

Borrador de Código de Ética de la Inteligencia Artificial para los Servicios Públicos de la República Dominicana¹

Esta versión: 31 de Marzo de 2026. Incorpora insumos del taller ecosistémico (90 participantes, 24 de febrero de 2026) y consulta pública (76 respuestas).

Preámbulo

Este Código de Ética de la Inteligencia Artificial (IA) aplica a todas las instituciones de la Administración Pública de la República Dominicana que diseñen, adquieran, utilicen o supervisen sistemas de IA o decisiones automatizadas en la provisión de servicios públicos. Complementa el Código de Integridad del Sector Público y desarrolla el Objetivo 1.2.3 de la Estrategia Nacional de Inteligencia Artificial (ENIA), que establece la necesidad de un código ético para el diseño y uso de la IA. Se inspira en la ENIA, la Recomendación de la UNESCO sobre la Ética de la IA y en los principios de IA de la OCDE, y se fundamenta en el diagnóstico nacional de ética de la IA, asegurando que los principios respondan directamente al contexto institucional de la República Dominicana.

Este Código es el resultado de un proceso de co-creación ciudadana que incluyó un taller ecosistémico con 90 participantes y una consulta pública con 76 respuestas de servidores públicos, academia, sociedad civil y sector privado (enero-febrero 2026). Su diseño en tres partes busca garantizar que los principios éticos se traduzcan en reglas concretas y en responsabilidades con capacidad de implementación.

I. PRINCIPIOS ÉTICOS PARA LA IA EN LOS SERVICIOS PÚBLICOS

1. Servicio al interés público y derechos humanos

La IA en el sector público debe utilizarse exclusivamente para promover el bienestar de la población, fortalecer la democracia, a través del empoderamiento de la deliberación individual y colectiva, y garantizar la protección de los derechos reconocidos en la Constitución, los tratados internacionales y el Código de Integridad del Sector Público. Queda prohibido emplear sistemas de IA para fines incompatibles con estos valores y derechos, como vigilancia masiva indiscriminada, persecución política o prácticas que vulneren la dignidad humana o violen el marco jurídico y constitucional.

2. Equidad, inclusión y no discriminación

Los sistemas de IA deberán diseñarse, entrenarse y evaluarse para evitar sesgos injustos y disparidades de trato por motivos de género, origen étnico, color de piel, nacionalidad, condición socioeconómica, discapacidad, territorio, edad u otras

¹ Preparado por Carla Bonina, Consultora Técnica, Alianza para el Gobierno Abierto.

condiciones protegidas. Las instituciones priorizarán usos de IA que contribuyan a reducir brechas y desigualdades, en coherencia con la ENIA y la Agenda Digital.

La equidad exige que los sistemas de IA evalúen a cada persona por sus circunstancias y méritos individuales. El uso de patrones históricos colectivos que perpetúen desventajas estructurales de grupos o territorios es contrario a este principio.

3. Transparencia, explicabilidad y trazabilidad

La ciudadanía tiene derecho a saber cuándo una decisión administrativa ha sido apoyada por sistemas de IA, a comprender su finalidad y a recibir explicaciones claras y comprensibles sobre los factores y razones principales que influyen en decisiones que le afecten significativamente. Todos los sistemas de IA utilizados en servicios públicos deberán ser documentados de forma que se pueda reconstruir su funcionamiento y evolución a lo largo del tiempo.

La transparencia no se limita a la publicación de información técnica: implica la capacidad real de la ciudadanía de comprender, cuestionar y corregir las decisiones apoyadas en IA. Una explicación que no puede ser entendida por la persona afectada no cumple este principio.

4. Privacidad, protección de datos y seguridad

Cualquier uso de IA deberá respetar estrictamente las normas y el derecho de la República Dominicana, especialmente los derechos y deberes en relación a la protección de datos personales y los estándares de seguridad de la información del Estado. Los sistemas deberán diseñarse con minimización de datos, medidas de seguridad desde el diseño y planes de respuesta ante incidentes que puedan afectar a la confidencialidad, integridad o disponibilidad de la información.

