

CIRCULAR EXTERNA N° xxxx DE 2026**Bogotá, D.C.,****PARA: SERVIDORES PÚBLICOS, CONTRATISTAS, DEMÁS COLABORADORES DE LA ENTIDAD Y TERCEROS QUE MANTENGAN CUALQUIER TIPO DE RELACIÓN O VÍNCULO CON EL INVIMA****DE: DIRECCIÓN GENERAL****ASUNTO: LINEAMIENTOS PARA EL USO DE LA INTELIGENCIA ARTIFICIAL****FECHA: 23 DE JULIO DE 2026**

Estimados servidores, contratistas, colaboradores y demás destinatarios:

Reciban un cordial saludo:

En el marco del Documento CONPES 4144 de 2025 y de la Directiva Conjunta 007 de 2025, y con el fin de asegurar un uso confiable, ético, seguro y responsable de la inteligencia artificial que preserve la seguridad de la información, la protección de los datos personales y los derechos de autor en el entorno digital y físico de la Entidad, la Dirección General imparte los siguientes lineamientos:

1. OBJETIVO

Establecer los lineamientos para el uso y aplicación de la inteligencia artificial que fortalezcan el desarrollo e impulsen las actividades del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, preservando la seguridad de la información, la protección de los datos personales y la protección de los derechos de autor, bajo condiciones de uso confiable en su entorno digital y físico, a través de una adecuada gestión de uso, riesgos y servicios asociados, y demás requisitos legales que rigen las funciones del Instituto.

2. ALCANCE

Los presentes lineamientos aplican a la totalidad de las dependencias del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, así como a todos sus procesos institucionales. Son de obligatorio cumplimiento para los servidores públicos, contratistas y demás colaboradores de la Entidad en el marco de sus funciones, obligaciones y actividades, así como para los terceros que en el desarrollo de sus actividades que mantengan cualquier tipo de relación o vínculo jurídico con el Instituto y tengan acceso a sus sistemas de información, recursos tecnológicos o activos digitales, estos lineamientos serán exigibles en la medida en que hayan sido incorporados mediante

cláusulas, obligaciones, anexos o disposiciones expresas del respectivo contrato, convenio, acuerdo o instrumento jurídico que regule la relación con el Invima

3. MARCO NORMATIVO Y DOCUMENTOS DE REFERENCIA

Los presentes lineamientos se fundamentan, entre otras, en las siguientes disposiciones:

- Constitución Política de Colombia de 1991.
- Ley 23 de 1982, sobre derechos de autor.
- Decisión Andina 351 de 1993, régimen común sobre derecho de autor y derechos conexos.
- Ley 1273 de 2009, sobre protección de la información y de los datos.
- Ley 1474 de 2011, Estatuto Anticorrupción.
- Ley 1581 de 2012, régimen general de protección de datos personales.
- Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2012.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 2573 de 2014, en materia de Gobierno en Línea.
- Resolución 500 de 2021 del MinTIC, Modelo de Seguridad y Privacidad de la Información.
- Decreto 1263 de 2022 y Decreto 338 de 2022, en materia de seguridad digital.
- Decreto 767 de 2022, política de Gobierno Digital.
- Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio.
- Documento CONPES 4144 de 2025.
- Directiva Conjunta 007 de 2025 de la Procuraduría General y la Defensoría del Pueblo.
- Guía Ética para la Implementación, Desarrollo y Uso de Sistemas de Inteligencia Artificial en Entidades Públicas de Colombia.

4. PRINCIPIOS

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, está comprometido con la protección y promoción de la salud de la población mediante la gestión del riesgo asociada al consumo y uso de alimentos, medicamentos, dispositivos médicos y demás productos objeto de vigilancia sanitaria. Para procurar la prestación óptima, continua y segura de sus servicios y el cumplimiento de sus procesos de vigilancia y control sanitario, el Instituto asegura la protección de la información y de los datos personales mediante un proceso permanente de gestión de riesgos que permite identificar, evaluar y tratar los riesgos —incluidos los derivados del uso de la inteligencia artificial— estableciendo los controles necesarios para que los niveles de exposición se mantengan dentro de los límites definidos por la Alta Dirección. Los presentes lineamientos se rigen por los siguientes principios:

4.1. Principios éticos para el uso de la inteligencia artificial

- **Proporcionalidad e inocuidad:** el alcance de los procesos de IA no debe exceder aquello que sea necesario para lograr sus objetivos legítimos y debe ser apropiado

al contexto en que se desenvuelva. Si existe riesgo de daño a las personas, a los derechos humanos, a las comunidades o al medio ambiente, deben implementarse evaluaciones de riesgo y medidas preventivas. Las decisiones finales con impacto irreversible o de vida o muerte deben ser tomadas por un ser humano. La IA no debe usarse para calificación social ni para vigilancia masiva.

