modelos de propósito general integrados en salud. Quien adapte o integre un modelo de propósito general para finalidad sanitaria asumirá las obligaciones del proveedor respecto de la adaptación y evaluará riesgos sistémicos, limitaciones del modelo base, procedencia de datos, propiedad intelectual, seguridad y actualizaciones.

Artículo 44. Prohibición de sustitución engañosa. Se prohíbe presentar un agente automatizado como profesional humano, atribuirle matrícula, especialidad o autoridad inexistente, o inducir al paciente a creer que existe valoración individual cuando solo se ha generado contenido automatizado.

Artículo 45. Sistemas robóticos, brazos robotizados y supervisión médica especializada. Los sistemas robóticos clínicos y brazos robotizados asistidos o controlados mediante inteligencia artificial no podrán operar autónomamente sobre seres humanos. Todo procedimiento diagnóstico invasivo, intervencionista, quirúrgico, terapéutico o rehabilitador que implique contacto físico, aplicación de energía, movimiento de instrumental o modificación del cuerpo requerirá

supervisión directa, continua y presencial de un médico especialista competente, habilitado y entrenado en el procedimiento y en el sistema utilizado, con autoridad y capacidad técnica para intervenir, detener o asumir el control inmediato.

Parágrafo 1. Antes de su utilización en seres humanos, el sistema deberá superar entrenamiento, simulación y validación preclínica documentada mediante modelos anatómicos, componentes anatómicos, simuladores, fantasmas, especímenes, tejidos o metodologías equivalentes científicamente aceptadas, según la finalidad, invasividad y nivel de riesgo.

Parágrafo 2. El proveedor y el implementador deberán establecer límites de autonomía, mecanismos redundantes de seguridad, parada de emergencia, conversión a control manual, registro de movimientos y comandos, mantenimiento, calibración, plan de contingencia y criterios de suspensión.

Parágrafo 3. La institución verificará y documentará la formación, competencia y habilitación del equipo humano antes de autorizar el uso del sistema. La capacitación deberá incluir simulación de fallos, recuperación del control y respuesta a eventos adversos.

Parágrafo 4. La inteligencia artificial podrá apoyar la planificación, navegación, estabilización, reconocimiento anatómico o ejecución controlada, pero no sustituirá la responsabilidad, el juicio clínico ni la presencia efectiva del médico especialista responsable.

TÍTULO VII.

OBLIGACIONES DE LOS ACTORES

Artículo 46. Obligaciones de proveedores. Garantizar diseño seguro, documentación, pruebas, calidad, información al usuario, monitoreo, soporte, gestión de incidentes, control de cambios y cooperación con autoridades; filtros de seguridad y autenticidad para contenido sintético; prevención de deep fakes médicos y falsificación de imágenes; y, en sistemas robóticos, límites de autonomía, pruebas anatómicas preclínicas, parada de emergencia y control manual seguro. No podrán ocultar limitaciones materialmente relevantes invocando secreto empresarial.

Artículo 47. Obligaciones de importadores y distribuidores. Verificarán autorización, identidad del proveedor, documentación, trazabilidad, condiciones de actualización y cumplimiento de alertas. Suspenderán la distribución cuando conozcan un riesgo no aceptable.

Artículo 48. Obligaciones de implementadores. Seleccionarán tecnologías pertinentes, verificarán autorización, capacitarán personal, definirán gobernanza, asegurarán supervisión humana, monitorearán resultados locales, reportarán

incidentes y mantendrán planes alternos, protocolos de autenticación de contenido clínico y procedimientos específicos de supervisión, parada y conversión manual para sistemas robóticos. No alterarán parámetros críticos sin evaluación.

Artículo 49. Obligaciones de los profesionales de la salud. Los profesionales usarán los sistemas dentro de su competencia y de la finalidad autorizada, considerarán sus limitaciones, contrastarán los resultados con la información clínica disponible y reportarán incidentes. Deberán respetar la autonomía del paciente y ejercer su autonomía profesional al aceptar, controvertir o apartarse de una recomendación algorítmica. No responderán por defectos ocultos, fallas de diseño, datos defectuosos, actualizaciones no informadas o información inexacta del proveedor que razonablemente no pudieran detectar.

Parágrafo. La utilización de un sistema de inteligencia artificial no exime al profesional de cumplir sus deberes éticos, bioéticos, de diligencia y de cuidado, ni traslada al profesional las responsabilidades propias del proveedor, fabricante, implementador u operador.

Artículo 50. Obligaciones EAPB e IPS. Las Entidades Administradoras de Planes de Beneficios (EAPB) y las Instituciones Prestadoras de Servicios de Salud (IPS) que implementen o utilicen sistemas de inteligencia artificial para actividades de gestión, auditoría, autorización, referencia y contrarreferencia, gestión del riesgo, priorización de servicios o cualquier otra función relacionada con el acceso, oportunidad, continuidad o prestación de servicios de salud deberán garantizar que dichos sistemas sean utilizados de manera segura, no podrán sustituir la valoración individual, crear barreras de acceso ni negar servicios exclusivamente por resultado algorítmico. Deberán en todo caso permitir revisión humana y conservar trazabilidad.

Artículo 51. Comités institucionales de gobernanza ética y bioética de la IA en salud. Las Instituciones Prestadoras de Servicios de Salud Públicas, Privadas o Mixtas que implementen sistemas de alto o crítico riesgo contarán con un comité o instancia interdisciplinaria de gobernanza ética y bioética de la IA en salud, articulado con los comités de ética hospitalaria y de ética en investigación cuando corresponda. Tendrá participación clínica, bioética, jurídica, científica, de datos, seguridad digital, calidad, ingeniería, administración y representación de pacientes o comunidades cuando resulte pertinente. Evaluará impactos, conflictos de interés, justicia distributiva, consentimiento, transparencia, riesgos residuales, incidentes y continuidad de uso, sin sustituir las competencias de las autoridades sanitarias.

Artículo 52. Formación, competencia y financiación de la capacitación. Las Instituciones Prestadoras de Servicios de Salud Públicas, Privadas o Mixtas verificarán que quienes desarrollen, configuren, evalúen o utilicen sistemas de alto o crítico riesgo posean las competencias adecuadas. La capacitación incluirá, como

mínimo, límites de uso, sesgos, seguridad, respuesta a fallos, protección de datos, supervisión humana, ética, bioética, autonomía profesional y reporte de incidentes, detección de contenido sintético fraudulento y, cuando corresponda, entrenamiento anatómico, simulación y recuperación del control de sistemas robóticos.

Parágrafo 1. El proveedor será responsable de suministrar la formación técnica inicial, los manuales, las actualizaciones y la información necesaria para el uso seguro del sistema. El implementador será responsable de asegurar la capacitación institucional, la evaluación de competencias, el reentrenamiento periódico y la disponibilidad de soporte.

