39D10020260000782

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERU

CONTRALORÍA

Firmado digitalmente por AGUILAR SURICHAQUI Cesar Enrique FAU 20131378972 hard
Motivo: Soy el autor del documento
Fecha: 15-06-2026 12:37:43 -05:00

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
Año de la Esperanza y el Fortalecimiento de la Democracia"

Jesús María, 15 de Junio de 2026

OFICIO N° 000782-2026-CG/DC

Señora Congresista
Ana Zadith Zegarra Saboya
Presidenta de la Comisión Descentralización, Regionalización, Gobiernos Locales y Modernización de la Gestión del Estado
Congreso de la República
Plaza Bolívar S/N - Palacio Legislativo
Lima/Lima/Lima

Asunto	:	Atención a solicitud de opinión institucional sobre el Proyecto de Ley N° 14544/2025-CR, "Proyecto de ley que complementa y fortalece el marco de gobernanza, transparencia, control y responsabilidad en el uso de la inteligencia artificial"	
Referencia	:	Oficio N° 2219-2025-2026-CDRGLMGE-CR Expediente N° 0820260308499	12/05/2026 12/05/2026

Tengo el agrado de dirigirme a usted en atención al documento de la referencia, mediante el cual solicitó la opinión de esta Entidad Fiscalizadora Superior sobre el Proyecto de Ley N° 14544/2025-CR, "Proyecto de ley que complementa y fortalece el marco de gobernanza, transparencia, control y responsabilidad en el uso de la inteligencia artificial".

Al respecto, se remite los comentarios vinculados a vuestra solicitud en el anexo al presente oficio en nueve (9) folios.

Hago propicia la oportunidad para expresarle las seguridades de mi consideración.

Atentamente,

Cesar Enrique Aguilar Surichaqui
Contralor General de la República

V°B°

Firmado digitalmente por PEREZ WICHT SAN ROMAN Gonzalo Jose Miguel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 09-06-2026 12:15:29 -05:00

(CAS/bcr)

Nro. Emisión: 02588 (D100 - 2026) Elab:(U18212 - C380)

V°B°

Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 09-06-2026 10:45:42 -05:00

ANEXO AL OFICIO N° 782-2026-CG/DC

1. ANTECEDENTE

Mediante Oficio N° 2219-2025-2026-CDRGLMGE-CR de 12 de mayo de 2026 (Expediente N° 0820260308499 de 12 de mayo de 2026), la congresista Ana Zadith Zegarra Saboya, presidenta de la Comisión de Descentralización, Regionalización, Gobiernos Locales y Modernización de la Gestión del Estado, solicitó la opinión institucional de esta Entidad Fiscalizadora Superior sobre el Proyecto de Ley N° 14544/2025-CR, "Proyecto de ley que complementa y fortalece el marco de gobernanza, transparencia, control y responsabilidad en el uso de la inteligencia artificial".

2. DE LA COMPETENCIA PARA EMITIR OPINIÓN SOBRE EL PROYECTO DE LEY

2.1 El artículo 82 de la Constitución Política del Perú establece que la Contraloría General de la República es el órgano superior del Sistema Nacional de Control, que tiene a su cargo la supervisión de la legalidad de la ejecución del presupuesto del Estado, de las operaciones de la deuda pública y de los actos de las instituciones sujetas a control; siendo desarrollado su alcance en Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, cuyo artículo 16 establece que esta Entidad Fiscalizadora Superior tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental; añadiendo que no puede ejercer atribuciones o funciones distintas a las establecidas en la Constitución Política ni en la mencionada Ley Orgánica.

2.2 En dicho propósito, es preciso indicar que, de conformidad con el literal h) del artículo 32 de la Ley N° 27785, el Contralor General de la República se encuentra facultado para *"Presentar u opinar sobre proyectos de normas legales que conciernan al control y a las atribuciones de los Órganos de Auditoría Interna"*.