- **Seguridad y protección:** deben evitarse y eliminarse los daños no deseados (riesgos de seguridad) y las vulnerabilidades a ataques (riesgos de protección) a lo largo del ciclo de vida de la IA, para garantizar la seguridad de las personas, del medio ambiente y de los ecosistemas.
- **Derecho a la intimidad y protección de datos:** los datos para sistemas de IA deben ser recolectados, usados, compartidos, archivados y eliminados conforme al ordenamiento vigente y a marcos de protección de datos y gobernanza robustos, aplicando el principio de privacidad desde el diseño.
- **Supervisión y decisión humana:** la responsabilidad ética y legal de las decisiones basadas en IA siempre debe ser atribuible a personas o entidades legales. La supervisión humana es indispensable y las decisiones de vida o muerte no deben cederse a los sistemas de IA.
- **Transparencia y explicabilidad:** constituyen requisitos fundamentales para el respeto de los derechos humanos y de los principios éticos. La transparencia permite la rendición de cuentas y la posibilidad de impugnar decisiones; la explicabilidad implica hacer comprensibles, para todos, los resultados y el funcionamiento de los sistemas de IA, de manera proporcional a su impacto y contexto.
- **Responsabilidad y rendición de cuentas:** los actores de la IA deben respetar y promover los derechos humanos y la protección del medio ambiente, asumiendo su responsabilidad ética y legal. Deben desarrollarse mecanismos de supervisión, evaluación de impacto, auditoría y debida diligencia que aseguren la rendición de cuentas y la trazabilidad de los sistemas de IA.

4.2. Principios de seguridad de la información

- **Disponibilidad:** garantía de que la información y los recursos asociados sean accesibles y utilizables de manera oportuna por las entidades, usuarios o procesos debidamente autorizados, cuando así se requiera.
- **Confidencialidad:** propiedad que asegura que la información no sea divulgada ni puesta a disposición de personas, entidades o procesos no autorizados, protegiendo su acceso de manera adecuada.
- **Integridad:** propiedad que salvaguarda la exactitud, consistencia y completitud de la información y de sus métodos de procesamiento, evitando modificaciones no autorizadas.

- **Autenticidad:** propiedad que garantiza que la identidad de un sujeto, sistema, recurso o información es válida y corresponde a la declarada, asegurando la confiabilidad en las interacciones y transacciones.

5. CLASIFICACIÓN DE LOS SISTEMAS DE IA SEGÚN EL NIVEL DE RIESGO Y EVALUACIÓN DE IMPACTO ALGORÍTMICO

En aplicación del principio de proporcionalidad e inocuidad, y con el fin de que los controles sean adecuados al contexto y al impacto de cada sistema, el Instituto clasificará los sistemas de inteligencia artificial que adquiera, desarrolle o utilice según su nivel de riesgo:

- Riesgo alto:** sistemas que intervienen en decisiones con efectos jurídicos o materiales significativos sobre los derechos de las personas o sobre la seguridad sanitaria —por ejemplo, los que apoyan actuaciones de vigilancia y control, la priorización de trámites que incide en el acceso a productos, o el tratamiento de datos sensibles—. Requieren evaluación de impacto algorítmico previa, supervisión humana reforzada y revisión periódica.
- Riesgo medio:** sistemas que apoyan procesos internos o la gestión documental sin decidir directamente sobre derechos, pero cuyo error puede afectar la calidad o la oportunidad del servicio. Requieren controles de validación y trazabilidad.
- Riesgo bajo:** sistemas de apoyo instrumental —búsqueda, organización o redacción asistida— sin incidencia en decisiones que afecten derechos. Se sujetan a los lineamientos generales de uso y verificación.

Antes de implementar un sistema de IA de riesgo alto, la dependencia responsable, con el acompañamiento de la Oficina de Tecnologías de la Información y del Oficial de Seguridad de la Información, adelantará una evaluación de impacto algorítmico que identifique los riesgos para los derechos de las personas, los datos personales y la seguridad de la información, y defina las medidas de mitigación. Cuando el sistema trate datos personales, dicha evaluación incorporará el análisis de impacto en la protección de datos correspondiente. La metodología, los criterios de clasificación y los formatos se desarrollarán en el anexo técnico el cual hace parte de la presente circular del Sistema de Gestión de Seguridad de la Información.