Parágrafo 2. Los costos de la capacitación obligatoria necesaria para la implementación y uso seguro del sistema serán asumidos por el proveedor y el implementador, de acuerdo con sus obligaciones contractuales y regulatorias. No podrán trasladarse a los trabajadores de la salud, pacientes o cuidadores.

Parágrafo 3. El Ministerio de Salud y Protección Social, en coordinación con los Ministerios de Educación Nacional y de Tecnologías de la Información y las Comunicaciones, establecerá lineamientos mínimos de competencias y formación continua para el uso responsable de inteligencia artificial en salud.

TÍTULO VIII. INVESTIGACIÓN, BIOÉTICA E INTEGRIDAD CIENTÍFICA

Artículo 53. Marco ético y bioético durante el ciclo de vida. Todo sistema de IA en salud deberá someterse a deliberación ética y bioética proporcional a su riesgo durante las etapas de diseño, entrenamiento, validación, adquisición, implementación, uso, actualización, vigilancia y retiro. La evaluación aplicará los principios de dignidad, autonomía, beneficencia, no maleficencia, justicia, solidaridad, equidad, precaución, privacidad, integridad y responsabilidad; examinará efectos individuales y colectivos, impactos distributivos, relación clínica, vulnerabilidad, conflictos de interés y alternativas menos riesgosas. La investigación con IA se sujetará, además, a revisión por comité de ética cuando corresponda, evaluación de riesgo, consentimiento informado o excepción legal debidamente justificada, protección de poblaciones vulnerables y normas de integridad científica.

Artículo 54. Integridad científica. Se prohíbe fabricar, falsificar u ocultar datos, métricas, incidentes o resultados; seleccionar comparadores de manera engañosa; presentar evidencia no reproducible como validación; o utilizar contenido generado por IA sin los controles de autoría, verificación y citación aplicables.

Artículo 55. Transparencia de evidencia. Los estudios de validación de alto o crítico riesgo deberán registrar protocolo, población, métricas, comparadores, limitaciones

y resultados adversos. La autoridad podrá exigir publicación de resúmenes de evidencia y acceso confidencial a información técnica.

Artículo 56. Propiedad intelectual y acceso regulatorio. La protección de propiedad intelectual y secreto empresarial será compatible con el acceso de las autoridades a la información necesaria para evaluar seguridad, eficacia, calidad y cumplimiento. La información reservada será protegida conforme a la ley.

TÍTULO IX.

RESPONSABILIDAD, AUDITORÍA Y GARANTÍAS

Artículo 57. Responsabilidad por rol y control. La responsabilidad se determinará según la conducta, el deber de cuidado, la información disponible, el control efectivo sobre el riesgo y el nexo causal. El proveedor responderá por diseño, datos, validación, información y actualización; el implementador, por selección, integración, vigilancia y uso institucional; y el operador, por uso manifiestamente contrario a indicaciones o estándares.

Artículo 58. Carga dinámica de la prueba. En controversias por sistemas de alto o crítico riesgo, el juez podrá aplicar carga dinámica cuando la información técnica se encuentre bajo control exclusivo del proveedor o implementador. La falta injustificada de registros o documentación podrá valorarse como indicio.

Artículo 59. Seguro y garantías. El Gobierno Nacional podrá exigir pólizas, garantías financieras u otros mecanismos de cobertura para sistemas de riesgo crítico o implementaciones de gran escala, según naturaleza y magnitud del riesgo, de acuerdo con la reglamentación que se expida para tal fin.

Artículo 60. Auditoría independiente. Los sistemas de alto y crítico riesgo estarán sujetos a auditorías técnicas, clínicas, éticas, de datos y ciberseguridad con periodicidad proporcional. La autoridad podrá exigir auditoría independiente, pruebas de penetración, evaluación de impacto o acceso controlado a registros.

TÍTULO X.

AUTORIDADES, INSPECCIÓN, VIGILANCIA Y SANCIONES

Artículo 61. Rectoría. El Ministerio de Salud y Protección Social ejercerá la rectoría de la política nacional de inteligencia artificial en salud y, en el marco de sus competencias, dirigirá, coordinará, orientará y evaluará su implementación en el territorio nacional, en articulación con las demás autoridades y entidades competentes.

Asimismo, desarrollará las medidas necesarias para garantizar la aplicación y cumplimiento de los lineamientos mínimos éticos de gobernanza y uso de la

inteligencia artificial en salud, incluyendo criterios de transparencia, seguridad, protección de datos, autonomía, no discriminación, supervisión humana y protección de los derechos de los pacientes, en los términos de la presente ley.

Parágrafo 1º. El Ministerio de Salud y Protección Social establecerá mecanismos asistencia técnica financiera, de acuerdo con la disponibilidad presupuestal y las competencias de las entidades involucradas, para brindar acompañamiento a las entidades territoriales e instituciones prestadoras de servicios de salud con menor capacidad, priorizando zonas rurales, apartadas y con brechas digitales.

Artículo 62. Inspección, vigilancia, control y régimen sancionatorio. El incumplimiento de las obligaciones previstas en la presente ley y en las disposiciones reglamentarias expedidas en ejercicio de habilitación legal dará lugar, según corresponda, a la adopción de las medidas preventivas, sanitarias, correctivas y sancionatorias previstas en los regímenes legales aplicables, de acuerdo con la naturaleza del sujeto obligado, la tecnología involucrada, el nivel de riesgo, la conducta realizada y la competencia de la autoridad correspondiente.

Corresponderá al Instituto Nacional de Vigilancia de Medicamentos y Alimentos — INVIMA —, dentro del marco de sus competencias legales, ejercer las funciones de inspección, vigilancia y control sanitario respecto de fabricantes, desarrolladores, proveedores, importadores, distribuidores y comercializadores de tecnologías en salud que incorporen sistemas de inteligencia artificial y se encuentren sometidas a vigilancia sanitaria.

La Superintendencia Nacional de Salud, en el ámbito de sus competencias, ejercerá las funciones de inspección, vigilancia y control e impondrá las medidas o sanciones que correspondan respecto de las Entidades Administradoras de Planes de Beneficios, Instituciones Prestadoras de Servicios de Salud y demás sujetos sometidos a su vigilancia, cuando las conductas constituyan incumplimiento de las obligaciones derivadas del Sistema General de Seguridad Social en Salud y de la presente ley.

Cuando una misma conducta pueda comprometer competencias de distintas autoridades, estas deberán actuar de forma coordinada, intercambiar la información necesaria y determinar el ámbito material de sus respectivas actuaciones, con el fin de evitar duplicidades y garantizar el principio de non bis in idem.