2.3 Ahora bien, del análisis y evaluación del Proyecto de Ley N° 14544/2025-CR, se advierte que su objeto reside en complementar y fortalecer el marco normativo vigente sobre inteligencia artificial; siendo su fórmula legal, la siguiente:

FORMULA LEGAL

LEY QUE COMPLEMENTA Y FORTALECE EL MARCO DE GOBERNANZA, TRANSPARENCIA, CONTROL Y RESPONSABILIDAD EN EL USO DE LA INTELIGENCIA ARTIFICIAL

Artículo 1. – Objeto de la Ley
La presente ley tiene por objeto complementar y fortalecer el marco normativo vigente sobre inteligencia artificial, estableciendo mecanismos jurídicos vinculantes de transparencia algorítmica, gestión de riesgos, evaluación de impacto, auditoría, responsabilidad y fiscalización, con especial énfasis en los sistemas de inteligencia artificial de alto riesgo, garantizando la protección de los derechos fundamentales, la seguridad jurídica y el interés público.

Artículo 2. – Ámbito de aplicación
La presente ley es de aplicación obligatoria a: a) Las entidades del Estado en todos los niveles de gobierno. b) Las personas naturales o jurídicas, públicas o privadas, que desarrollen, implementen, comercialicen o utilicen sistemas de inteligencia artificial en el territorio nacional o cuyos efectos se produzcan en él.

Artículo 3. – Derecho a la información sobre el uso de inteligencia artificial
Toda persona tiene derecho a ser informada, de manera clara, accesible y comprensible, cuando una decisión, recomendación o evaluación que le afecte de forma significativa haya sido adoptada o asistida mediante un sistema de inteligencia artificial, indicando como mínimo:
a) La utilización de dicho sistema.
b) Su finalidad.
c) La existencia de supervisión humana

V°B°
Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Vista Bueno
Fecha: 04-06-2026 16:26:04 -05:00

V°B°
Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Vista Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

Artículo 4. – Derecho a la explicación y revisión humana
En los supuestos de decisiones automatizadas o asistidas por inteligencia artificial que incidan en derechos, intereses legítimos o servicios esenciales, la persona afectada tiene derecho a: a) Solicitar una explicación significativa de los criterios generales que influyeron en la decisión. b) Obtener la revisión de la decisión por una persona humana competente.

Artículo 5. – Registro Nacional de Sistemas de Inteligencia Artificial de Alto Riesgo
Créase el Registro Nacional de Sistemas de Inteligencia Artificial de Alto Riesgo, de carácter obligatorio, a cargo del órgano rector del Sistema Nacional de Transformación Digital. El registro contiene información mínima sobre: a) Identificación del sistema y responsable. b) Finalidad y sector de aplicación. c) Categoría de riesgo. d) Medidas de mitigación y supervisión humana. e) Incidentes relevantes reportados. La información del registro es pública, salvo aquella protegida por secreto comercial, seguridad nacional o datos personales.

Artículo 6. – Evaluación de Impacto de Sistemas de Inteligencia Artificial
La implementación o uso de sistemas de inteligencia artificial de alto riesgo requiere, de manera previa, la elaboración de una Evaluación de Impacto Algorítmico, que identifique y analice: a) Riesgos para los derechos fundamentales. b) Sesgos, errores y limitaciones del sistema. c) Calidad y origen de los datos. d) Medidas de mitigación y monitoreo continuo. La evaluación es revisable periódicamente y obligatoria ante modificaciones sustanciales del sistema.

Artículo 7. – Auditoría de sistemas de inteligencia artificial
Los sistemas de inteligencia artificial de alto riesgo están sujetos a auditorías técnicas y éticas, internas y externas, conforme a los estándares que establezca la autoridad competente, sin perjuicio de las funciones de control de los órganos del Sistema Nacional de Control.

Artículo 8. – Responsabilidad por daños derivados del uso de inteligencia artificial
El desarrollador, proveedor u operador de un sistema de inteligencia artificial responde por los daños causados cuando: a) Incumpla las obligaciones de gestión de riesgos, transparencia o supervisión humana. b) Omita la evaluación de impacto exigida. c) No garantice la trazabilidad y documentación del sistema. En los sistemas de alto riesgo, la carga de la prueba se rige por criterios de razonabilidad y asimetría informativa, conforme a ley.

Artículo 9. – Transparencia en contenidos generados por inteligencia artificial
El contenido sintético generado por inteligencia artificial que pueda inducir a error razonable sobre su origen debe ser debidamente identificado, conforme a las disposiciones reglamentarias. Se prohíbe la generación o difusión de contenidos sintéticos destinados a la suplantación de identidad, fraude o afectación de derechos fundamentales.

