



Rad. 2026201696
Cod. 11000
Bogotá, D.C.

Honorable Senador
JOHN AMAYA RODRÍGUEZ
CONGRESO DE LA REPÚBLICA DE COLOMBIA
Carrera 7 No. 8 – 68, Edificio Nuevo del Congreso
Correos electrónicos: john.amaya@senado.gov.co; comision.sexta@senado.gov.co

Radicado:	2026533317
Fecha:	2/10/2026 10:58:28 A. M.
Proceso:	11000 PROSPECTIVA ESTRATÉGICA E INNOVACIÓN
Destino:	CONGRESO DE LA REPÚBLICA DE COLOMBIA OBSERVACIONES AL PROYECTO DE LEY No. 065 DE 2026 SENADO «POR MEDIO DE LA CUAL SE REGULA INTEGRALMENTE LA INTELIGENCIA ARTIFICIAL Y SE DICTAN OTRAS DISPOSICIONES».
Asunto:	

REF.: Observaciones al Proyecto de Ley No. 065 de 2026 Senado «Por medio de la cual se regula integralmente la inteligencia artificial y se dictan otras disposiciones».

Honorable Senador Amaya,

La Comisión de Regulación de Comunicaciones (CRC), en ejercicio de las funciones previstas en la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, presenta las siguientes observaciones al Proyecto de Ley No. 065 de 2026 Senado, “Por medio de la cual se regula integralmente la inteligencia artificial y se dictan otras disposiciones”, con el propósito de contribuir al debate legislativo sobre esta iniciativa y aportar elementos de análisis relacionados con los desafíos regulatorios, institucionales y de política pública asociados al desarrollo y adopción de sistemas de Inteligencia Artificial (IA) en Colombia.

Las consideraciones que se presentan a continuación recogen criterios generales de análisis que, desde las competencias de la CRC y las características técnicas y económicas del ecosistema digital, pueden contribuir al examen de esta y de futuras iniciativas relacionadas con inteligencia artificial.

El Proyecto de Ley No. 065 de 2026 Senado tiene como propósito establecer un marco integral para el desarrollo, investigación, diseño, implementación, comercialización, utilización y supervisión de sistemas de IA en Colombia, mediante la definición de conceptos asociados a esta tecnología, la adopción de disposiciones relacionadas con su desarrollo y uso, la creación de mecanismos institucionales de coordinación y la incorporación de medidas orientadas a promover su investigación, apropiación e implementación.

Las observaciones que siguen se formulan desde las competencias de la CRC y a partir de las características técnicas y económicas del ecosistema digital. El documento examina, primero, la arquitectura sobre la que opera la IA; posteriormente analiza las disposiciones del Proyecto relacionadas con gobernanza, promoción y gestión de riesgos; y finalmente plantea algunos criterios para su desarrollo legislativo y regulatorio. El análisis parte de reconocer que la IA se desarrolla sobre una arquitectura tecnológica y económica compuesta por distintas capas interdependientes, cuyos riesgos, estructuras competitivas y capacidades de intervención regulatoria no son necesariamente equivalentes.

1. Consideraciones generales sobre el enfoque regulatorio de la IA.

Comprender los desafíos regulatorios de la inteligencia artificial exige mirar primero el ecosistema sobre el que se desarrolla. La IA no constituye una capa autónoma ni, por sí sola, un mercado único. Su desarrollo depende de distintos mercados, insumos e infraestructuras que cumplen funciones diferentes a lo largo de la cadena de valor¹. Para efectos de este análisis, pueden distinguirse seis componentes: (i) infraestructura física y conectividad; (ii) capacidad de cómputo y almacenamiento; (iii) datos; (iv) modelos de inteligencia artificial; (v) servicios de integración y plataformas; y (vi) las aplicaciones, a través de las cuales estas capacidades se incorporan a procesos productivos o llegan a los usuarios.