5. Robustez técnica, soberanía digital y gestión responsable del riesgo

Los sistemas de IA en el sector público deben ser técnicamente robustos, confiables y sometidos a pruebas, monitoreo y revisión periódica, especialmente en casos de alto impacto social. El Estado dominicano debe mantener soberanía efectiva sobre los sistemas de IA que utiliza para gobernar. La dependencia tecnológica que elimine la capacidad del Estado de conocer, auditar, corregir o retirar los sistemas que operan en su nombre es incompatible con el ejercicio democrático de las funciones públicas.

6. Responsabilidad, rendición de cuentas y sostenibilidad

Siempre debe existir una autoridad humana claramente identificada y responsable de las decisiones apoyadas por IA. La ciudadanía deberá contar con vías accesibles para impugnar decisiones automatizadas, solicitar revisión humana y participar en el diálogo sobre el uso de IA en los servicios públicos.

La responsabilidad en el uso de IA pública incluye una dimensión ambiental: el Estado debe considerar y minimizar el impacto de la infraestructura tecnológica sobre los

recursos naturales y las comunidades. La búsqueda de eficiencia tecnológica no puede trasladar costos ambientales y sociales a las poblaciones más vulnerables.

II. REGLAS PRÁCTICAS PARA EL DISEÑO, ADQUISICIÓN Y USO DE IA EN SERVICIOS PÚBLICOS

7. Evaluaciones de impacto antes del despliegue

Todo sistema de IA que pueda afectar derechos, acceso a servicios esenciales, asignación de recursos públicos o el ejercicio de potestades sancionadoras deberá someterse, antes de su puesta en producción, a una Evaluación de Impacto Ético y de Derechos (EIED). La EIED deberá analizar:

- Finalidad legítima y necesidad del uso de IA.
- Riesgos para derechos, inclusión, privacidad, seguridad y confianza pública.
- Medidas de mitigación, incluidos límites de uso y supervisión humana.
- Alternativas no automatizadas o menos intrusivas.
- Impacto ambiental: consumo energético e hídrico estimado de la infraestructura requerida, afectaciones potenciales a comunidades cercanas y medidas de mitigación propuestas.

Ningún sistema de IA de alto impacto podrá pasar a producción sin que la EIED haya sido completada, revisada por el órgano de supervisión nacional y publicado un resumen accesible para la ciudadanía.

8. Registro institucional y portal público de sistemas de IA

Cada institución deberá mantener un registro interno de los sistemas de IA que utiliza, con información mínima sobre finalidad, tipo de datos, proveedor, área responsable, nivel de riesgo y resultados de la EIED. Un extracto de este registro será publicado periódicamente para garantizar transparencia hacia la ciudadanía, respetando los límites de seguridad nacional y protección de datos. Las excepciones a la publicación por razones de seguridad nacional deberán estar justificadas y ser estrictamente limitadas.

9. Transparencia hacia las personas usuarias

Cuando un trámite o servicio incluya decisiones significativas apoyadas por IA, la institución deberá informar de manera clara en los canales habituales (web, oficinas, formularios) que se emplea un sistema automatizado, cuál es su finalidad y cómo solicitar aclaraciones o revisión humana. En comunicaciones individuales relevantes, se indicará si la decisión ha sido asistida por IA y se ofrecerá una explicación comprensible de los factores relevantes de la decisión.

Esta obligación aplica con igual fuerza en los canales físicos de atención ciudadana, incluyendo Punto GOB y oficinas presenciales, garantizando el acceso de personas con baja conectividad o limitada alfabetización digital. Una explicación comprensible es aquella que permite a la persona afectada identificar qué dato o criterio determinó la decisión y cómo puede impugnarla, sin necesidad de conocimientos técnicos.

10. Requisitos éticos en la contratación pública

Los procesos de contratación de soluciones de IA deberán incluir cláusulas específicas que obliguen a los proveedores a cumplir este Código de Ética de IA, la normativa de protección de datos y los estándares de seguridad de la Administración Pública. Deberán exigirse evidencias suficientes sobre gestión de sesgos, documentación técnica, posibilidades de auditoría y mecanismos de actualización responsable del sistema.