Artículo 10. – Estándares mínimos en la contratación pública de sistemas de inteligencia artificial *Toda contratación pública que involucre sistemas de inteligencia artificial debe incorporar cláusulas mínimas sobre:*
a) Transparencia y documentación técnica.
b) Gestión de riesgos y auditoría.
c) Protección de datos y seguridad.
d) Trazabilidad, interoperabilidad y salida tecnológica

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

Primera. – Modificación del Título Preliminar de la Ley N° 31814
Se modifica el artículo único del Título Preliminar la Ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país incorporando el literal g), en los términos siguientes:

*"**Artículo único. Principios para el desarrollo y uso de la inteligencia artificial***
Son principios para el desarrollo y uso de la inteligencia artificial:
[...]
g) Transparencia algorítmica y rendición de cuentas: los sistemas de inteligencia artificial deben ser diseñados, implementados y utilizados de manera que sus finalidades, criterios generales de funcionamiento, fuentes de datos relevantes, niveles de intervención humana y responsables institucionales sean identificables, verificables y explicables, permitiendo la supervisión, fiscalización y atribución de responsabilidades por sus resultados y efectos."
Segunda. – Incorporación de artículo nuevo en la Ley N° 31814

V°B°
Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

V°B°
Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

Se incorpora el artículo 6 a la Ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, en los siguientes términos:

"Artículo 6. Fiscalización del uso de sistemas de inteligencia artificial El incumplimiento de las obligaciones, principios y deberes establecidos en la presente ley, su reglamento y normas complementarias es fiscalizable y sancionable conforme a los regímenes administrativos sectoriales aplicables, sin perjuicio de la responsabilidad civil o penal que pudiera corresponder."

DISPOSICIONES COMPLEMENTARIAS Y FINALES

Primera. – Adecuación normativa
El Poder Ejecutivo adecúa el Reglamento de la Ley N° 31814, aprobado mediante Decreto Supremo N°115-2025-PCM, a lo dispuesto en la presente ley en un plazo no mayor de ciento veinte (120) días hábiles.

Segunda. – Financiamiento
La implementación de la presente ley se financia con cargo al presupuesto institucional de las entidades competentes, sin demandar recursos adicionales al Tesoro Público.

2.4 En lo concerniente a su exposición de motivos, se menciona la necesidad de complementar el marco legal vigente que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, a efectos de reforzar los mecanismos de transparencia, control, supervisión y responsabilidad, particularmente en aquellos supuestos en los que el uso de sistemas de inteligencia artificial incide de manera significativa en derechos fundamentales, servicios esenciales o decisiones con efectos jurídicos relevantes.

En ese sentido, la propuesta busca fortalecer el marco legal aplicable, estableciendo parámetros generales vinculantes para la transparencia algorítmica, la gestión de riesgos, la evaluación de impacto, la auditoría, la fiscalización y la responsabilidad derivada del uso de sistemas de inteligencia artificial, en concordancia con los principios constitucionales, el debido procedimiento y el interés público.

2.5 Respecto al análisis costo-beneficio, se indica que la iniciativa legislativa generará costos de implementación institucional (diseño y operación del Registro Nacional de IA de Alto Riesgo; adecuación de procedimientos; contratación/fortalecimiento de capacidades para evaluaciones de impacto, auditorías y gestión de incidentes), aumento de carga administrativa inicial (estandarización documental, trazabilidad, supervisión humana), necesidad de interoperabilidad y gobernanza de datos; y, a nivel presupuestal, implica la reasignación y priorización de recursos dentro de pliegos, especialmente en PCM/SGTD y entidades usuarias intensivas.

En lo referido al beneficio, se mencionan como efectos monetarios, la reducción de costos de litigiosidad, controversias y contingencias derivadas de decisiones automatizadas opacas; disminución de pérdidas por adquisiciones/implementaciones fallidas de IA (mejor compra pública por estándares mínimos); mayor eficiencia en procesos por adopción ordenada. Asimismo, se precisa como efecto no monetario, el incremento de legitimidad institucional, confianza ciudadana, trazabilidad y control ex ante/ex post; mejora de calidad regulatoria y gobernanza digital; fortalecimiento de la seguridad jurídica en decisiones administrativas asistidas por IA. De otro lado, en lo referido al impacto presupuestal, se aduce la mejora en la asignación eficiente del gasto público digital y reducción de costos futuros por correcciones reactivas, sanciones, auditorías ex post y crisis reputacionales.