Estos componentes no funcionan de manera aislada. Las redes permiten conectar usuarios, dispositivos, centros de datos y recursos de cómputo, mientras que las funciones de procesamiento pueden distribuirse entre infraestructura centralizada, nodos edge y dispositivos finales. En arquitecturas de IA distribuidas, la ubicación del procesamiento depende, entre otros factores, de los requerimientos de latencia, ancho de banda, privacidad y capacidad computacional de cada aplicación. La UIT ha documentado, para determinados casos de uso, arquitecturas en las que el *cloud* concentra almacenamiento, entrenamiento y optimización a gran escala, mientras el *edge* puede asumir procesamiento local, ajuste de modelos e inferencia cuando las condiciones técnicas y los recursos disponibles lo permiten²⁻³. El entrenamiento, el ajuste y la inferencia no requieren, por tanto, necesariamente la misma combinación ni localización de recursos de red y cómputo.

Esta relación entre conectividad y capacidad de procesamiento resulta cada vez más relevante. La distribución de cargas entre *cloud*, *edge* y dispositivo modifica los recursos de comunicación y cómputo necesarios para prestar un servicio. No existe una ubicación técnicamente óptima para todos los casos.

Las diferencias entre estos componentes también se reflejan en su estructura económica. En el hardware especializado, los altos costos fijos, las economías de escala y alcance y los largos ciclos de desarrollo pueden configurar barreras de entrada y, dependiendo de las condiciones del mercado, favorecer estructuras más concentradas. La infraestructura cloud y los centros de datos comparten varias de estas características, pero añaden otras dinámicas relevantes para la competencia, como los costos de cambio, las dificultades de interoperabilidad y la dependencia respecto de arquitecturas o servicios propietarios. En los datos cobran importancia factores como el acceso exclusivo, los ciclos de retroalimentación y las complementariedades con otros servicios. Por su parte, el desarrollo de modelos fundacionales exige elevados costos fijos y hundidos y puede beneficiarse de economías de escala tanto en entrenamiento como en inferencia. Finalmente, en las aplicaciones ubicadas aguas abajo pueden adquirir mayor peso los efectos de red, el lock-in, las ventajas de distribución y el empaquetamiento con otros servicios digitales.⁴. Estas diferencias

¹ OECD (2026), "Artificial Intelligence markets: Recent developments and competition issues", OECD Publishing, Paris, <https://doi.org/10.1787/d531d73f-en>.

² ITU-T Recommendation Y.4618 (06/2026), Artificial intelligence of things – Reference model and requirements, secs. 7 y 8. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4618-202606-I!!PDF-E&type=items

³ ITU-T Recommendation F.748.79 (12/2025), Requirements and framework of artificial intelligence-based multimedia data generation systems using core cloud and edge cloud. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-F.748.79-202512-I!!PDF-E&type=items

⁴ OECD (2026), "Artificial Intelligence markets: Recent developments and competition issues", OECD Publishing, Paris, <https://doi.org/10.1787/d531d73f-en>.

muestran por qué no resulta adecuado analizar el ecosistema de IA como si respondiera a una única estructura de mercado.

La distinción resulta especialmente importante cuando una misma empresa opera en varias partes de esta cadena. La integración entre infraestructura de cómputo, servicios cloud, modelos, APIs y aplicaciones puede generar eficiencias al reducir costos de transacción y coordinación, mejorar la interoperabilidad y el desempeño técnico y facilitar inversiones conjuntas entre actividades complementarias. Sin embargo, cuando un mismo actor controla insumos relevantes para competir en capas posteriores, también puede adquirir la capacidad de favorecer servicios vinculados, restringir la interoperabilidad o elevar los costos de cambio de empresas que dependen de esos insumos⁵. El análisis no debería presumir, por tanto, que la escala o la integración vertical son problemáticas en sí mismas. Lo relevante es establecer, en cada mercado, si las eficiencias asociadas a la integración prevalecen o si el control de una capa puede reducir materialmente la contestabilidad, limitar la entrada o dificultar la expansión de otros actores.

La experiencia reciente del mercado *cloud* muestra por qué esta distinción importa. La autoridad de competencia del Reino Unido identificó barreras de interoperabilidad y cargos asociados a la salida de datos que restringían el cambio de proveedor y el uso simultáneo de varios servicios *cloud*. Estas restricciones no derivaban de la inteligencia artificial como tecnología, sino de las condiciones técnicas y comerciales de una infraestructura que, a su vez, constituye un insumo relevante para su desarrollo y despliegue.⁶

El ejemplo permite precisar el criterio regulatorio. Antes de asignar una obligación conviene identificar dónde se origina o materializa el riesgo, la falla de mercado o el problema regulatorio; qué actor dispone de la información y del control técnico o económico para intervenir; y en qué mercado, servicio o contexto se producen sus efectos. De esta forma, las responsabilidades pueden vincularse con la función y capacidad efectiva de cada actor, distinguiendo problemas de seguridad, datos, competencia, infraestructura, contenidos o protección de usuarios.