6. LINEAMIENTOS PARA EL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

En el uso de las herramientas de inteligencia artificial deberá darse cumplimiento a los siguientes parámetros:

- Los sistemas de inteligencia artificial – IA usados en la entidad, deberán ser lícitos, de modo que, en todo momento se garantice el cumplimiento legal y demás normas complementarias que le apliquen a su uso.

- Los sistemas de inteligencia artificial – IA utilizados en la entidad, solo deberán ser adquiridos a través de fuentes legales y siguiendo los procedimientos del proceso de contratación vigente.
- Asegurar que la información y los datos se utilicen aplicando las medidas de seguridad exigidas por el Estado, para garantizar el derecho de habeas data de los ciudadanos y prevenir pérdidas de confidencialidad, integridad y disponibilidad sobre los datos tratados por la IA.
- No utilizar datos sensibles salvo autorización de su titular. Por mandato del artículo 6 de la Ley 1581 de 2012, ello incluye los datos que afecten la intimidad del titular o cuyo uso indebido pueda generar discriminación, tales como los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos u organizaciones sociales o de derechos humanos, o que promuevan intereses de cualquier partido político o garanticen los derechos de partidos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, en los términos del artículo 5 ibidem.
- En aplicación de los principios de confidencialidad y seguridad, la información que no se considere pública no podrá ser empleada por la IA sin autorización previa de su propietario, adoptando todas las medidas tendientes a evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de conformidad con el literal h) del artículo 4 y con el artículo 9 de la Ley 1581 de 2012.
- Adoptar todas las medidas de seguridad de la información —administrativas y tecnológicas— que estén a su alcance para preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información contenida en los activos bajo responsabilidad del Instituto, que sea generada, consultada o aplicada mediante el uso de la IA, atendiendo lo dispuesto en los numerales VIII y IX de la Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio.
- Implementar acciones de mejora continua que permitan identificar, reportar y controlar oportunamente los eventos que, por el uso indebido de la IA, puedan constituir amenazas o vulnerabilidades potenciales o reales sobre los activos de información institucionales.
- Adoptar todas las medidas tendientes a evitar que las herramientas que utilicen IA tomen como base creaciones protegidas por derechos de autor, para lo cual deberá tenerse certeza de que las obras son de dominio público o no atribuibles a un creador determinado.

7. USOS NO PERMITIDOS

Sin perjuicio de las demás restricciones previstas en la presente circular, en ningún caso podrá emplearse la inteligencia artificial para:

- a) Adoptar de manera automatizada y sin intervención humana decisiones administrativas definitivas que produzcan efectos jurídicos o afecten los derechos de las personas.
- b) **Sustituir la motivación del acto administrativo.** Los fundamentos de hecho y de derecho de toda decisión deben ser elaborados y validados por el servidor competente, sin que la IA reemplace el análisis jurídico o técnico exigido por la ley.

- c) Ingresar en herramientas de IA de acceso público o no autorizadas información reservada, clasificada o sometida a reserva legal, datos personales o sensibles, información de investigaciones o actuaciones de vigilancia y control en curso, o secretos empresariales conocidos por el Instituto.
- d) Realizar calificación social de personas o vigilancia masiva, o efectuar tratamientos que generen discriminación.
- e) Utilizar contenido generado por IA, no verificado como fundamento de decisiones, conceptos o comunicaciones oficiales.
- f) Emplear herramientas de IA, que se basen en obras protegidas por derechos de autor sin la debida autorización o sin certeza de que se trata de contenido de dominio público.

Parágrafo. Las restricciones previstas en el presente numeral serán obligatorias para los terceros vinculados al Instituto únicamente cuando hayan sido incorporadas expresamente en el respectivo contrato, convenio, acuerdo o instrumento jurídico aplicable, sin perjuicio del cumplimiento de las obligaciones legales que les resulten exigibles.

8. LINEAMIENTOS ESPECÍFICOS PARA EL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA

El uso de herramientas de inteligencia artificial generativa —aquellas capaces de producir texto, imágenes, audio, código u otros contenidos— se sujeta, además, a las siguientes reglas:

- a) **Verificación obligatoria:** todo resultado generado por IA, debe ser revisado y validado por el servidor responsable antes de su uso. La IA es una herramienta de apoyo y no releva del deber de diligencia.
- b) **Control de exactitud:** deberán verificarse especialmente las referencias normativas, jurisprudenciales, técnicas y cuantitativas, dada la posibilidad de que la herramienta genere información inexacta o inexistente (“alucinaciones”).
- c) **Prohibición de uso no verificado:** ningún contenido generado por IA, podrá incorporarse a actos administrativos, conceptos jurídicos, respuestas a peticiones o comunicaciones oficiales sin verificación previa de su exactitud y pertinencia.
- d) **Trazabilidad:** cuando resulte relevante, se dejará constancia del uso de IA como herramienta de apoyo en la elaboración del documento, sin que ello altere la responsabilidad del servidor sobre su contenido.
- e) **Protección de la información:** no se ingresará en herramientas generativas de acceso público información que no tenga carácter público, conforme a los usos no permitidos de la presente circular.