2.6. Ahora bien, desde la perspectiva de la competencia y atribuciones de la Contraloría General de la República, si bien la exposición de motivos de la iniciativa legislativa precisa que la implementación de mecanismos de gobernanza y supervisión de sistemas de inteligencia artificial requerirá que las entidades incorporen criterios de evaluación, trazabilidad y gestión de riesgos tecnológicos dentro de sus procesos internos. Ello supondrá acciones de adecuación institucional y fortalecimiento de capacidades que deberán ser financiadas con

V°B°
Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

V°B°
Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

cargo al presupuesto aprobado de cada pliego, sin demandar recursos adicionales al Tesoro Público.

2.7. En ese contexto, si bien el objeto de la iniciativa legislativa materia de opinión no se encuentra referido al control gubernamental, su contenido contempla disposiciones que impactarían en las entidades del Estado en general; en tal sentido, con fines orientadores e ilustrativos, se emite la presente opinión legal.

3. ANÁLISIS Y COMENTARIOS AL PROYECTO DE LEY

a) Gobernanza, Calidad y Trazabilidad en el Ciclo de Vida del Dato

3.1 Los sistemas de IA son altamente dependientes de la calidad y el manejo de los datos con los que operan, por lo que la legislación debería normar la obligatoriedad de registrar de forma auditable todo el recorrido de la información, desde su recolección inicial y clasificación, hasta la fase de entrenamiento y el despliegue operativo del modelo. Esta trazabilidad y el análisis minucioso del linaje de datos[1] constituyen un control necesario para prevenir y detectar ataques de envenenamiento de datos[2], donde un actor malicioso altera el conjunto de entrenamiento para sesgar el comportamiento del modelo.

3.2 De igual manera, se deberían definir políticas estrictas para la retención y eliminación segura de los datos utilizados en el ciclo de vida de la IA, asegurando que los repositorios cumplan con la protección de activos. El diseño técnico de los sistemas implementados por el Estado debería permitir registrar y reconstruir de forma transparente la lógica que llevó a una salida o decisión específica, garantizando el derecho del ciudadano a recibir una explicación clara sobre el resultado.

b) Protección de Datos Personales y Privacidad por Diseño

3.3 El tratamiento de datos personales por parte de sistemas de IA en las entidades públicas debe estar subordinado a los principios de finalidad, proporcionalidad y minimización de la información. Las entidades públicas deberían asegurar que los datos personales de los ciudadanos solo sean procesados únicamente cuando no exista una alternativa técnica viable que permita el uso de datos anonimizados o seudonimizados, mediante la implementación técnicas avanzadas de Privacidad por Diseño y por Defecto[3] desde las etapas iniciales de la concepción del algoritmo.

3.4 Para mitigar los riesgos asociados al cruce masivo de datos estatales, la ley debería exigir la aplicación de mecanismos de anonimización irreversible o privacidad diferencial antes de que la información alimente las capas de entrenamiento de la IA. Asimismo, se deberían establecer salvaguardas técnicas para evitar que los sistemas de IA de carácter generativo o predictivo deduzcan, almacenen o expongan de forma no autorizada categorías especiales de datos sensibles (como salud, biometría u opiniones políticas) a partir de datos comunes proporcionados por el usuario durante la realización de sus trámites remotos.

c) Seguridad contra Ataques Específicos de IA (Resiliencia del Modelo)

3.5 La IA introduce nuevos vectores de amenaza y vulnerabilidades técnicas en sus componentes lógicos que los firewalls y herramientas de seguridad convencionales no están diseñados para mitigar; por tanto, la ley debería exigir que las entidades públicas sometan sus sistemas de

V°B°
Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

[1] El linaje de datos se define como la especificación técnica que describe el ciclo de vida completo de los datos, permitiendo rastrear de forma exacta su origen, los flujos de movimiento entre sistemas y las transformaciones aplicadas a lo largo de su procesamiento (ISO, 2023).