Esta aproximación encuentra puntos comunes con distintos marcos internacionales que, aun bajo diseños institucionales diferentes, combinan reglas horizontales con obligaciones diferenciadas según el riesgo, el tipo de sistema y el contexto en el que se utiliza. En la Unión Europea, por ejemplo, el Reglamento (UE) 2024/1689 (AI Act) establece un marco horizontal que prohíbe determinadas prácticas, somete los sistemas de alto riesgo a requisitos específicos, establece obligaciones de transparencia para ciertos sistemas y usos y contempla un régimen particular para los modelos de IA de propósito general. El Reglamento entró en vigor el 1 de agosto de 2024 y su aplicación se ha previsto de manera gradual, con distintos grupos de obligaciones que entran en vigor en momentos diferentes⁷.

⁵ OECD (2025), "Artificial intelligence and competitive dynamics in downstream markets", OECD Roundtables on Competition Policy Papers, No. 331, OECD Publishing, Paris, <https://doi.org/10.1787/ccf0624a-en>.

⁶ Competition and Markets Authority (CMA), Cloud services market investigation – Final decision report. <https://www.gov.uk/cma-cases/cloud-services-market-investigation>

⁷ Consejo de la UE / Parlamento Europeo, "AI Omnibus — Provisional Agreement" (mayo 2026). Consejo de la UE, Comunicado de prensa, 7 de mayo de 2026. Disponible en: <https://www.consilium.europa.eu>. Véase también: Mishcon de Reya, "EU AI Act Simplified: Unpacking the AI Omnibus Agreement of May 2026."

La existencia de este marco horizontal no supone que todas las funciones de supervisión deban concentrarse en una única autoridad. El artículo 70 del AI Act permite que los Estados miembros establezcan o designen una o varias autoridades nacionales competentes de acuerdo con sus necesidades organizativas⁸. Irlanda adoptó precisamente un modelo distribuido. La AI Office of Ireland ejerce funciones de coordinación nacional, mientras que la supervisión y aplicación del Reglamento se apoyan en autoridades ya existentes con competencias en ámbitos como comunicaciones, competencia y protección al consumidor, protección de datos, servicios financieros, salud, transporte y relaciones laborales⁹. El diseño busca incorporar las nuevas funciones regulatorias dentro de estructuras que ya cuentan con conocimiento sectorial, preservando al mismo tiempo una instancia común de coordinación.

La evolución reciente del marco europeo también muestra que su implementación puede requerir ajustes. El Reglamento (UE) 2026/1744 modificó determinadas disposiciones del AI Act para simplificar su aplicación, facilitar el cumplimiento y ajustar algunos de sus mecanismos y plazos¹⁰. La reforma mantiene la arquitectura general del Reglamento, pero muestra que el diseño regulatorio puede requerir calibraciones a medida que se desarrollan los estándares, las capacidades institucionales y la experiencia de implementación.

En Estados Unidos, distintas autoridades federales también han aplicado sus competencias existentes a usos concretos de inteligencia artificial. La Federal Trade Commission ha aplicado las normas sobre prácticas desleales o engañosas a conductas vinculadas con IA y también ha examinado posibles cuellos de botella competitivos a lo largo del denominado AI stack. La Food and Drug Administration, por su parte, ha desarrollado orientaciones específicas para dispositivos médicos habilitados por IA dentro de su marco sectorial de seguridad y eficacia.¹¹ Estos ejemplos muestran cómo una nueva capacidad tecnológica puede incorporarse a marcos regulatorios existentes, aunque requiera adaptar criterios técnicos e instrumentos de supervisión.