Parágrafo 1º. Los procedimientos sancionatorios se adelantarán de conformidad con el régimen especial aplicable a cada sujeto, actividad y tecnología. En lo no previsto por dichos regímenes se aplicarán las disposiciones pertinentes del procedimiento administrativo sancionatorio previstas en la Ley 1437 de 2011 y las normas que la modifiquen, adicionen o sustituyan. En todo caso se garantizarán los principios de

legalidad, tipicidad, debido proceso, defensa, contradicción, proporcionalidad, razonabilidad, responsabilidad administrativa y non bis in idem.

Parágrafo 2°. Los lineamientos, protocolos, recomendaciones, guías y estándares técnicos que expidan o adopten las autoridades en desarrollo de la presente ley constituirán instrumentos para orientar su implementación, facilitar la evaluación técnica y determinar condiciones de seguridad y buenas prácticas. No obstante, dichos instrumentos no constituirán por sí solos fuente autónoma de infracciones administrativas ni fundamento exclusivo para la imposición de sanciones, salvo que desarrollen una obligación previamente establecida en la ley o en un reglamento expedido con habilitación legal suficiente.

Parágrafo 3°. La adopción de medidas sanitarias preventivas, de seguridad, suspensión, restricción, retiro, inmovilización, alerta o cese temporal del uso de un sistema no tendrá naturaleza sancionatoria cuando tenga por finalidad prevenir o controlar un riesgo grave o inminente para la vida, la salud, la seguridad del paciente o la integridad de los datos, sin perjuicio del procedimiento administrativo sancionatorio que posteriormente pueda resultar procedente.

Artículo 63. Articulación Institucional. Las autoridades y entidades competentes en materia de inteligencia artificial en salud ejercerán sus funciones de manera articulada, de conformidad con sus competencias legales.

La Superintendencia de Industria y Comercio ejercerá las competencias que le correspondan en materia de protección de datos personales, protección al consumidor y libre competencia; el Ministerio de Tecnologías de la Información y las Comunicaciones apoyará, en el marco de sus competencias, las acciones relacionadas con interoperabilidad, infraestructura y seguridad digital; el Instituto Nacional de Salud contribuirá en los asuntos relacionados con vigilancia y salud pública; y el Instituto de Evaluación Tecnológica en Salud -IETS-, o quien haga sus veces, podrá realizar o apoyar evaluaciones de tecnologías y sistemas de inteligencia artificial aplicados a la salud, de acuerdo con sus competencias.

Las entidades establecerán mecanismos y protocolos de intercambio seguro de información, reporte de incidentes y gestión coordinada de riesgos, procurando evitar duplicidades, reducir cargas administrativas y garantizar una respuesta oportuna frente a riesgos que puedan afectar la vida, la salud o la seguridad de los pacientes.

TÍTULO XI.

INNOVACIÓN, CAPACIDADES, COMPRA PÚBLICA Y COOPERACIÓN

Artículo 64. Fomento de investigación e innovación. El Gobierno Nacional en cabeza del Ministerio de Ciencia, Tecnología e Innovación o la entidad que haga sus veces, promoverá la investigación pública y privada, validación multicéntrica, repositorios seguros, estándares abiertos, emprendimiento y cooperación entre

instituciones, universidades, sociedades científicas y sector productivo, con enfoque territorial.

Artículo 65. Formación, alfabetización ética y cultura de seguridad. El Ministerio de Salud y Protección Social, el Ministerio de Educación y Ministerio Tecnologías de la Información y las Comunicaciones, en el marco de sus funciones promoverán la formación de competencias en inteligencia artificial, ética, bioética, derechos humanos, integridad científica, datos, ciberseguridad, seguridad del paciente y pensamiento crítico para profesionales, desarrolladores, directivos, pacientes, cuidadores y servidores públicos. La formación deberá prevenir la dependencia acrítica de resultados automatizados y fortalecer la capacidad de cuestionar, verificar, documentar y detener sistemas inseguros.

Artículo 66. Cooperación y confianza regulatoria. Las autoridades competentes para la implementación, inspección, vigilancia y control de lo dispuesto en la presente ley podrán establecer mecanismos de cooperación con organismos internacionales, autoridades sanitarias y regulatorias extranjeras, así como con redes y organismos técnicos especializados, para el intercambio de información, alertas sanitarias, conocimientos, metodologías y buenas prácticas relacionadas con la inteligencia artificial en salud.

Así mismo, podrán conformar mesas técnicas de carácter consultivo con participación de la academia, sociedades científicas, organizaciones de pacientes, sector tecnológico e industria, garantizando la transparencia, independencia técnica y manejo adecuado de los conflictos de interés.

TÍTULO XII. IMPLEMENTACIÓN, TRANSICIÓN Y VIGENCIA

Artículo 67. Reglamentación. El Gobierno Nacional, a través del Ministerio de Salud y Protección Social, en coordinación con las demás autoridades competentes, reglamentará la presente ley dentro de los doce (12) meses siguientes a su expedición, estableciendo las condiciones, procedimientos y mecanismos necesarios para su implementación y cumplimiento, de manera proporcional al nivel de riesgo y a la finalidad de los sistemas de inteligencia artificial en salud.

La reglamentación podrá desarrollarse de forma progresiva y escalonada, priorizando los sistemas de alto y crítico riesgo y garantizando la participación de los pacientes, profesionales de la salud, sociedades científicas, academia, sector tecnológico, industria y entidades territoriales.

Artículo 68. Financiación. La implementación de las disposiciones previstas en la presente ley se financiará con cargo a las apropiaciones presupuestales que las entidades competentes incluyan en sus respectivos presupuestos, de conformidad con sus competencias y disponibilidad de recursos.

En todo caso, las medidas derivadas de la presente ley se desarrollarán de conformidad con el Marco Fiscal de Mediano Plazo, el Marco de Gasto de Mediano Plazo y las disponibilidades presupuestales.

Artículo 69. Informe y monitoreo. Al inicio de cada legislatura, el Gobierno Nacional en cabeza del Ministerio de Salud y Protección Social, presentará a las Comisiones Séptimas Constitucionales del Congreso de la República un informe de evaluación sobre su implementación y resultados, que incluirá, como mínimo, el impacto en la innovación, la seguridad y calidad de la atención en salud, la equidad en el acceso, los incidentes y riesgos identificados, los resultados de las medidas de supervisión y control, el impacto fiscal y las capacidades institucionales desarrolladas.

El informe incluirá recomendaciones sobre la necesidad de actualizar, modificar o fortalecer el marco regulatorio, de acuerdo con la evolución tecnológica, científica y de los riesgos asociados a la inteligencia artificial en salud.

Artículo 70. Vigencia y derogatorias. La presente ley rige a partir de su publicación y deroga las disposiciones que le sean contrarias.