[2] El envenenamiento de datos es un ataque adversario contra sistemas de aprendizaje automático que consiste en la manipulación deliberada del conjunto de datos de entrenamiento mediante la introducción de información falsa, modificada o maliciosa, con el objetivo de alterar el comportamiento del modelo final y corromper sus predicciones o clasificaciones (National Institute of Standards and Technology, 2024).

[3] La Privacidad por Diseño y por Defecto es un enfoque estratégico en la ingeniería de sistemas que exige integrar las salvaguardas de protección de datos personales desde la fase inicial de concepción y diseño de cualquier software, proceso o plataforma tecnológica (por diseño), garantizando además que, de manera automática, solo se traten los datos estrictamente necesarios para el fin específico, sin requerir la intervención activa del usuario (por defecto) (Agencia Española de Protección de Datos, 2020).

V°B°
Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

IA a pruebas y validaciones adecuadas periódicas para evitar que perturbaciones maliciosas imperceptibles en los datos de entrada hagan fallar las decisiones del modelo.

3.6 En el caso de las entidades que implementen asistentes virtuales o agentes basados en modelos de lenguaje, la legislación debería obligar al uso de filtros estrictos de entrada y salida para evitar incidentes de inyección de comandos, donde usuarios externos manipulan las instrucciones base del sistema. Adicionalmente, se deberían implementar controles de acceso y límites en las consultas automatizadas para impedir que atacantes ejecuten técnicas de inversión o extracción de modelos, las cuales buscan reconstruir los datos privados de entrenamiento o robar el algoritmo institucional.

d) Gestión de Riesgos de Terceros y Continuidad Tecnológica

3.7 El sector público depende frecuentemente de soluciones provistas por terceros, tales como software comercial cerrado o servicios en la nube, por lo que sería recomendable que la ley establezca la obligatoriedad de suscribir acuerdos de nivel de servicio que definan claramente las responsabilidades de seguridad del proveedor. Para mitigar el riesgo de dependencia tecnológica y asegurar la continuidad operativa de la infraestructura ante una interrupción prolongada, las entidades deberían exigir contratos de custodia de código fuente o planes de contingencia tecnológica equivalentes.

3.8 Las metodologías de análisis de riesgos tradicionales de la organización deberían actualizarse para abordar la naturaleza dinámica y el comportamiento probabilístico de los algoritmos de IA. Las entidades públicas deberían realizar un proceso formal de Valoración de Riesgos de Seguridad de la Información específico para IA antes de su adquisición o desarrollo, midiendo los impactos asociados a sesgos algorítmicos, fallas de precisión, dependencias de datos y pérdida de control operativo.

e) Clasificación de Sistemas de IA por Niveles de Riesgo

3.9 La legislación debería adoptar un enfoque de gestión basado en el riesgo que catalogue las aplicaciones de IA según su impacto potencial en la seguridad de la información y los derechos fundamentales de las personas. Bajo este criterio, quedarían estrictamente prohibidos los sistemas de IA de riesgo inaceptable, tales como la puntuación social administrada por el Estado o los sistemas de vigilancia masiva descontrolada que vulneren las garantías constitucionales.

3.10 Los sistemas catalogados como de "Alto Riesgo", como los aplicados a infraestructura crítica, administración de justicia, salud pública o identificación biométrica, deberían estar sujetos a la máxima rigurosidad de control, requiriendo una Evaluación de Impacto en la Protección de Datos previa y auditorías de seguridad anuales obligatorias. Por el contrario, las aplicaciones de riesgo bajo o mitigado, como las herramientas de soporte administrativo interno o indexadores de búsqueda, solo deberían cumplir con directrices generales de transparencia y buenas prácticas de TI.

f) El Papel Humano en las Decisiones Finales y Modelo RASCI

3.11 Para evitar la automatización descontrolada, la legislación debería exigir la implementación de mecanismos de supervisión humana activa orientados a prevenir o minimizar los riesgos de seguridad, alucinaciones y sesgos operativos del sistema, (como *Human-in-the-loop* o *Human-on-the-loop*[4]). En el caso específico de los sistemas de IA diseñados para asistir en la toma de decisiones, la legislación debería garantizar que el resultado del algoritmo sea considerado únicamente como un insumo informativo o una recomendación técnica no

Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

[4] Los enfoques Human-in-the-loop (humano en el bucle) y Human-on-the-loop (humano sobre el bucle) definen el nivel de intervención humana en sistemas automatizados de toma de decisiones; en el modelo in-the-loop, la máquina genera una recomendación, pero se requiere obligatoriamente la validación o acción directa del operador humano para ejecutar cada decisión, mientras que en el modelo on-the-loop, el sistema opera y toma decisiones de forma autónoma.

Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

vinculante, prohibiendo explícitamente que la herramienta sustituya el juicio crítico o la potestad discrecional del servidor público.

3.12 El diseño técnico de los flujos de trabajo debería obligar a que el personal calificado verifique de forma independiente las premisas y lógicas utilizadas por la IA antes de proceder a la ejecución de cualquier acto administrativo con efectos jurídicos, garantizando asimismo el derecho del ciudadano a impugnar la decisión y solicitar una revisión estrictamente humana. Con la finalidad de formalizar estos niveles de participación en el sector público, las funciones y obligaciones técnicas se podrían estructurar bajo el modelo de la matriz RASCI[5]

- **Responsable:** El funcionario público o unidad orgánica encargada de operar la herramienta de IA en el día a día. En los sistemas de asistencia, este rol tiene la obligación legal de revisar de forma independiente la sugerencia del algoritmo antes de elevarla, poseyendo la facultad plena de ignorar o corregir la salida de la máquina si detecta anomalías o sesgos en el procesamiento.

- **Aprobador:** El funcionario de alta dirección que posee la autoridad y asume la responsabilidad administrativa, legal y técnica final por los actos emitidos o asistidos por la IA, considerando que la decisión final es un acto estrictamente humano e indelegable por ley, y que el uso de una recomendación algorítmica errónea no exime al funcionario de su responsabilidad.

- **Soporte:** La unidad orgánica o el equipo técnico encargado de proveer la infraestructura, aplicar los parches de seguridad, monitorear el tráfico de red, evitar desvíos del modelo (*Data Drift*) y garantizar la resiliencia tecnológica del sistema.

- **Consultado:** Los roles especializados de gobernanza y control normativo, quienes deben evaluar de forma previa los riesgos de seguridad, la privacidad por diseño y la conformidad legal del modelo antes de su despliegue en producción.

- **Informado:** Los ciudadanos y los usuarios internos de la institución, quienes tienen el derecho a ser notificados de manera clara y explícita cuando una resolución que afecte sus intereses haya sido generada o asistida por un proceso automatizado

g) **Roles Clave de Gobernanza: Oficial de Seguridad y Confianza Digital y Oficial de Datos Personales**

3.13 Para garantizar la correcta segregación de funciones exigida por estándares como el ISO/IEC 27001:2022, la ley debería definir roles especializados con autonomía suficiente para supervisar la conformidad de los sistemas de IA. Estos roles se integran en la matriz RASCI en la condición de Consultado, obligatorios durante el diseño, y Soporte, estratégico en el monitoreo continuo, dividiendo sus competencias de la siguiente manera:

1. Oficial de Seguridad y Confianza Digital (OSCD)

El OSCD podría supervisar la implementación de los controles requeridos para fortalecer la resiliencia y la integridad de los modelos de IA dentro de la entidad pública. Sus competencias específicas bajo esta ley podrían incluir:

- **Validación de la Resiliencia Lógica:** Liderar y supervisar la ejecución de las valoraciones de riesgo específicas para IA indicadas en el literal d), exigiendo la documentación técnica que demuestre que el modelo está protegido contra ataques adversarios, inyección de comandos y extracción de datos.

[5] La matriz RASCI es una herramienta de gestión y diseño organizacional utilizada para asignar de forma inequívoca los roles y responsabilidades en la ejecución de procesos o proyectos; sus siglas corresponden a las cinco funciones asignables: Responsable de la ejecución (Responsible), Autoridad que aprueba y rinde cuentas (Accountable), Soporte operativo (Support), Consultado para aportar conocimiento (Consulted) e Informado sobre los resultados (Informed) (ISACA, 2019).