Ofcom ofrece un ejemplo similar en comunicaciones y servicios digitales. En noviembre de 2024 explicó que la Online Safety Act puede aplicarse a herramientas de IA generativa y chatbots cuando, por las funciones que prestan, encajan en alguna de las categorías de servicios regulados por la Ley. Una herramienta que permite interacción y difusión de contenidos entre usuarios puede quedar comprendida como servicio user-to-user, mientras determinadas herramientas de búsqueda pueden quedar sujetas al régimen aplicable a search services. La obligación depende, por tanto, de la función regulada y del riesgo asociado al servicio, no únicamente de que incorpore inteligencia artificial¹².

⁸ Reglamento (UE) 2024/1689, Art. 70 (Designación de autoridades nacionales competentes). Disponible: <http://data.europa.eu/eli/reg/2024/1689/oj>

⁹ IDA Ireland, "What EU AI Act means for firms operating in Ireland" (abril 2026); UNESCO, "Who Governs AI in the EU? A Breakdown of Authorities in the EU AI Act" (febrero 2026), disponible en: <https://www.unesco.org/en/articles/who-governs-ai-eu-breakdown-authorities-eu-ai-act>.

¹⁰ Reglamento (UE) 2026/1744 (Digital Omnibus on AI). Disponible: <http://data.europa.eu/eli/reg/2026/1744/o>

¹¹ GDPR Local, "AI Regulations in the US: What You Need to Know in 2025" (septiembre 2025); Astraea Counsel, "Federal AI Regulation Landscape: What's Coming in 2025–2026" (noviembre 2025). Véase también: Pacific AI, "AI regulations in the US" (noviembre 2025).

¹² Ofcom, "Open letter to UK online service providers regarding Generative AI and chatbots", 8 de noviembre de 2024. Disponible: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/open-letter-to-uk-online-service-providers-regarding-generative-ai-and-chatbots>

La aplicación del régimen depende, entonces, de las características y funciones del servicio y no simplemente de que utilice inteligencia artificial. Las obligaciones sobre contenido ilegal entraron en vigor el 17 de marzo de 2025 y las relativas a la protección de niños frente a contenidos perjudiciales, el 25 de julio del mismo año¹³⁻¹⁴. La experiencia británica muestra que nuevas funcionalidades tecnológicas pueden quedar comprendidas dentro de competencias y categorías regulatorias existentes cuando el riesgo que se busca atender ya forma parte de su ámbito de aplicación.

Esta lógica también tiene una consecuencia institucional. La transversalidad de la inteligencia artificial no implica que su regulación deba concentrarse en una única autoridad. Los riesgos asociados a datos, competencia, consumidores, comunicaciones, contenidos, servicios financieros, salud o trabajo se manifiestan en contextos distintos y requieren capacidades técnicas, conocimiento de los mercados e instrumentos de intervención diferentes. Una institucionalidad multicéntrica permite aprovechar esas competencias especializadas y mantener la responsabilidad en las autoridades que ya conocen y supervisan cada ámbito.

Este modelo no supone fragmentar la gobernanza. Exige, por el contrario, reglas claras de articulación entre autoridades, intercambio de información y mecanismos para resolver riesgos que atraviesen varios sectores o capas del ecosistema. La literatura sobre gobernanza policéntrica describe modelos con múltiples centros de decisión que conservan autonomía dentro de sus ámbitos e interactúan mediante mecanismos de coordinación, aprendizaje y adaptación¹⁵. En inteligencia artificial, esta lógica encuentra expresiones concretas en modelos como el irlandés, que distribuye la supervisión del AI Act entre autoridades sectoriales existentes y asigna a la AI Office funciones centrales de coordinación; y el enfoque británico desarrollado en el White Paper de 2023 propuso a los reguladores existentes la aplicación de principios transversales de IA dentro de sus respectivos mandatos¹⁶⁻¹⁷.