De los congresistas autores,

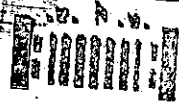

 NADIA BLEL SCAFF
 Senadora de la República
 AUTORA

Senador de la República
 COAUTOR

Senador de la República
 COAUTOR

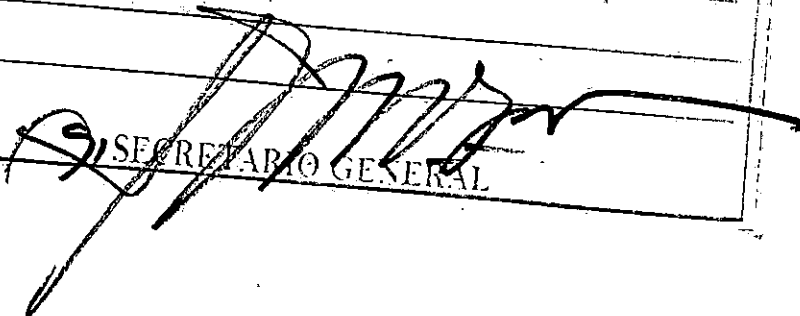
Senador de la República
 COAUTOR

Senador de la República
 COAUTOR



SENADO DE LA REPÚBLICA
SECRETARÍA GENERAL

EL día 01 de Sept del año 2020
Ha sido presentado en este despacho el
Proyecto de ley X Acto legislativo _____
No. 216/20 Con su correspondiente
Exposición de Motivos, suscrito Por: _____


SECRETARIO GENERAL

PROYECTO DE LEY No. _____ DE 2026 SENADO DE LA REPÚBLICA.

Por medio del cual se establecen los lineamientos normativos éticos y de integridad científica para la gobernanza de sistemas de inteligencia artificial en el sector salud, se garantiza la seguridad del paciente, la protección de los datos de salud, la autonomía profesional y se dictan otras disposiciones.

La presente iniciativa fue elaborada con acompañamiento del comité técnico, científico, clínico, ético, bioético, epidemiológico, tecnológico, jurídico y gremial. La participación del comité técnico tiene carácter asesor¹.

EXPOSICIÓN DE MOTIVOS

La exposición de motivos que fundamenta la presente iniciativa estará estructurada de la siguiente manera:

1. Fundamento Constitucional y Antecedentes legales.
2. Objeto de la iniciativa
3. Justificación.
4. Contenido de la iniciativa.
5. Manifestación de conflicto de interés.
6. Impacto fiscal.
7. Proposición
8. Articulado.

1. FUNDAMENTO CONSTITUCIONAL Y ANTECEDENTES LEGALES.

Constitución Política.

La iniciativa desarrolla los artículos 1, 2, 13, 15, 16, 20, 29, 44, 48, 49, 74, 78, 83, 95, 209, 333, 334 y 365 de la Constitución Política. De ellos se derivan la protección de la dignidad humana; la efectividad de los derechos; la igualdad y no discriminación; la intimidad y el habeas data; el libre desarrollo de la personalidad; el debido proceso; la protección reforzada de niños, niñas y adolescentes; el derecho fundamental a la salud; los derechos de consumidores y usuarios; la buena fe; la

¹ Integrantes del Comité: Adrián Gonzalo Hernández Aldana, Carmen Amelia de los Reyes Victoria, Edgar Antonio Ibáñez Pinilla, Jaime Carmona Clavijo, Favio Cala Vitery, Johnny Fabian Córdoba Ipuz, José Luis Reyes Villamizar, José Sinay Arévalo Leal, Juan Esteban Martínez, Juan Manuel Utria Molina, Miguel Ángel Murcia Rodríguez, Roberto Baquero Haeblerlin, Wanderley Augusto Arias Ortiz. Ver Anexo 1.

función administrativa; la intervención estatal en la economía y la prestación eficiente de los servicios públicos.

El artículo 49 impone al Estado el deber de organizar, dirigir y reglamentar la prestación de servicios de salud conforme a los principios de eficiencia, universalidad y solidaridad. Cuando una tecnología puede influir en diagnósticos, tratamientos, priorización, cobertura o seguridad clínica, el legislador está habilitado para establecer controles proporcionales, estándares de calidad y responsabilidades.

El artículo 15 exige una protección reforzada de los datos de salud, genéticos y biométricos. Los sistemas de inteligencia artificial amplifican los riesgos de inferencia, reutilización, combinación de bases, reidentificación, vigilancia y discriminación, por lo que la regulación general de datos debe complementarse con reglas sanitarias específicas. La propuesta tiene naturaleza de ley ordinaria sectorial. No redefine el núcleo esencial del derecho fundamental a la salud ni sustituye el régimen estatutario de protección de datos; desarrolla deberes técnicos, sanitarios, institucionales y de prestación de servicios. Esta delimitación preserva la competencia del legislador ordinario y evita invadir materias reservadas a ley estatutaria.

Antecedentes legales.

Colombia dispone de un conjunto normativo relevante pero fragmentado. La Ley 23 de 1981 regula la ética médica; la Ley 1581 de 2012, el tratamiento de datos personales; la Ley 1712 de 2014, la transparencia; la Ley Estatutaria 1751 de 2015, el derecho fundamental a la salud; la Ley 1419 de 2010 y sus modificaciones, la telesalud; la Ley 2015 de 2020, la historia clínica electrónica interoperable; la Ley 2108 de 2021, el acceso a internet como servicio público esencial; y el Decreto 780 de 2016 compila la regulación del sector salud. A ello se suman las normas sobre dispositivos médicos, investigación clínica, habilitación, calidad, seguridad del paciente y responsabilidad.

✓ CONPES 3975 de 2019.

El Documento CONPES 3975 de 2019 trazó la política de transformación digital e inteligencia artificial. Posteriormente, el CONPES 4144 de 2025 adoptó la Política Nacional de Inteligencia Artificial, orientada al fortalecimiento de capacidades, gobernanza, investigación, infraestructura, talento y uso ético y sostenible. Estos instrumentos ofrecen una hoja de ruta, pero no reemplazan un régimen legal vinculante para riesgos clínicos.

Durante 2025 y 2026 el Congreso ha avanzado en un proyecto general de inteligencia artificial identificado como Proyecto de Ley 043 de 2025 Senado - 324 de 2025

Cámara. La presente iniciativa se concibe como ley especial sanitaria y deberá armonizarse con el texto general que resulte aprobado, aplicando el principio de especialidad respecto de seguridad clínica, tecnologías sanitarias, datos de salud y prestación de servicios.

2. OBJETO DE LA INICIATIVA.

Establecer el marco normativo especial para la gobernanza, desarrollo, entrenamiento, validación, importación, comercialización, implementación, uso, actualización, supervisión, vigilancia y retiro de sistemas de inteligencia artificial en salud, con el fin de proteger la vida, la salud, la dignidad humana, la autonomía, la igualdad, la privacidad, la seguridad del paciente y la integridad científica, y promover innovación segura, responsable y sostenible.