Los contratos de adquisición de IA deberán garantizar:

- que los datos de ciudadanos dominicanos permanezcan bajo soberanía del Estado, con encriptación cuyas llaves de acceso sean controladas exclusivamente por el Gobierno dominicano. –
- que el Estado tenga derecho irrestricto a auditar el código y la lógica del sistema en cualquier momento durante la vigencia del contrato;
- que los proveedores cuenten con un código de ética verificable como condición contractual.

Ningún sistema de IA podrá ser desplegado en servicios públicos bajo cláusulas de confidencialidad comercial que impidan su auditoría técnica o ética. Si el proveedor no puede garantizar estas condiciones, el Estado no podrá contratar el sistema.

11. Usos prohibidos y restricciones de alto riesgo

Las instituciones públicas no podrán implantar sistemas de IA que, por su diseño o finalidad, sean incompatibles con los principios de este Código.

Quedan estrictamente prohibidos los siguientes usos de IA en el sector público:

- Sistemas de *scoring* o clasificación social generalizada de ciudadanas y ciudadanos para determinar su acceso a derechos, servicios públicos o su tratamiento diferenciado por parte del Estado.
- Identificación biométrica masiva e indiscriminada en espacios públicos —incluyendo reconocimiento facial, de voz o de marcha— sin orden judicial específica, finalidad legítima claramente definida, base legal suficiente y supervisión independiente.
- Perfilamiento criminal predictivo que clasifique a personas como potenciales infractores en función de su lugar de residencia, origen étnico, condición socioeconómica o historial territorial, en violación del principio de presunción de inocencia y el debido proceso.

- Sistemas que recomienden, determinen o ejecuten de forma autónoma sentencias penales, medidas de coerción o privación de libertad sin intervención humana directa y garantías plenas del debido proceso.
- Uso de IA para manipulación del comportamiento ciudadano, incluyendo propaganda política, desinformación institucional o técnicas de influencia encubierta desde el Estado.
- Sistemas de armas autónomas o cualquier aplicación de IA que pueda decidir causar daño físico o letal a personas sin intervención humana directa, deliberada y responsable.
- Cualquier sistema de IA desplegado sin base legal clara, sin evaluación de impacto previa documentada, sin responsable institucional identificado y sin mecanismo de auditoría independiente activo.

Los usos de alto riesgo no incluidos en esta lista, que sean definidos como tales por la ENIA o por futuras leyes, deberán someterse a criterios reforzados de evaluación, supervisión y autorización expresa antes de su despliegue.

11.1. Restricciones especiales en niñez, infancias y juventudes

Cualquier uso de IA que tenga como público objetivo principal, o como usuarios previsibles, a niñas, niños o adolescentes queda prohibido hasta que haya evidencia científica suficiente, la cual dará certeza de que el riesgo es mínimo o nulo.

Se exceptúan de esta prohibición los usos de IA expresamente diseñados para proteger a niñas, niños y adolescentes de riesgos en línea, como la detección de contenido abusivo o la alerta temprana de situaciones de violencia, siempre que cuenten con EIED específica, supervisión humana permanente y aprobación expresa del órgano nacional de supervisión. Queda absolutamente prohibido el uso de IA que genere, facilite o distribuya contenido sexualizado o denigrante de niñas, niños o adolescentes, incluso si es de naturaleza sintética o generada artificialmente.

12. Mecanismos de recurso y corrección

Las personas afectadas por decisiones significativas apoyadas por IA tendrán derecho a:

- Solicitar información adicional sobre el proceso de decisión.
- Pedir revisión humana de la decisión.
- Presentar quejas o recursos administrativos por los canales habituales.

Las instituciones deberán establecer procedimientos de apelación para aquellos que arguyen su derecho a una decisión humana así como para corregir errores sistémicos detectados en los sistemas de IA y notificar a las personas afectadas cuando corresponda.

III. RESPONSABILIDADES, GOBERNANZA Y SEGUIMIENTO

13. Responsabilidad de las máximas autoridades y alineación con el Código de Integridad

Las máximas autoridades de cada institución son responsables de garantizar el cumplimiento de este Código y su coherencia con el Código de Integridad del Sector Público de la República Dominicana. Cada entidad deberá integrar la ética de la IA en sus políticas internas de integridad, gestión de riesgos, tecnología y protección de datos.