Para Colombia, esta aproximación permitiría construir sobre la institucionalidad existente antes que superponer nuevas competencias de manera general. El punto de partida debería ser identificar dónde se materializa el riesgo, qué autoridad cuenta con las competencias y capacidades para gestionarlo y cuándo resulta necesaria la actuación conjunta de varias entidades. La coordinación horizontal resulta particularmente importante frente a riesgos que atraviesan varias capas del ecosistema o no tienen un único ámbito sectorial, pero no requiere desplazar el conocimiento especializado ni las competencias que el ordenamiento ya ha asignado. El objetivo es contar con

¹³ Ofcom, "Important dates for Online Safety compliance". Disponible: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/important-dates-for-online-safety-compliance>

¹⁴ Ofcom, "Protecting people from online suicide and self-harm material". Disponible: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/protecting-people-from-online-suicide-and-self-harm-material>

¹⁵ Inga Ulnicane, Governance fix? Power and politics in controversies about governing generative AI, Policy and Society, Volume 44, Issue 1, January 2025, Pages 70–84. Disponible: <https://doi.org/10.1093/polsoc/puae022>

¹⁶ Véase AI Office of Ireland, National Competent Authorities, que describe el modelo irlandés como un "distributed model of competent authorities" apoyado en competencias y áreas de especialización ya existentes. Disponible: <https://aioffice.gov.ie/national-competent-authorities/>

¹⁷ UK Department for Science, Innovation and Technology (2023), A pro-innovation approach to AI regulation, especialmente párrs. 47 y ss., donde se atribuye a los reguladores existentes la aplicación de los principios de IA dentro de sus respectivos ámbitos de especialidad. Disponible: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>.

una arquitectura institucional capaz de actuar como sistema, sin convertir la inteligencia artificial en un nuevo sector regulado por una autoridad única.

2. Consideraciones al Proyecto de Ley 065 de 2026 Senado.

a. Modelo de Gobernanza Institucional

Bajo este marco, el diseño institucional previsto en el Proyecto podría distinguir con mayor claridad las funciones de coordinación horizontal de las competencias regulatorias y de supervisión que corresponden a las autoridades sectoriales. Una instancia horizontal puede aportar coherencia en estándares comunes, cooperación internacional y seguimiento de la política nacional, mientras el conocimiento de la arquitectura tecnológica, la estructura de los mercados y las características de los usuarios sigue siendo relevante para atender los riesgos que se materializan en ámbitos específicos.

La arquitectura institucional prevista en el Proyecto de Ley también debería reflejarse en las funciones de vigilancia y control. El artículo 12 atribuye a la Superintendencia de Industria y Comercio las funciones de vigilancia y control para el cumplimiento de la ley. Esta previsión debería articularse expresamente con las competencias que el ordenamiento ya asigna a otras autoridades sectoriales, particularmente cuando el uso de IA se inserte en mercados o servicios sometidos a regulación especializada.

Esta precisión resulta especialmente importante bajo una lógica multicéntrica. Para la CRC, el punto no es quién asume las funciones sancionatorias, sino preservar la coherencia entre la vigilancia general prevista en el Proyecto, las reglas ex ante aplicables a los mercados regulados y la distribución legal de competencias. Una cláusula que disponga que las funciones del artículo 12 se ejercen sin perjuicio de las competencias atribuidas a otras autoridades contribuiría a reducir superposiciones y vacíos.

b. Promoción para el desarrollo de la Inteligencia Artificial.

El Proyecto incorpora instrumentos orientados a la investigación, formación, apropiación y desarrollo del ecosistema nacional de IA. Desde la perspectiva de la CRC, su efectividad también depende de las condiciones de la infraestructura digital que soporta estos desarrollos.

La capacidad para adoptar y desarrollar IA no depende únicamente del talento o de la financiación. También intervienen la conectividad de alta capacidad, el acceso a infraestructura de cómputo y servicios *cloud*, la disponibilidad de centros de datos y almacenamiento, el acceso a datos y los mecanismos de integración y distribución de modelos y aplicaciones. Restricciones relevantes en cualquiera de estas capas pueden limitar la entrada, la experimentación o el escalamiento; por ello, las políticas de promoción ganan precisión cuando permiten identificar dónde se encuentran efectivamente esos cuellos de botella.