3. JUSTIFICACIÓN.

La inteligencia artificial constituye una de las transformaciones tecnológicas más relevantes del siglo XXI. En salud, sus aplicaciones comprenden el apoyo diagnóstico, el análisis de imágenes y señales, la predicción de riesgos, la medicina de precisión, la investigación biomédica, el descubrimiento y seguimiento de medicamentos, la gestión hospitalaria, la vigilancia epidemiológica, la telesalud y la automatización de procesos administrativos.

Estas capacidades pueden ampliar el acceso, mejorar la oportunidad, reducir errores evitables y fortalecer la toma de decisiones basada en evidencia. No obstante, cuando un sistema algorítmico interviene en decisiones que comprometen la vida, la integridad, el tratamiento, el acceso a servicios o el uso de datos sensibles, deja de ser una herramienta tecnológica neutral y se convierte en un objeto de interés sanitario, ético y jurídico.

El presente proyecto establece un régimen sectorial especial, basado en riesgo y en el ciclo de vida, que articula la regulación sanitaria, la protección de datos, la ética clínica, la seguridad digital, la investigación, la responsabilidad y la innovación. Su finalidad no es frenar la transformación digital, sino crear condiciones de confianza para que la inteligencia artificial se desarrolle y use de manera segura, transparente, equitativa y responsable.

3.1 ESTADO DEL ARTE Y BENEFICIOS DE LA IA EN SALUD.

La evidencia científica y la experiencia institucional muestran que la IA puede mejorar la detección de patrones en radiología, patología, dermatología, oftalmología, cardiología y medicina nuclear, entre otras especialidades y de la medicina en general; apoyar la estratificación de riesgo; acelerar la investigación; optimizar turnos, camas y recursos; fortalecer la vigilancia epidemiológica y ampliar

capacidades en zonas con escasez de especialistas. Su valor depende, sin embargo, de la calidad de los datos, la pertinencia clínica, el diseño del flujo de trabajo, la capacitación, la interoperabilidad y la supervisión humana. Una buena métrica técnica no equivale por sí sola a beneficio clínico.

Riesgos del uso no regulado.

- Daño clínico por falsos negativos, falsos positivos, recomendaciones incorrectas o automatización excesiva.
- Discriminación algorítmica por datos no representativos o variables sustitutas de categorías protegidas.
- Pérdida de autonomía del paciente y del profesional por dependencia acrítica del sistema.
- Filtración, uso secundario incompatible o reidentificación de datos sensibles.
- Alucinaciones y contenido sintético engañoso en modelos generativos.
- Ataques cibernéticos, manipulación de entradas, envenenamiento de datos o cambios no autorizados.
- Generación, alteración o difusión de contenido sintético clínico engañoso, incluidos deepfakes médicos, falsificación de imágenes radiológicas, modificación fraudulenta de señales, informes o registros asistenciales y suplantación de profesionales o pacientes.
- Concentración tecnológica, dependencia de proveedores y barreras de interoperabilidad.
- Dificultad probatoria y ausencia de reparación cuando no existe trazabilidad.

No regular también tiene costos: incertidumbre para la inversión, fragmentación de estándares, compras públicas deficientes, pérdida de confianza y adopción desigual. La regulación proporcional crea seguridad jurídica y favorece la innovación responsable.

La inteligencia artificial deberá entenderse como una herramienta de apoyo y consulta para el ejercicio de las profesiones de la salud. Sus resultados no serán de seguimiento obligatorio y no podrán desplazar la valoración integral del caso, el juicio clínico ni la autonomía profesional. El profesional de la salud conservará la responsabilidad por las decisiones que adopte dentro del ámbito de sus competencias, sin perjuicio de la responsabilidad que corresponda al proveedor, fabricante, implementador u otros actores por defectos, fallas, omisiones o riesgos bajo su control.

En los sistemas robóticos y brazos robotizados destinados a procedimientos diagnósticos, intervencionistas, quirúrgicos o terapéuticos, la inteligencia artificial no podrá operar de manera autónoma sobre una persona. Su utilización exigirá supervisión directa y continua de un médico especialista competente, habilitado y entrenado, con capacidad real de intervenir, detener o asumir el control inmediato.

Antes de su uso en seres humanos, el sistema deberá superar entrenamiento, simulación y validación preclínica mediante modelos anatómicos, componentes anatómicos, simuladores, fantasmas, especímenes o métodos equivalentes científicamente aceptados, de acuerdo con su finalidad y nivel de riesgo.

3.2 FUNDAMENTO ÉTICO Y BIOÉTICO.

La ética y la bioética constituyen ejes estructurales y jurídicamente exigibles del proyecto. La inteligencia artificial aplicada a la salud debe orientarse por el respeto de la dignidad humana, la autonomía, la beneficencia, la no maleficencia, la justicia, la solidaridad, la equidad, la privacidad, la integridad, la precaución, la responsabilidad y el interés superior de las personas y comunidades.

La evaluación bioética no se limita a la investigación clínica. Debe acompañar todo el ciclo de vida del sistema: definición del problema, selección y gobernanza de datos, diseño, entrenamiento, validación, adquisición, implementación, uso asistencial, actualización, vigilancia y retiro. Deberá examinar, como mínimo, la proporcionalidad entre beneficio y riesgo, los efectos distributivos, la posible discriminación, la autonomía del paciente, el impacto en la relación clínica, la protección de poblaciones vulnerables y la existencia de alternativas menos intrusivas.

El control humano debe ser real, competente y oportuno. No basta con la presencia formal de una persona cuando esta carece de información, autoridad, tiempo o capacidad para comprender, controvertir o detener el resultado algorítmico. La supervisión deberá diseñarse para prevenir la automatización irreflexiva, el sesgo de autoridad tecnológica y la dilución de responsabilidades.

Los comités institucionales de ética, bioética e investigación, según corresponda, deberán participar en la evaluación de sistemas de alto y crítico riesgo. Su intervención no sustituirá las competencias sanitarias ni la responsabilidad de proveedores e implementadores, pero aportará deliberación interdisciplinaria, participación social y vigilancia sobre conflictos de interés, justicia distributiva, consentimiento, transparencia y protección de derechos.

3.3 REGULACIÓN INTERNACIONAL COMPARADA

El análisis de los marcos oficiales aportados a la iniciativa muestra una convergencia internacional en cinco componentes: clasificación por riesgo, validación previa, gobernanza de datos, supervisión humana y vigilancia durante el ciclo de vida.