El incumplimiento de las obligaciones establecidas en este Código por parte de las máximas autoridades institucionales constituirá una falta administrativa grave, sujeta a los mecanismos de sanción previstos en el Código de Integridad del Sector Público y otra normativa aplicable.

14. Roles internos y capacidad institucional

Cada institución identificará:

- Una unidad responsable de la gobernanza de IA (por ejemplo, TIC, gobernanza de datos, o una unidad específica de transformación digital).
- Personas responsables de cada sistema de IA en operación (propietarios del servicio).

El Estado fomentará la formación continua en ética de IA, protección de datos, sesgos algorítmicos y evaluación de impacto para funcionarios involucrados en diseño, contratación, uso y auditoría de sistemas de IA, en coherencia con la ENIA.

La formación en ética de IA será requisito obligatorio para los funcionarios que lideren, contraten, supervisen u operen sistemas de IA de alto impacto. Ningún funcionario podrá validar ni firmar la puesta en producción de un sistema de IA de alto impacto sin haber completado dicha formación. El Estado desarrollará además programas accesibles y gratuitos de alfabetización en IA y derechos digitales dirigidos a la ciudadanía general, con especial atención a grupos históricamente excluidos.

15. Órgano de supervisión y coordinación nacional

El órgano que se designe en el marco de la ENIA (por ejemplo, un Consejo o Comité Nacional de IA) tendrá la responsabilidad de:

- Emitir lineamientos complementarios y modelos de EIED.
- Fomentar buenas prácticas y el intercambio de experiencias entre instituciones.
- Monitorear el cumplimiento general del Código.
- Gestionar el portal público de transparencia de IA del Estado, de acceso abierto, garantizando su actualización permanente.

- Recibir, investigar y dar respuesta pública a denuncias ciudadanas sobre posibles incumplimientos del Código, con capacidad de recomendar correcciones y proponer sanciones a las autoridades competentes.
- Aprobar las EIED de sistemas de alto riesgo antes de su despliegue y llevar un registro público de los sistemas aprobados, aprobados con condiciones y rechazados.
- Garantizar la actualización periódica y participativa del Código, con un ciclo de revisión mínimo de dos años, incorporando avances tecnológicos, jurisprudencia emergente y aprendizajes de la implementación.

16. Participación ciudadana y colaboración internacional

El Estado garantizará la participación activa y continua de la ciudadanía en la gobernanza ética de la IA pública a través de los siguientes mecanismos:

- Consejo Ciudadano de Ética de IA: espacio multi-actor, consultivo y permanente, integrado por representantes de sociedad civil, academia, sector privado, funcionariado público y ciudadanía independiente. Tendrá mandato para revisar el Código, opinar sobre sistemas de alto impacto y emitir recomendaciones públicas. Su gobernanza será de arquitectura multi-actor: ninguna entidad, pública ni privada, podrá controlarlo de forma unilateral.
- Auditorías ciudadanas de algoritmos: mecanismo formal por el cual organizaciones de sociedad civil y academia acreditadas podrán participar en la revisión de sistemas de IA, con acceso a documentación técnica suficiente para evaluar riesgos, sesgos y cumplimiento del Código, y con capacidad de publicar sus hallazgos de forma independiente.
- Sistema de alertas públicas: notificación accesible (por canales digitales y físicos) cuando el Estado adquiera, despliegue o modifique significativamente un sistema de IA de alto impacto, con plazo razonable para recibir observaciones ciudadanas antes de su entrada en vigor.
- Consultas públicas previas obligatorias: antes de desplegar sistemas de IA de alto impacto, las instituciones realizarán un proceso de consulta pública con plazos razonables, canales múltiples y publicación de los resultados, especificando cómo fueron incorporados o, en su caso, por qué no lo fueron.
- Capacitación ciudadana: el Estado desarrollará programas accesibles y gratuitos de formación en IA ética y derechos digitales dirigidos a la ciudadanía general, para que la participación en los mecanismos anteriores sea real y no meramente formal.

En el plano internacional, la República Dominicana cooperará activamente con otros países y organismos (UNESCO, OCDE, BID, región LAC, SICA) para intercambiar

experiencias, participar en foros de gobernanza de IA, actualizar estándares y promover una IA confiable y centrada en las personas.