Desde una perspectiva de ecosistema, la capacidad nacional para adoptar IA no depende únicamente de la disponibilidad de talento o de la financiación de proyectos. También requiere conectividad de alta capacidad, acceso competitivo a infraestructura de cómputo, servicios *cloud* y

almacenamiento, disponibilidad de centros de datos, acceso a datos y mecanismos que faciliten la integración y distribución de modelos y aplicaciones. Las restricciones en cualquiera de estas capas pueden convertirse en cuellos de botella para las restantes. En consecuencia, las políticas de promoción deberían identificar qué restricciones afectan efectivamente la capacidad de entrada, experimentación y escalamiento de empresas y usuarios colombianos.

c. Enfoque de riesgos en el desarrollo de la Inteligencia Artificial.

El Proyecto de Ley contiene elementos importantes para construir un enfoque basado en riesgos. Reconoce distintos actores dentro del ciclo de desarrollo y uso de la IA, identifica riesgos asociados a estos sistemas y establece una categoría de alto riesgo sujeta a obligaciones reforzadas. El punto central, por tanto, no está en incorporar nuevamente estos conceptos, sino en conectarlos de manera más precisa con las obligaciones que posteriormente desarrolla la iniciativa.

Los artículos 10 y 11 ofrecen un espacio concreto para hacerlo. Allí se reúnen riesgos de naturaleza muy distinta y se establece un deber general de informar sobre ellos y sobre sus mecanismos de mitigación. Una regulación basada en riesgos exige dar un paso adicional: determinar cómo cambia la intensidad de la obligación según la naturaleza, probabilidad e impacto del riesgo, la función que cumple cada actor y, especialmente, su capacidad efectiva para prevenirlo, controlarlo o mitigarlo. No todos los participantes de la cadena disponen de la misma información ni controlan los mismos elementos del sistema. Tratarlos de manera equivalente puede trasladar obligaciones hacia actores que no están en posición de gestionar eficazmente el riesgo que se pretende atender.

La arquitectura descrita anteriormente permite convertir ese principio en una regla de decisión regulatoria. Antes de imponer una obligación conviene identificar dónde se origina o materializa el problema, en qué capa puede intervenir con mayor eficacia, qué actor dispone del control técnico o económico relevante y dónde se producen finalmente sus efectos. Este análisis permite separar problemas que pueden parecer similares bajo la etiqueta de IA, pero que responden a lógicas distintas de seguridad, protección de usuarios, datos, competencia, infraestructura o contenidos. La obligación debería recaer, en consecuencia, allí donde exista capacidad real de intervención y guardar proporción con el riesgo que busca corregir.

La gestión del riesgo también debe reconocer que los actores de esta cadena no disponen de la misma información ni controlan los mismos componentes. Un proveedor de conectividad, un operador de infraestructura *cloud*, un desarrollador de un modelo fundacional, un integrador que consume dicho modelo mediante una API y una empresa que utiliza la aplicación resultante intervienen en momentos diferentes del sistema. Imponerles obligaciones equivalentes puede resultar ineficaz. La obligación debería recaer, en principio, sobre el actor que razonablemente dispone de la información, capacidad técnica y control necesarios para prevenir o mitigar el riesgo.

Asimismo, determinados riesgos pueden tener origen no en el funcionamiento algorítmico del modelo, sino en la estructura económica del ecosistema. Altos costos fijos y hundidos, economías de escala y alcance, restricciones de acceso a infraestructura de cómputo o datos, costos de cambio, incompatibilidades técnicas y efectos de red pueden afectar las condiciones de entrada o expansión. La relevancia de cada característica dependerá de la capa analizada y no debería presumirse de manera uniforme para todo el ecosistema de IA.

Particular atención merecen las capas que funcionan bajo lógicas de plataforma. Cuando una infraestructura o servicio empareja simultáneamente a desarrolladores, proveedores de modelos, empresas usuarias, complementadores y consumidores, pueden surgir efectos indirectos de red: la utilidad de participar en un lado del ecosistema aumenta con la presencia de actores en otro. Bajo determinadas condiciones, estas dinámicas, sumadas a ventajas de distribución, configuraciones predeterminadas, empaquetamiento o costos de cambio, pueden favorecer procesos de concentración o dependencia tecnológica. No obstante, dichos efectos deben acreditarse caso por caso, considerando también la posibilidad de multihoming, interoperabilidad y entrada de nuevos modelos o proveedores.