9. TRANSPARENCIA ALGORÍTMICA

En cumplimiento del artículo 9 de la Directiva Conjunta 007 de 2025 de la Procuraduría General y la Defensoría del Pueblo, el Instituto publicará en su página web y a través de los medios apropiados para alcanzar a sus grupos de interés información clara,

comprensible y actualizada sobre los sistemas algorítmicos que emplee. Como mínimo, se divulgará la siguiente información:

- a) **Nombre del sistema:** denominación completa o acrónimo que permita identificar de manera clara e inequívoca el sistema algorítmico.
- b) **Objetivo del sistema:** propósito general que orienta el diseño, adquisición, uso o implementación del sistema algorítmico.
- c) **Función institucional:** descripción de la función, acción, programa, trámite o proceso de la Entidad en el que interviene el sistema algorítmico, incluyendo el rol específico que cumple dentro del mismo.
- d) **Estado del sistema:** etapa en que se encuentra el sistema algorítmico (desarrollo, implementación, suspensión o discontinuación). En fases de desarrollo se informará la fecha estimada de paso a implementación.
- e) **Tratamiento de datos personales:** declaración expresa sobre si el sistema algorítmico utiliza o no datos personales en su funcionamiento.
- f) **Tipo de datos utilizados:** categorías de datos procesados por el sistema, tales como texto, imágenes, sonidos, documentos, registros transaccionales, datos biométricos, datos de localización y georreferenciación, datos personales o registros censales, entre otros.
- g) **Desarrollador:** indicación expresa de si el sistema fue desarrollado internamente por la Entidad o, en caso contrario, identificación de la entidad, organización o empresa responsable de su diseño o suministro.
- h) **Contacto para objeciones:** correo electrónico y/o medio de contacto institucional de la dependencia o persona responsable de recibir solicitudes de revisión, reclamos u objeciones frente a decisiones automatizadas, individuales o grupales, incluyendo el plazo para su presentación conforme al artículo 12 de la citada directiva.
- i) **Contacto para más información:** medio de contacto del área o persona responsable del sistema, disponible para recibir consultas. El término para resolverlas será el previsto en el artículo 14 de la Ley 1755 de 2015.

En aplicación del principio de transparencia pasiva, toda persona tiene derecho a solicitar y recibir información clara, veraz, completa y comprensible sobre los sistemas algorítmicos utilizados por el Instituto.

10. GARANTÍAS FRENTE A DECISIONES AUTOMATIZADAS EN ACTUACIONES QUE PUEDAN AFECTAR DERECHOS

Cuando un sistema de inteligencia artificial o sistema algorítmico intervenga, intervenga, apoye o incida en actuaciones administrativas, trámites, conceptos, respuestas institucionales o decisiones que puedan producir efectos jurídicos o materiales sobre las personas, el Instituto garantizará en el marco del debido proceso administrativo, el derecho de petición, el acceso a la información pública y los estándares de transparencia algorítmica aplicables, las siguientes garantías:

- a) **Información y Transparencia:** que la persona conozca que en la actuación intervino un sistema de inteligencia artificial o sistema algorítmico, en los términos de la sección de transparencia algorítmica.
- b) **Supervisión y decisión humana:** toda decisión administrativa definitiva o actuación institucional que produzca efectos jurídicos o materiales significativos sobre las personas deberá ser adoptada o validada por un servidor público competente, quien asume la responsabilidad sobre la decisión. La inteligencia artificial no sustituirá la competencia, el juicio técnico o jurídico, ni la motivación exigida por la normativa aplicable.
- c) **Revisión, reclamo u objeción:** que la persona pueda presentar solicitudes de revisión, reclamos u objeciones frente a decisiones total o parcialmente apoyadas en sistemas de inteligencia artificial o sistemas algorítmicos o automatizadas, individuales o grupales a través de los canales institucionales dispuestos para tal fin conforme al artículo 12 de la Directiva Conjunta 007 de 2025. Dichas solicitudes serán tramitadas como manifestaciones del derecho de petición o dentro de la actuación administrativa correspondiente, según su naturaleza, con observancia del debido proceso, el CPACA y la Ley 1755 de 2015 o la norma que lo modifique o sustituya., ,
- d) **Trámite conforme al CPACA:** que dichas solicitudes se resuelvan con observancia del debido proceso administrativo y de los términos del derecho de petición previstos en la Ley 1755 de 2015 o la norma que lo modifique o sustituya.
- e) **Protección de datos personales:** cuando el sistema de inteligencia artificial o sistema algorítmico implique tratamiento de datos personales, el Instituto garantizará el cumplimiento de los principios, derechos, deberes y procedimientos previstos en la Ley 1581 de 2012 y sus normas reglamentarias, sin perjuicio de las demás garantías administrativas, constitucionales y legales aplicables.

11. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del uso de la inteligencia artificial; a revisar periódicamente el avance de su implementación y su adecuado uso; y a garantizar los recursos suficientes —tecnológicos y de talento humano calificado— para implementarla y mantenerla, incorporándola dentro de las decisiones estratégicas asociadas a la seguridad de la información.

12. ROLES Y RESPONSABILIDADES

El Instituto define los roles y responsabilidades para la implementación y uso de sistemas de inteligencia artificial, en cumplimiento de los lineamientos de seguridad de la información y de las obligaciones descritas en los manuales, procedimientos, formatos y demás documentación del sistema de gestión integrado del Instituto:

Dependencia	Responsabilidades frente a la implementación y uso de la IA
Dirección General	- Liderar y aprobar los presentes lineamientos y garantizar los recursos tecnológicos y de talento humano requeridos para su implementación, mantenimiento y mejora. - Adoptar las decisiones estratégicas asociadas al uso de la IA y a la seguridad de la información. - Asegurar que las decisiones con impacto irreversible o sobre los derechos de las personas conserven la supervisión y la decisión humana.
Comité Institucional de Gestión y Desempeño	- Articular el uso de la IA con el Modelo Integrado de Planeación y Gestión (MIPG) y con los planes institucionales. - Evaluar y recomendar la incorporación, actualización, suspensión o discontinuación de sistemas algorítmicos. - Hacer seguimiento a la implementación de los presentes lineamientos.
Servidores públicos, contratistas, colaboradores	- Usar las herramientas de IA conforme a estos lineamientos y a sus funciones u obligaciones. - Abstenerse de ingresar en las herramientas de IA información no pública, reservada o clasificada, así como datos personales o sensibles sin la debida autorización. - Verificar y validar los resultados generados por la IA antes de su utilización; la responsabilidad de la decisión es siempre humana. - Respetar los derechos de autor y reportar oportunamente los incidentes o usos indebidos.
Terceros vinculados mediante contrato o convenio	- Cumplir las obligaciones relacionadas con el uso de la inteligencia artificial, la protección de datos personales, la confidencialidad, la seguridad de la información y la propiedad intelectual que hayan sido pactadas en el respectivo contrato, convenio o instrumento jurídico suscrito con el Instituto. - Atender los controles y requisitos que, en materia de uso de IA, hayan sido incorporados contractualmente por el Invima.
Oficial de Seguridad de la Información / Representante de	Incorporar los riesgos asociados al uso de la IA en el proceso de gestión de riesgos de seguridad

Dependencia	Responsabilidades frente a la implementación y uso de la IA
la Dirección para el SGSI	de la información. - Definir, implementar y monitorear los controles para mantener los niveles de exposición dentro de los límites definidos por la Alta Dirección. - Gestionar los incidentes de seguridad de la información asociados al uso de la IA.
Oficina de Tecnologías de la Información	- Evaluar técnicamente, autorizar y administrar las herramientas y sistemas de IA, gestionando su ciclo de vida. - Mantener el inventario y registro de los sistemas algorítmicos y garantizar las condiciones técnicas de confidencialidad, integridad, disponibilidad y autenticidad. - Implementar mecanismos de trazabilidad y auditoría técnica. - Coordinar la evaluación de impacto algorítmico de los sistemas de IA de riesgo alto y su clasificación por niveles de riesgo.
Grupo de Soporte Tecnológico	- Brindar el soporte operativo y la mesa de ayuda para el uso autorizado de las herramientas de IA. - Escalar al Oficial de Seguridad de la Información y a la Oficina de Tecnologías de la Información los eventos o incidentes detectados.
Gestión de Talento Humano	- Fortalecer las competencias del talento humano en el uso ético, seguro y responsable de la IA. - Promover una cultura institucional de uso responsable y de buenas prácticas de seguridad.
Grupo Gestión Contractual	- Incorporar en los contratos, convenios y demás instrumentos jurídicos que impliquen acceso a información, sistemas o recursos tecnológicos del Instituto, las cláusulas relacionadas con la protección de datos personales, propiedad intelectual, confidencialidad y seguridad de la información y uso responsable de IA por terceros. - Verificar que los proveedores de sistemas de IA y demás terceros cumplan estos lineamientos y las obligaciones contractuales legales aplicables y asociadas al uso de la IA.
Oficina Asesora de Planeación	Articular los sistemas de IA con la planeación institucional y con los instrumentos de