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

- **Auditoría del Linaje Técnico:** Verificar la seguridad en la trazabilidad y el linaje de datos en las fases de entrenamiento y despliegue, asegurando que los registros de eventos del sistema permitan realizar auditorías forenses ante incidentes de seguridad.

- **Mecanismos de Interrupción de Emergencia:** Autorizar y supervisar los protocolos de apagado seguro cuando el monitoreo técnico revele desvíos que pongan en peligro la precisión y seguridad de las operaciones del Estado

2. Oficial de Datos Personales (ODP)

El ODP actúa como el custodio del derecho fundamental a la privacidad de los ciudadanos, asegurando el cumplimiento normativo en el tratamiento de datos por parte de los algoritmos. Sus competencias específicas bajo esta ley podrían incluir:

- **Supervisión de la Privacidad por Diseño:** Fiscalizar que las áreas técnicas implementen de forma efectiva los controles de minimización, anonimización avanzada y privacidad diferencial antes de que cualquier base de datos institucional sea procesada por una IA.

- **Aprobación de la Evaluación de Impacto (EIPD):** Dirigir, evaluar y emitir el dictamen de conformidad de la Evaluación de Impacto en la Protección de Datos obligatoria para sistemas de alto riesgo, garantizando que el uso del algoritmo no genere sesgos discriminatorios ni afecte los derechos y libertades de las personas.

- **Garante de los Derechos Ciudadanos:** Asegurar el establecimiento de canales accesibles para que los ciudadanos ejerzan sus derechos de acceso, rectificación y, específicamente, el derecho a la oposición frente a decisiones automatizadas asistidas por IA, actuando como el canal de escalamiento ante quejas por sesgos o falta de explicabilidad en las decisiones.

3.14 El artículo 4 del proyecto de Ley establece el reconocimiento del derecho de toda persona a obtener una explicación y solicitar la revisión humana de las decisiones adoptadas con asistencia de IA. Esta disposición impacta directamente en los sistemas con componentes de inteligencia artificial que se desarrollen o mantengan, los cuales deberán incorporar en su diseño flujos que garanticen la validación humana antes de que sus resultados produzcan efectos, implicando los ajustes necesarios en la arquitectura de aplicaciones y en los estándares del ciclo de vida de los sistemas institucionales.

3.15 La propuesta de redacción contenida en el artículo 6 del proyecto de ley que exige de forma obligatoria la elaboración previa de una evaluación de impacto algorítmico para los sistemas de Inteligencia Artificial (IA) de alto riesgo, requiriendo un análisis estricto sobre la "calidad y origen de datos", es una propuesta positiva debido a que dota a las unidades orgánicas de tecnologías de la información de cada entidad pública un respaldo legal para imponer estándares estrictos de gobernanza de datos dentro de la institución.

V°B°

Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

3.16 El proyecto de ley propone incorporar a través de una modificatoria de la Ley N° 31814, Ley que promueve el uso de inteligencia artificial a favor del desarrollo económico y social del país, el principio de "transparencia algorítmica y rendición de cuentas", estableciendo que los criterios de funcionamiento, fuentes de datos y niveles de intervención humana deben ser plenamente identificables y explicables, lo cual consideramos sería un avance positivo, dado que se tendría un marco claro de diseño, ya que los principios actúan como una guía de desarrollo seguro y ético, permitiendo que los sistemas sean verificables y que se puedan atribuir responsabilidades por sus efectos.

3.17 El artículo 7 del proyecto de ley regula a la auditoria de sistemas de inteligencia artificial, estableciendo que los sistemas de IA de alto riesgo estarán sujetos a auditoria técnicas y éticas, internas y externas, precisando que esto se da "sin perjuicio de las funciones de control

V°B°

Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

de los órganos del Sistema Nacional de Control". Al respecto, consideramos que el proyecto de ley valida e impulsa la necesidad de que la Contraloría General de la República modernice sus enfoques de fiscalización hacia el control de algoritmos, en ese sentido, esta tendría un rol protagónico al diseñar las herramientas analíticas especializadas que utilizarán los auditores para fiscalizar el uso de la IA en todas las entidades sujetas a control.