Por esta razón, además de evaluar concentración, resulta relevante observar la contestabilidad de las distintas capas: la capacidad real de nuevos actores para entrar, acceder a insumos, interoperar, cambiar de proveedor y alcanzar usuarios. En mercados tecnológicos dinámicos, una elevada participación de mercado no necesariamente demuestra por sí sola un ejercicio de poder de mercado persistente; del mismo modo, una estructura aparentemente dinámica puede ocultar dependencias relevantes cuando determinados insumos o canales de distribución resultan difíciles de sustituir.

3. Propuesta de la CRC para fortalecer el desarrollo del ecosistema de la Inteligencia Artificial.

El diseño regulatorio también debe partir de las condiciones del ecosistema colombiano. El Índice Latinoamericano de Inteligencia Artificial (ILIA 2025) elaborado por la CEPAL y el Centro Nacional de Inteligencia Artificial de Chile (CENIA), mantiene a Colombia dentro del grupo de países “adoptantes”, mientras Chile, Brasil y Uruguay se ubican entre los “pioneros”¹⁸. Lo anterior no justifica una menor protección frente a los riesgos de la IA, pero sí muestra que las obligaciones regulatorias operarán sobre un ecosistema con capacidades de inversión, infraestructura y talento distintas a las de mercados más maduros.

Estas condiciones también inciden en los efectos de la regulación. En segmentos con altos costos fijos, economías de escala o dependencia de insumos como cómputo, cloud, datos o canales de distribución, una obligación de costo fijo puede pesar proporcionalmente más sobre empresas pequeñas y nuevos entrantes. Al mismo tiempo, cuellos de botella, restricciones de interoperabilidad o costos de cambio elevados pueden dificultar por sí mismos la entrada y la innovación. La discusión resulta más útil si se concentra en el riesgo o falla identificada, los efectos previsibles de la intervención y el instrumento menos distorsionante para atenderla, en lugar de plantearse simplemente en términos de mayor o menor regulación.

A partir de estas consideraciones, la CRC estima que el desarrollo legislativo y regulatorio de la inteligencia artificial podría orientarse por los siguientes criterios:

¹⁸ CEPAL/CENIA, Índice Latinoamericano de Inteligencia Artificial (ILIA 2024). Santiago de Chile, 2024. Disponible en: <https://indicelatam.cl/>. Véase también: CEPAL/CENIA, ILIA 2025 (<https://www.cepal.org/es/publicaciones/82514-indice-latinoamericano-inteligencia-artificial-ilia-2025>).

- **Neutralidad tecnológica:** En la medida de lo posible, las obligaciones deberían concentrarse en los riesgos, efectos o resultados que se busca prevenir o corregir, evitando vincularlas innecesariamente a una arquitectura, modelo o solución tecnológica específica. Esto permite que la regulación conserve su utilidad frente a cambios tecnológicos y que riesgos equivalentes reciban un tratamiento comparable, aun cuando se materialicen mediante soluciones distintas.
- **Proporcionalidad y gradualidad:** La intensidad de la intervención debería guardar relación con la naturaleza, probabilidad e impacto del riesgo y con el contexto en el que este se materializa. La gradualidad resulta especialmente relevante en un ecosistema en evolución, pues permite ajustar las obligaciones a partir de nueva evidencia, cambios tecnológicos y transformaciones en la estructura de los mercados, sin extender cargas equivalentes a actividades con perfiles de riesgo sustancialmente distintos.
- **Asignación de obligaciones según rol y capacidad de control:** Los actores que intervienen en la arquitectura de IA no disponen de la misma información ni controlan los mismos componentes. Las obligaciones deberían considerar la función que cada uno desempeña, la información a la que tiene acceso y su capacidad efectiva para prevenir, controlar o mitigar el riesgo. Esta diferenciación evita trasladar responsabilidades hacia actores que, aun participando en la cadena, no se encuentran en posición de gestionar eficazmente el problema que se pretende atender.
- **Institucionalidad multicéntrica y coordinación:** La transversalidad de la IA exige una arquitectura institucional capaz de aprovechar las competencias y capacidades técnicas ya existentes, sin concentrar su regulación y supervisión alrededor de la tecnología como una categoría autónoma. La protección de datos, la competencia, los consumidores, las comunicaciones, los contenidos, los servicios financieros o la salud plantean riesgos distintos y requieren conocimiento especializado. El reto está en articular esas capacidades y establecer mecanismos claros de coordinación cuando un mismo sistema o caso de uso atraviese varios sectores o capas del ecosistema. Así se preserva la especialización institucional y, al mismo tiempo, se reducen superposiciones, vacíos y respuestas regulatorias inconsistentes.
- **Análisis de impacto, generación de evidencia y experimentación regulatoria:** Las decisiones de intervención deberían apoyarse en evidencia sobre el riesgo identificado, sus efectos y las alternativas disponibles para atenderlo. En un entorno tecnológico sujeto a cambios rápidos, el análisis de impacto puede complementarse con mecanismos de experimentación, entornos controlados y revisiones periódicas que permitan observar el funcionamiento de nuevas soluciones antes de consolidar obligaciones de carácter general. Más que trasladar automáticamente modelos desarrollados en otros mercados, resulta relevante valorar sus efectos bajo las condiciones tecnológicas, económicas e institucionales del ecosistema colombiano.
- **Contestabilidad, interoperabilidad y capacidad de elección:** La evolución de la IA también plantea preguntas sobre las condiciones de competencia entre las distintas capas del ecosistema. Cuando resulte relevante para el mercado analizado, conviene considerar el acceso a insumos, la interoperabilidad, la portabilidad de datos y cargas, el multihoming, los costos de cambio, las ventajas de distribución y los efectos de la integración vertical. El análisis debería