Jurisdicción u organismo	Instrumento de referencia	Elemento incorporado
Unión Europea	Reglamento (UE) 2024/1689 – AI Act	Clasificación de riesgo, obligaciones para alto riesgo, transparencia,

Jurisdicción u organismo	Instrumento de referencia	Elemento incorporado
		supervisión humana y gobernanza.
Estados Unidos	FDA: IA en funciones de software de dispositivos, ciclo de vida y planes predeterminados de cambio	Evidencia regulatoria, gestión de actualizaciones, desempeño real y vigilancia posmercado.
OMS	Ética y gobernanza de la IA para la salud; orientación sobre modelos multimodales	Derechos humanos, seguridad, transparencia, inclusión, rendición de cuentas y control de modelos generativos.
IMDRF	Software as a Medical Device: Clinical Evaluation	Asociación clínica válida, validación analítica y desempeño clínico.
Canadá	Guía previa a mercado para dispositivos médicos habilitados por aprendizaje automático	Evidencia, riesgo, cambios y ciclo de vida.
Reino Unido	Programa de cambio para software e IA como dispositivo médico	Reforma de clasificación, seguridad, desempeño y vigilancia.
Singapur	Artificial Intelligence in Healthcare Guidelines 2.0	Gobernanza para adopción clínica e institucional.
Corea del Sur, Japón, China y Australia	Guías y programas regulatorios de autoridades sanitarias	Clasificación, ensayos, sesgos, software médico y vigilancia.
UNESCO y OCDE	Recomendación sobre ética de la IA y Principios de IA	Derechos, equidad, transparencia, robustez y responsabilidad.

Situación regional latinoamericana.

En América Latina predomina una combinación de leyes de datos personales, regulación de dispositivos médicos, estrategias nacionales y proyectos generales de IA. Brasil, Chile, México, Argentina, Perú y Uruguay han desarrollado iniciativas de gobernanza o proyectos legislativos que suelen considerar la salud como ámbito de alto impacto. El panorama confirma la oportunidad para que Colombia adopte una regulación sanitaria especializada, interoperable con estándares internacionales y adaptada a su sistema de aseguramiento y prestación.

3.4 MODELO REGULATORIO PROPUESTO.

El Modelo regulatorio propuesto hace especial énfasis en:

- Clasificación de riesgo mínimo, limitado, alto y crítico.
- Prohibición de decisiones exclusivamente automatizadas con efectos clínicos o de acceso significativos.
- Validación analítica, técnica y clínica, incluida validación local cuando la evidencia externa no sea representativa.
- Registro nacional de sistemas de alto y crítico riesgo y articulación con autorización sanitaria del INVIMA.

- Evaluación institucional previa, comité de gobernanza y monitoreo local.
- Gobernanza de datos, interoperabilidad, ciberseguridad y trazabilidad.
- Reglas específicas para modelos generativos, agentes conversacionales, contenido sintético y filtros de seguridad para prevenir, detectar, autenticar y trazar deepfakes médicos, falsificación de imágenes radiológicas y otras alteraciones clínicas engañosas.
- Responsabilidad distribuida según el rol y control efectivo sobre el riesgo.
- Sandbox regulatorio, investigación responsable, formación y compra pública segura.

Regulación reforzada de brazos robotizados y robots clínicos, con prohibición de operación autónoma sobre seres humanos, supervisión médica especializada y validación preclínica anatómica obligatoria.

La arquitectura institucional evita crear una nueva entidad. El Ministerio de Salud y Protección Social ejercerá rectoría; el INVIMA, control sanitario; la Superintendencia Nacional de Salud, vigilancia sobre actores del sistema; la Superintendencia de Industria y Comercio, competencias en datos, consumo y competencia; el Ministerio TIC, interoperabilidad y seguridad digital; y el Instituto Nacional de Salud y el IETS apoyarán salud pública y evaluación de tecnologías.

4. CONTENIDO DE LA INICIATIVA.

- Título I. Disposiciones generales
- Título II. Principios y derechos
- Título III. Clasificación por riesgo y prácticas prohibidas
- Título IV. Evaluación, validación y autorización
- Título V. Gobernanza de datos, interoperabilidad y ciberseguridad
- Título VI. IA generativa y modelos de propósito general
- Título VII. Obligaciones de los actores
- Título VIII. Investigación, bioética e integridad científica
- Título IX. Responsabilidad, auditoría y garantías
- Título X. Autoridades, vigilancia y sanciones
- Título XI. Innovación, capacidades y compra pública
- Título XII. Implementación, transición y vigencia

5. IMPACTO FISCAL.

Respecto del concepto impacto fiscal que los proyectos de ley pudieran generar, la Corte ha dicho:

"Las obligaciones previstas en el artículo 7º de la Ley 819 de 2003 constituyen un parámetro de racionalidad legislativa, que está encaminado a cumplir propósitos constitucionalmente valiosos, entre ellos el orden de las finanzas públicas, la estabilidad macroeconómica y la aplicación efectiva de las leyes. Esto último en tanto un estudio previo de la compatibilidad entre el contenido del proyecto de ley y las proyecciones de la política económica, disminuye el margen de incertidumbre respecto de la ejecución material de las previsiones legislativas. El mandato de adecuación entre la justificación de los proyectos de ley y la planeación de la política económica, empero, no puede comprenderse como un requisito de trámite para la aprobación de las iniciativas legislativas, cuyo cumplimiento recaiga exclusivamente en el Congreso. Lo anterior, en tanto (i) el Congreso carece de las instancias de evaluación técnica para determinar el impacto fiscal de cada proyecto, la determinación de las fuentes adicionales de financiación y la compatibilidad con el marco fiscal de mediano plazo; y (ii) aceptar una interpretación de esta naturaleza constituiría una carga irrazonable para el legislador y otorgaría un poder correlativo de veto al Ejecutivo, a través del Ministerio de Hacienda, respecto de la competencia del Congreso para hacer las leyes. Un poder de este carácter, que involucra una barrera en la función constitucional de producción normativa, se muestra incompatible con el balance entre los poderes públicos y el principio democrático. Si se considera dicho mandato como un mecanismo de racionalidad legislativa, su cumplimiento corresponde inicialmente al Ministerio de Hacienda y Crédito Público, una vez el Congreso haya valorado, mediante las herramientas que tiene a su alcance, la compatibilidad entre los gastos que genera la iniciativa legislativa y las proyecciones de la política económica trazada por el Gobierno. (...). El artículo 7º de la Ley 819/03 no puede interpretarse de modo tal que la falta de concurrencia del Ministerio de Hacienda y Crédito Público dentro del proceso legislativo, afecte la validez constitucional del trámite respectivo". (Sentencia C-315 de 2008).

Como lo ha resaltado la Corte, si bien compete a los miembros del Congreso la responsabilidad de estimar y tomar en cuenta el esfuerzo fiscal que el proyecto bajo estudio puede implicar para el erario público, es claro que es el Poder Ejecutivo, y al interior de aquel, el Ministerio de Hacienda y Crédito Público, el que dispone de los elementos técnicos necesarios para valorar correctamente ese impacto, y a partir de ello, llegado el caso, demostrar a los miembros del órgano legislativo la inviabilidad financiera de la propuesta que se estudia. En consecuencia, sin perjuicio de que el Proyecto de Ley continúe su trámite en el Congreso los autores acordamos solicitar concepto de la presente iniciativa legislativa al Ministerio de Hacienda, el cual deberá adjuntarse al Proyecto una vez llegue la respuesta al mismo.