Dependencia	Responsabilidades frente a la implementación y uso de la IA
	transparencia. • Coordinar y publicar en la página web la información de los sistemas algorítmicos exigida por la Directiva Conjunta 007 de 2025. • Definir indicadores de seguimiento a la implementación de los presentes lineamientos.
Grupo de Gestión Administrativa	• Gestionar los recursos administrativos y logísticos necesarios para la operación de las herramientas de IA autorizadas.
Grupo de Gestión Documental y Correspondencia	• Asegurar la gestión, conservación y disposición de los documentos producidos con apoyo de IA, conforme a las tablas de retención documental de la Entidad.
Oficina Asesora Jurídica	• Emitir los conceptos y lineamientos jurídicos sobre el uso de la IA y velar por la legalidad, la protección de datos personales, el habeas data y los derechos de autor. • Acompañar la atención de objeciones y reclamos frente a decisiones automatizadas y la defensa judicial asociada.
Oficina de Control Interno	• Evaluar de manera independiente y objetiva la implementación y el cumplimiento de los presentes lineamientos. • Incluir el uso de la IA dentro del plan anual de auditoría basado en riesgos.
Grupo de Control Disciplinario Interno	• Adelantar, cuando corresponda, la actuación disciplinaria derivada del uso indebido de la IA o del incumplimiento de los presentes lineamientos.
Dependencias Misionales y Oficina de Laboratorios y Control de Calidad	• Aplicar la IA en los procesos misionales garantizando la supervisión y la decisión humana en las determinaciones con impacto sobre la salud, los derechos o la seguridad sanitaria. • Documentar el rol del sistema algorítmico en el trámite o proceso en que interviene.

13. MECANISMOS DE COMUNICACIÓN

La presente circular será socializada a los servidores públicos, contratistas y demás colaboradores del Instituto a través de los canales de comunicación disponibles en la

Entidad, y estará disponible para consulta a través del portal web y de la plataforma Integra.

14. DEFINICIONES

Activo: en relación con la seguridad de la información, cualquier información o elemento relacionado con su tratamiento (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: posible causa de un incidente no deseado que puede producir daño a un sistema u organización.

Análisis de riesgos: proceso de comprender la naturaleza del riesgo y determinar su nivel.

Confidencialidad: propiedad de la información que la hace no disponible o que impide su divulgación a individuos, entidades o procesos no autorizados.

Control(es): medida que modifica el riesgo. Sinónimo: salvaguarda.

Decisión automatizada: decisión adoptada por medios tecnológicos, total o parcialmente, con base en el tratamiento de datos mediante un sistema algorítmico, sin intervención humana directa.

Evaluación de impacto algorítmico: análisis previo dirigido a identificar y valorar los riesgos que un sistema de IA puede generar sobre los derechos de las personas, los datos personales y la seguridad de la información, y a definir las medidas para su mitigación.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Información: conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen (Ley 1712 de 2014).

Disponibilidad: propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Integridad: propiedad de la información que busca preservar su exactitud y completitud.

Inteligencia artificial: tecnología que permite a las computadoras y máquinas simular el aprendizaje humano, la comprensión, la resolución de problemas, la toma de decisiones, la creatividad y la autonomía.

Inteligencia artificial generativa: subconjunto de la inteligencia artificial capaz de crear contenidos nuevos —texto, imágenes, audio, video o código— a partir de patrones aprendidos de grandes volúmenes de datos.

Parte interesada (stakeholder): persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Riesgo: posibilidad de que una amenaza concreta explote una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO Guía 73:2009).

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sesgo algorítmico: desviación sistemática en los resultados de un sistema de IA que puede producir tratos injustificados o discriminatorios respecto de personas o grupos.

Sistema algorítmico: conjunto de reglas, modelos o procesos computacionales que, a partir de datos de entrada, generan resultados, predicciones, recomendaciones o decisiones.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de manuales, procedimientos, controles y técnicas utilizados para controlar y salvaguardar los activos que se manejan dentro de una entidad.