reconocer tanto las eficiencias que pueden derivarse de la escala y de la integración tecnológica como las condiciones bajo las cuales el control de una capa o de un insumo relevante puede limitar la entrada, la sustitución o la expansión de otros actores.

4. Consideraciones Finales

La CRC reconoce el valor de que el Congreso abra una discusión integral sobre el desarrollo, uso y gobernanza de la inteligencia artificial en Colombia. El Proyecto de Ley ofrece una oportunidad para dar mayor claridad al marco institucional, fortalecer la gestión de riesgos y generar condiciones que acompañen la adopción de estas tecnologías. Precisamente por la amplitud de esa discusión, resulta importante que la regulación conserve suficiente flexibilidad para responder a un ecosistema que evoluciona con rapidez y en el que conviven actores, mercados y capacidades muy diferentes.

La tesis que orienta estas observaciones es que la regulación de la inteligencia artificial no debería seguir a la tecnología en abstracto, sino a la arquitectura sobre la que opera, a los riesgos que se materializan en sus distintas capas y a la capacidad técnica o económica de cada actor para prevenirlos, controlarlos o mitigarlos. Esta aproximación permite diferenciar obligaciones según el riesgo y la función de cada participante, preservar la neutralidad tecnológica y reconocer que problemas de competencia, datos, contenidos, infraestructura, consumidores o seguridad requieren respuestas regulatorias distintas.

Desde esa perspectiva, el Proyecto puede fortalecerse mediante una institucionalidad multicéntrica, apoyada en las competencias y capacidades ya existentes y acompañada de mecanismos de coordinación para los casos en que un sistema o caso de uso atraviese varios sectores o capas del ecosistema. La proporcionalidad y la generación de evidencia permiten, a su vez, acompasar la protección de derechos y usuarios con las condiciones necesarias para la entrada, la inversión, la adopción tecnológica y la innovación.

Con estas observaciones, la CRC busca contribuir constructivamente al debate legislativo sobre el Proyecto de Ley No. 065 de 2026 Senado y a la construcción de un marco capaz de gestionar riesgos concretos de la inteligencia artificial, atendiendo las condiciones tecnológicas, económicas e institucionales en las que deberá operar en Colombia.

Quedamos a su entera disposición para cualquier duda o aclaración que pueda surgir.

Cordialmente,

DÍAZ SUAIZA

FELIPE

AUGUSTO

Firmado digitalmente
por DÍAZ SUAIZA
FELIPE AUGUSTO
Fecha: 2026.10.02
11:04:00 -05'00'

FELIPE AUGUSTO DÍAZ SUAIZA

Director Ejecutivo

Proyectado por: Ana Beatriz Ruiz

Revisado por: Víctor Baldrich

Aprobado por: Zoila Vargas