6. CONFLICTOS DE INTERÉS.

Respecto del conflicto de intereses teniendo en cuenta el artículo 3º de la Ley 2003 de 2019, por la cual se modifica parcialmente la Ley 5ª de 1992 y se dictan otras disposiciones, que modifica el artículo 291 de la misma Ley, que establece la obligación al autor del proyecto presentar la descripción de las posibles

circunstancias o eventos que podrían generar un conflicto de interés para la discusión y votación del proyecto, siendo estos, criterios guías para que los congresistas tomen una decisión en torno a si se encuentran en una causal de impedimento, se considera que frente al presente proyecto, no se generan conflictos de interés alguno, puesto que las disposiciones aquí contenidas son generales y no generan beneficios particulares, actuales y directos.

Sin perjuicio de lo anterior, se debe tener en cuenta que la descripción del posible conflicto de interés que se pueda presentar frente al trámite del presente proyecto de ley, no exime del deber del Congresista de identificar causales adicionales.

7. PROPOSICIÓN.

Por las razones expuestas, solicitamos al honorable Congreso de la República dar trámite y aprobar el presente Proyecto de Ley, mediante el cual se establece el marco normativo especial para la inteligencia artificial en salud en Colombia.

De los honorables congresistas,



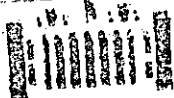
NADIA BLEL SCAFF
Senadora de la República
AUTORA

Senador de la República
COAUTOR

Senador de la República
COAUTOR

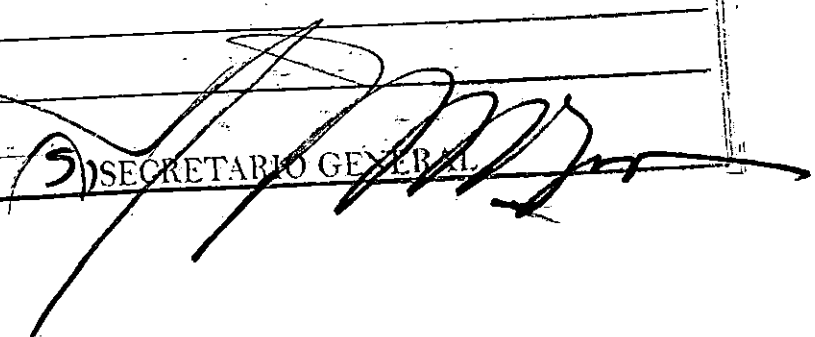
Senador de la República
COAUTOR

Senador de la República
COAUTOR



SENADO DE LA REPÚBLICA
SECRETARÍA GENERAL

EL día 01 de Sept del año 2026
Ha sido presentado en este despacho el
Proyecto de ley X Acto legislativo
No. 216/26 Con su correspondiente
Exposición de Motivos, suscrito Por:


(5) SECRETARIO GENERAL

ANEXO 1. COMITÉ TÉCNICO, CIENTÍFICO, ÉTICO, BIOÉTICO Y JURÍDICO

Adrián Gonzalo Hernández Aldana, Ingeniero Industrial, Máster en Dirección de Centros Educativos, Especialista en Psicología y Comportamiento del Consumidor e Investigación de mercados, Especialista en Mercadeo, Minor en Informática, Minor en Gerencia de Proyectos, Minor en Justicia Restaurativa y Convivencia Ciudadana. Actual Gerente General de la Corporación CIFEP y Director Ejecutivo de la Corporación COAI. Coautor del libro: Revolución en Salud: INNOVACIÓN Y EMPRENDIMIENTO (2025), Gerente General de ALAS CBG, empresa consultora y aceleradora de negocios, Gerente General y Representante legal de STARPROT, empresa de reubicación transfronteriza de servicios profesionales, técnicos y tecnológicos del talento humano en salud en el exterior; evaluador ad hoc premio galardón COOMEVA; evaluador adhoc Premio Nacional de Emprendimiento, Innovación y Gestión (PNEIG)

Carmen Amelia de los Reyes Victoria, Médica especialista en medicina nuclear. Máster en Manejo de Proyectos. Profesora emérita del Instituto Nacional de Cancerología. Actual presidente de ACMNIM : La Asociación Colombiana de Medicina Nuclear e Imágenes Moleculares. Expresidente de ALASBIMMN: La Asociación Latinoamericana de Sociedades de Biología, Imágenes Moleculares y Medicina Nuclear. Directora Médica y de Proyectos de NUCLEOFARMA.

Edgar Antonio Ibáñez Pinilla, Doctor en Estudios Políticos, Universidad Externado de Colombia; Magíster en Epidemiología Clínica, Universidad Nacional de Colombia; Especialista en Estadística, Universidad Nacional de Colombia, Especialista en Docencia Universitaria, Universidad El Bosque. Coordinador de Investigación, Facultad de Medicina, Universidad El Bosque. Profesor de los programas de Maestría en Epidemiología, Salud Pública, Salud Mental Comunitaria, Salud Sexual y Reproductiva, Enfermería en Cuidados Paliativos y Doctorado en Salud Pública, Facultad de Medicina, Universidad El Bosque. Investigador Senior MinCiencias.

Favio Cala Vitery, Director del Doctorado en Modelado en Política y Gestión Pública y profesor titular de la Universidad de Bogotá Jorge Tadeo Lozano; físico de la Universidad Industrial de Santander; magíster en Física Teórica, magíster en Historia de la Ciencia y doctor en Filosofía por la Universidad Autónoma de Barcelona. Coordinador institucional del proyecto Jean Monnet HEMISPHERES sobre gobernanza tecnológica e IA. Investigador sénior de MinCiencias.

Jaime Carmona Clavijo, Médico especialista en Radiología e Imágenes Diagnósticas, Universidad Favaloro, Argentina; Especialista en Medicina Nuclear e Imágenes Híbridas PET/CT y SPECT/CT, Universidad de Chile; formación en inteligencia artificial aplicada a la medicina, orientada a la innovación y optimización de los

servicios de imágenes diagnósticas; Director Médico de IMADExA S.A.S; Director Médico de Gamanuclear LTDA; Trayectoria profesional en Colombia, Chile y Argentina, experiencia en radiología, medicina nuclear, telerradiología y dirección médica.