Tercero: proveedores, empresas, organizaciones o entidades del Estado con las que se realice algún convenio de acceso o transferencia de información.

En cumplimiento de lo establecido en la Ley 1437 de 2011, Decreto 385 de 2026 y Circular INVIMA 1000-009-2026 el INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS – INVIMA, publicó el proyecto de Circular en su página web oficial, para comentarios y observaciones de la ciudadanía, garantizando la participación ciudadana y atendiendo al principio de publicidad y transparencia durante el periodo comprendido entre el [X] de [X] y el [X] de [X] de 202[X].

COMUNÍQUESE, PUBLIQUESE Y CÚMPLASE.

FRANCISCO A. G. ROSSI BUENAVENTURA

Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima

Proyectó: Oficina de Tecnologías de la Información.
Revisó y aprobó: Oficina Asesora Jurídica.

ANEXO TÉCNICO

Metodología de clasificación de riesgo, evaluación de impacto algorítmico y Registro de Sistemas Algorítmicos

1. OBJETO

El presente anexo desarrolla las secciones 5 y 9, establece la metodología para clasificar los sistemas de inteligencia artificial según su nivel de riesgo, el contenido y la plantilla de la evaluación de impacto algorítmico, y la ficha del Registro de Sistemas Algorítmicos del Invima.

2. ALCANCE

Aplica a todos los sistemas de inteligencia artificial que el Instituto adquiera, desarrolle, contrate o utilice, en cualquiera de sus fases —desarrollo, implementación, suspensión o discontinuación—, y a las dependencias responsables de su gestión.

3. CRITERIOS DE CLASIFICACIÓN DEL NIVEL DE RIESGO

La clasificación se realiza valorando, como mínimo, los siguientes criterios:

Criterio	Nivel bajo	Nivel medio	Nivel alto
Efecto sobre los derechos de las personas	Sin efecto	Apoyo a decisiones con validación humana	Decisión con efectos jurídicos o materiales
Autonomía de la decisión	Apoyo informativo	Recomendación sujeta a validación	Decisión automatizada
Tratamiento de datos personales	No trata datos personales	Datos personales no sensibles	Datos sensibles, de NNA o biométricos
Impacto en la seguridad sanitaria o la salud pública	Nulo	Indirecto	Directo
Alcance poblacional	Individual acotado	Colectivo determinado	Masivo o indeterminado
Reversibilidad de los efectos	Reversible	Difícilmente reversible	Irreversible

NNA: niños, niñas y adolescentes.

4. REGLAS DE ASIGNACIÓN DEL NIVEL DE RIESGO

El nivel de riesgo del sistema corresponde al más alto que resulte de aplicar las siguientes reglas:

- **Riesgo alto:** se asigna cuando concorra al menos uno de los siguientes factores: (i) decide de forma automatizada sobre derechos con efectos jurídicos o materiales significativos; (ii) trata datos sensibles, de niños, niñas y adolescentes o datos biométricos; (iii) impacta directamente la seguridad sanitaria o la salud

pública; (iv) produce efectos irreversibles; o (v) opera a escala masiva o indeterminada sobre personas.

- **Riesgo medio:** cuando apoye decisiones sobre derechos sujetas a validación humana obligatoria, trate datos personales no sensibles, o cuando su error pueda afectar la calidad o la oportunidad del servicio sin decidir directamente sobre derechos.
- **Riesgo bajo:** cuando constituya un apoyo instrumental sin incidencia en decisiones que afecten derechos ni tratamiento relevante de datos personales.

En caso de duda entre dos niveles, se asignará el de mayor exigencia.

5. CONTROLES DIFERENCIADOS POR NIVEL DE RIESGO

Control	Alto	Medio	Bajo
Evaluación de impacto algorítmico previa	Obligatoria	Recomendada	No exigible
Supervisión y decisión humana	Reforzada documentada y	Ordinaria	General
Registro en el Registro de Sistemas Algorítmicos	Obligatorio	Obligatorio	Obligatorio
Publicación en la página web (Directiva 007)	Obligatoria	Obligatoria	Según aplique
Pruebas de exactitud y de sesgo	Obligatorias	Recomendadas	No exigibles
Trazabilidad y auditoría técnica	Completa	Estándar	Básica
Revisión periódica	Anual o ante cambios	Bienal o ante cambios	Ante cambios relevantes

6. EVALUACIÓN DE IMPACTO ALGORÍTMICO

6.1. Procedencia

La evaluación de impacto algorítmico es obligatoria, con carácter previo a la implementación, para los sistemas clasificados como de riesgo alto, y recomendada para los de riesgo medio. Se actualizará ante cambios sustanciales en el sistema, en los datos o en su finalidad.