3.18 El artículo 10 del proyecto de ley define los Estándares mínimos en la contratación pública de sistemas de inteligencia artificial, obligando a las entidades públicas incluir cláusulas de transparencia y documentación técnica, gestión de riesgos y auditoría, protección de datos y seguridad, y trazabilidad, interoperabilidad y salida tecnológica. Al respecto, dichas cláusulas mínimas son aspectos positivos de mejora que garantizarán que cualquier solución adquirida sea totalmente compatible con la infraestructura técnica institucional y los estándares de interoperabilidad del Estado.

4. CONCLUSIONES

4.1 El Proyecto de Ley N° 14544/2025-CR, "Proyecto de ley que complementa y fortalece el marco de gobernanza, transparencia, control y responsabilidad en el uso de la inteligencia artificial", no se encuentra referido al control gubernamental; no obstante, su contenido contempla disposiciones que impactarían en las entidades públicas en general; en tal sentido, se emiten comentarios y aportes con carácter orientador para consideración.

4.2 El proyecto de ley introduce disposiciones que impactan directamente en el diseño, desarrollo y operación de los sistemas que incorporan inteligencia artificial, destacando la incorporación del derecho a la explicación y revisión humana de las decisiones automatizadas, lo que implica la necesidad de adecuar los sistemas institucionales para garantizar mecanismos de validación humana.

4.3 Se resalta la exigencia de evaluaciones de impacto algorítmico en sistemas de alto riesgo, el fortalecimiento de la gobernanza de datos, la incorporación del principio de transparencia algorítmica y la regulación de auditorías técnicas y éticas de los sistemas de inteligencia artificial, lo que contribuiría con modernizar los enfoques de fiscalización de la Contraloría General de la República.

4.4 Se destacan los estándares mínimos propuestos para la contratación de soluciones de inteligencia artificial, orientados a garantizar interoperabilidad, trazabilidad y seguridad, advirtiéndose que la implementación de estas disposiciones requerirá el fortalecimiento de la infraestructura tecnológica y el desarrollo de capacidades especializadas.

4.5 Desde la perspectiva de la seguridad de la información, la adopción de inteligencia artificial en el sector público requiere un marco normativo que garantice la confidencialidad, integridad y disponibilidad de los sistemas y datos.

4.6 En ese contexto, se propone el fortalecimiento de la trazabilidad del ciclo de vida de los datos, la implementación de principios de privacidad por diseño, y la adopción de medidas de seguridad específicas frente a amenazas propias de la inteligencia artificial, tales como ataques adversarios o manipulación de modelos.

CONTRALORÍA V°B°
Firmado digitalmente por PACHECO CASTRO Joao Manuel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:26:04 -05:00

4.7 Asimismo, se plantea la necesidad de gestionar adecuadamente los riesgos asociados a terceros y asegurar la continuidad tecnológica, clasificar los sistemas de IA según niveles de riesgo, y reforzar el rol humano en la toma de decisiones mediante mecanismos de supervisión. Del mismo modo, se propone la incorporación de roles especializados como el Oficial de Seguridad y Confianza Digital y el Oficial de Datos Personales, orientados a garantizar el cumplimiento de las exigencias técnicas y normativas.

CONTRALORÍA V°B°
Firmado digitalmente por BERTOLA VALDIVIA Karen Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

4.8 El proyecto de ley constituye un avance significativo en el fortalecimiento del marco normativo sobre inteligencia artificial, al incorporar principios orientados a la transparencia, control, responsabilidad y seguridad; no obstante, su implementación implicará importantes retos institucionales relacionados con la adecuación de la arquitectura tecnológica, el

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe

fortalecimiento de la gobernanza de datos, la implementación de controles especializados y el desarrollo de capacidades en materia de inteligencia artificial y auditoría de algoritmos.

****

Firmado digitalmente por
PACHECO CASTRO Joao Manuel
FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 16:28:04 -05:00

Firmado digitalmente por
BERTOLA VALDIVIA Karen
Raquel FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 04-06-2026 15:14:10 -05:00

Jr. Camilo Carrillo 114 - Jesús María Lima 11, Lima - Perú
Central: +511 330-3000
www.contraloria.gob.pe