Johnny Fabian Córdoba Ipuz, Ingeniero de sistemas, líder de informática y tecnología del grupo corporativo SCCOT; líder de innovación e informática del Centro Latinoamericano de Entrenamiento Médico e investigación CLEMI; Gestor y fundador del centro de convenciones virtual de la sociedad colombiana de ortopedia; líder de sistemas y plataformas digitales de la federación latinoamericana de ortopedia y traumatología SLAOT Federación, y la Federación Latinoamericana de Medicina y Cirugía de la Pierna y el Pie FLAMECIPP.

José Luis Reyes Villamizar. Abogado, Pontificia Universidad Javeriana. Máster en Administración Pública y Negocios Internacionales, The George Washington University (becario Fulbright); exasesor legal del Despacho SIC y de Despachos de los Ministros de Justicia y de Comercio; asesor empresarial y gremial; consultor y docente en asuntos legales, corporativos, de propiedad intelectual (especialmente, en las áreas de patentes de invención, signos distintivos, derechos de autor y secretos empresariales), derecho de la salud, contratación y negocios internacionales. Abogado litigante en materias relacionadas con la contratación civil y mercantil, la propiedad intelectual y el derecho de la competencia.

José Sinay Arévalo Leal, médico de la Escuela Colombiana de Medicina y especialista en medicina nuclear de la Universidad Javeriana. Especialista y magíster en bioética y especialista en filosofía de la ciencia. Black Belt en Lean Health Care. Cursos de Doctorado en Bioética y Biojurídica Universidad Rey Juan Carlos de Madrid. . Profesor de la Universidad del Rosario (escuelas de medicina, Jurisprudencia y administración) y de la Fundación Universitaria de Ciencias de la Salud -FUCS- en medicina nuclear. Magistrado del Tribunal Nacional de Ética Médica

Juan Esteban Martínez, ingeniero industrial, Universidad de los Andes; empresario en los sectores de HealthTech e inteligencia artificial; Experiencia y trayectoria en el sector Fintech en Latinoamérica.

Juan Manuel Utria Molina, ingeniero industrial de la Universidad del Norte, especialista en gerencia de proyectos, Universidad de la Costa, maestrante en gerencia de proyectos. Profesional experto en dirección de proyectos estratégicos, transformación organizacional, optimización de procesos, planeación financiera y excelencia operacional en manufactura, salud y servicios. Experto en analítica de datos bajo metodologías PMI, Scrum y Lean Six Sigma. Evaluador del Premio Coomeva 2026.

Miguel Ángel Murcia Rodríguez, médico Especialista en ortopedia y traumatología. Especialista en Docencia Universitaria, Certificación en calidad en atención en salud, Expresidente de la Sociedad Colombiana de Cirugía Ortopedia y Traumatología, Expresidente de la Asociación Colombiana de Sociedades Científicas, Miembro Fundador del Colegio Médico Colombiano. Exdirector general Clínica Centenario. Ex Director General Hospital Universitario Clínica San Rafael de Bogotá

Roberto Baquero Haeblerlin, Médico especialista en oftalmología, docente del programa de oftalmología de Unisanitas, expresidente de la Sociedad Colombiana de Oftalmología, Expresidente del Colegio Médico Colombiano. Miembro de la Gran Junta Médica que fijó las bases de la Ley 1751, Ley Estatutaria de la Salud. Maestría de Bioética, Maestría en Liderazgo y Dirección de Centros educativos, Gerente General de la Corporación COAI y Director Ejecutivo de la Corporación CIFEP

Wanderley Augusto Arias Ortiz, Candidato a Doctor en Modelado en Política y Gestión Pública de la Universidad Jorge Tadeo Lozano, Magíster en Epidemiología, Universidad El Bosque; Especialista en Estadística Aplicada, Especialista en Docencia Universitaria, Maestrante en Salud Digital, Universidad Europea de Madrid; Profesional en Instrumentación Quirúrgica. Coordinador del Centro de Investigaciones de la Facultad de Medicina y Ciencias de la Salud de la Universidad de los Andes. Profesor de los programas de Maestría en Informática Biomédica, Fisiología Traslacional, Farmacología, Epidemiología y Administración en Salud de la Facultad de Medicina y de la Maestría en Educación Inclusiva e Intercultural de la Facultad de Educación de la Universidad El Bosque. Investigador Asociado MinCiencias, Miembro del proyecto Jean Monnet HEMISPHERES sobre gobernanza y tecnologías.

ANEXO 2. MATRIZ ORIENTADORA DE CLASIFICACIÓN.

Nivel	Ejemplos	Impacto	Obligaciones mínimas	Control principal
Mínimo	Agenda, logística, transcripción sin finalidad clínica	Bajo	Seguridad, privacidad, información veraz	Implementador
Limitado	Educación, orientación general, apoyo administrativo con impacto menor	Moderado y reversible	Transparencia, documentación, revisión y reporte	Minsalud / Supersalud
Alto	Diagnóstico, triage, pronóstico, tratamiento, cobertura, dispositivo médico	Significativo	Validación, registro, evaluación de impacto, auditoría y vigilancia	INVIMA / Supersalud
Crítico	Control terapéutico autónomo o sistemas con alto potencial de daño	Muerte o daño grave	Autorización expresa, supervisión intensiva, contingencia, seguro cuando proceda	INVIMA

ANEXO 3. CORRESPONDENCIA ENTRE RIESGOS Y SALVAGUARDAS.

Riesgo	Salvaguarda principal	Artículos relacionados
Error clínico	Validación contextual, supervisión, vigilancia y contingencia	8, 22 a 31
Sesgo y discriminación	Evaluación por subgrupos, calidad de datos y revisión humana	12, 13, 24, 34
Privacidad y reidentificación	Gobernanza, minimización, uso secundario controlado y seguridad	32 a 39
Alucinaciones generativas	Verificación humana, fuentes, límites y escalamiento	40 a 44
Opacidad y dificultad probatoria	Información, trazabilidad, auditoría y carga dinámica	9, 38, 57, 59

Riesgo	Salvaguarda principal	Artículos relacionados
Dependencia tecnológica	Interoperabilidad, portabilidad y compra pública responsable	36, 39, 70
Deepfakes médicos y falsificación de imágenes	Filtros de seguridad, autenticidad, procedencia, conservación del original, detección de manipulación y reporte de incidentes	20, 22, 29, 42, 45, 62
Operación robótica autónoma o insegura	Supervisión médica especializada, validación anatómica preclínica, límites de autonomía, control manual y parada de emergencia	19, 20, 22 a 24, 29, 44A, 45, 47, 51, 62

REFERENCIAS NORMATIVAS Y TÉCNICAS

- Constitución Política de Colombia.
- Ley 23 de 1981, por la cual se dictan normas en materia de ética médica.
- Ley 1581 de 2012, régimen general de protección de datos personales.
- Ley 1712 de 2014, transparencia y acceso a la información pública.
- Ley Estatutaria 1751 de 2015, derecho fundamental a la salud.