6.2. Contenido mínimo

- Identificación del sistema y de la dependencia responsable.
- Finalidad y función institucional.
- Descripción técnica y desarrollador o proveedor.
- Datos utilizados: tipos, fuente y base de legitimación, con indicación del tratamiento de datos sensibles.
- Nivel de riesgo asignado y su justificación.

- Riesgos identificados para los derechos de las personas, los datos personales y la seguridad de la información, así como riesgos de sesgo, discriminación o inexactitud.
- Medidas de mitigación y controles previstos.
- Mecanismo de supervisión y decisión humana.
- Mecanismo de revisión y objeción (contacto y plazo).
- Conclusión y decisión: aprobado, aprobado con condiciones o no aprobado.
- Responsables (elaboró, revisó, aprobó) y fechas.

Cuando el sistema trate datos personales, la evaluación incorporará el análisis de impacto en la protección de datos, conforme a la Ley 1581 de 2012 y sus normas reglamentarias.

6.3. Plantilla de evaluación de impacto algorítmico

Identificación del sistema	
Dependencia responsable	
Finalidad y función institucional	
Descripción técnica y desarrollador/proveedor	
Datos utilizados y base de legitimación	
Nivel de riesgo asignado y justificación	
Riesgos identificados	
Medidas de mitigación y controles	
Supervisión y decisión humana	
Mecanismo de revisión y objeción	
Conclusión y decisión	
Elaboró / Revisó / Aprobó y fechas	

7. REGISTRO DE SISTEMAS ALGORÍTMICOS

El Instituto mantendrá el Registro de Sistemas Algorítmicos, que consolidará la información de todos los sistemas de IA en uso o desarrollo. Por cada sistema se

diligenciará la siguiente ficha. Los campos a) a i) se publicarán en la página web conforme a la Directiva Conjunta 007 de 2025.

7.1. Información de publicación (campos a–i)

a) Nombre del sistema	
b) Objetivo del sistema	
c) Función institucional y rol del sistema	
d) Estado y fecha estimada de implementación	
e) ¿Trata datos personales? (Sí / No)	
f) Tipo de datos utilizados	
g) Desarrollador (interno / externo; identificación)	
h) Contacto para objeciones y plazo (art. 12 Directiva 007)	
i) Contacto para más información (art. 14 Ley 1755 de 2015)	

7.2. Información interna de gestión

Nivel de riesgo asignado	
Fecha de la evaluación de impacto algorítmico	
Dependencia responsable	
Fecha de registro y de última actualización	
¿Publicado en la página web? (Sí / No)	

8. PROCEDIMIENTO

Etapas	Responsable	Producto
1. Identificación y solicitud	Dependencia interesada	Solicitud de incorporación
2. Clasificación de riesgo	OTI y Oficial de Seguridad de la Información, con la dependencia	Nivel de riesgo asignado
3. Evaluación de impacto algorítmico (riesgo alto)	Dependencia responsable, OTI y Oficial de Seguridad; concepto de la OAJ cuando se afecten derechos	Evaluación de impacto algorítmico

Etapa	Responsable	Producto
4. Aprobación	Comité Institucional de Gestión y Desempeño (alto); OTI (medio y bajo)	Decisión de aprobación
5. Registro y publicación	Oficina Asesora de Planeación	Ficha registrada y publicada
6. Revisión periódica	Dependencia responsable y OTI	Ficha actualizada

9. REVISIÓN Y ACTUALIZACIÓN DEL ANEXO

El presente anexo técnico hace parte integral de la presente Circular y será revisado por lo menos una (01) vez al año, o cuando lo exijan cambios normativos, tecnológicos o institucionales o de gestión del riesgo asociado al uso de la inteligencia artificial.

La revisión técnica del anexo será liderada por la Oficina de Tecnologías de la Información y el Oficial de Seguridad de la Información, con el acompañamiento la Oficina Asesora Jurídica y de las demás dependencias competentes de la Entidad, según la materia objeto de actualización.

Las propuestas de modificación o actualización del anexo técnico serán presentadas al Comité Institucional de Gestión y Desempeño para su análisis y recomendación. La aprobación formal de dichas modificaciones corresponderá a la Dirección General, en atención a que el anexo forma parte integral de la presente Circular.

Proyectó: Oficina de Tecnologías de la Información.

Revisó y aprobó: Oficina Asesora Jurídica.