Antes de temerle a la inteligencia artificial, comprenderla

Manifiesto y principios Yachay Deep para una adopción responsable, crítica y soberana de la inteligencia artificial en Ecuador

Carlos Vásconez-Paredes
Yachay Deep Research Institute, Cayambe, Ecuador

PUBLICADO	VERSIÓN	DOI	LICENCIA
22 de septiembre de 2026	1.1 · 19 oct. 2026	10.5281/zenodo.23489388	CC BY 4.0

RESUMEN

El debate público sobre los riesgos de la inteligencia artificial suele confundir dos planos: los riesgos sistémicos de los modelos de frontera y los riesgos sociales, educativos, laborales y de privacidad de las herramientas de uso cotidiano. Este documento sostiene que, en Ecuador, la prioridad inmediata es el segundo plano y que la respuesta no es el miedo ni la prohibición, sino la alfabetización en IA, la gobernanza institucional y la soberanía de datos. Advierte tanto contra la alarma indiscriminada como contra la adopción sin comprensión, y cierra con siete principios para la adopción responsable de la IA, propuestos como marco conceptual para su adaptación y evaluación en distintas instituciones.

Palabras clave: inteligencia artificial; alfabetización en IA; gobernanza de la IA; soberanía de datos; educación superior; Ecuador

ABSTRACT

Before fearing artificial intelligence, understand it: Yachay Deep manifesto and principles for a responsible, critical and sovereign adoption of AI in Ecuador

Public debate on the risks of artificial intelligence tends to conflate two levels: the systemic risks of frontier models and the social, educational, labour and privacy risks of everyday tools. This paper argues that Ecuador's immediate priority lies at the second level, and that the response should be neither fear nor prohibition but AI literacy, institutional governance and data sovereignty. It cautions against both indiscriminate alarm and uncritical adoption, and closes with seven principles for the responsible adoption of AI, offered as a conceptual framework to be adapted and evaluated across institutions.

Keywords: artificial intelligence; AI literacy; AI governance; data sovereignty; higher education; Ecuador

En Ecuador y en el mundo, la inteligencia artificial ha entrado con fuerza en el debate público por los riesgos que podría representar para la sociedad e incluso para la humanidad. Y está bien que ese debate exista: necesitamos discutir sus límites, sus riesgos y sus implicaciones. Pero también necesitamos poner cada riesgo en su verdadera dimensión.

Cuando escuchamos a investigadores, desarrolladores y directivos de empresas tecnológicas advertir sobre escenarios en los que la IA podría representar un riesgo para la humanidad, casi siempre hablan de algo mucho más complejo que el

ChatGPT, el Gemini o el Claude que una persona abre desde su teléfono. La preocupación se concentra en los llamados **modelos de frontera**: sistemas cada vez más potentes, con mayores niveles de autonomía y capacidades que podrían utilizarse en ámbitos como la ciberseguridad, la biotecnología, la manipulación a gran escala o el desarrollo de nuevos sistemas de inteligencia artificial.

Eso no significa que las herramientas que usamos hoy sean inofensivas. Una persona puede usar IA para redactar un correo, aprender un idioma, programar, analizar información o generar una imagen divertida. Pero esas mismas tecnologías también sirven para crear montajes convincentes, clonar voces, fabricar videos falsos, suplantar identidades, producir desinformación o cometer fraudes.

Son dos niveles distintos de riesgo, y necesitamos aprender a diferenciarlos. Una cosa es discutir los **riesgos sistémicos y potencialmente catastróficos de futuras generaciones de IA**, y otra, igualmente necesaria, discutir los **riesgos sociales, educativos, laborales, informativos y de privacidad de las herramientas que ya tenemos disponibles**.

En Ecuador, nuestra prioridad inmediata debería estar en lo segundo. No porque el debate sobre los modelos de frontera no importe, sino porque Ecuador no está en el centro de su desarrollo. Nuestra realidad es otra: millones de personas empezando a usar estas herramientas, instituciones que todavía no saben cómo incorporarlas, docentes intentando decidir qué hacer con ellas, trabajadores que ven transformarse sus actividades y organizaciones que cargan información en plataformas externas sin políticas claras sobre su uso. Ahí está nuestra discusión urgente.

De dónde viene la alarma

Conviene recordar de dónde nace buena parte de este debate. La alarma no la encendieron los usuarios, sino los propios laboratorios de frontera —Anthropic, OpenAI y xAI (Grok), entre otros— y sus líderes. En mayo de 2023, cientos de investigadores y directivos, incluidos los de estas empresas junto a figuras como Geoffrey Hinton y Yoshua Bengio, firmaron una breve declaración que situaba el riesgo de extinción por IA a la altura de las pandemias y la guerra nuclear (Center for AI Safety, 2023).

Y el debate no proviene solo de declaraciones firmadas hace años: sigue vivo y, a veces, surge desde dentro. En septiembre de 2026, Jacob Coxon —investigador que trabajó en Anthropic y OpenAI— renunció públicamente advirtiendo que las compañías están, en sus palabras, "apostando con nuestras vidas" en una carrera hacia una superinteligencia capaz de mejorarse a sí misma; según él, dentro de las empresas se comprenden bien los riesgos, pero pesa la presión de llegar primero. Sus mensajes fueron vistos por más de cien millones de personas (Huamani, 2026).

Pero —y esto es lo que se suele pasar por alto— esas mismas empresas no se quedaron en la alarma: construyeron marcos que gradúan el riesgo por nivel de capacidad. La política de escalamiento responsable de Anthropic define niveles de seguridad (ASL), inspirados en los niveles de bioseguridad: los asistentes actuales se ubican en un nivel bajo y los controles estrictos se reservan para sistemas futuros con capacidades peligrosas (Anthropic, 2023). El marco de preparación de OpenAI evalúa categorías como ciberseguridad, riesgos químicos, biológicos, radiológicos y nucleares (QBRN) y autonomía del modelo en una escala de bajo a crítico, y bloquea el despliegue por encima de cierto umbral (OpenAI, 2025). Y el marco de xAI se concentra en evitar que sus modelos ayuden a fabricar armas de destrucción masiva o a ejecutar ciberataques a gran escala (xAI, 2025).

La lección es la que atraviesa este documento: incluso quienes lanzan las alarmas más fuertes distinguen niveles. Su preocupación apunta a los modelos de frontera con capacidades peligrosas específicas —no al asistente generativo que un estudiante abre en el teléfono—. Confundir ambos planos, y tratar a cada chatbot como si fuera una amenaza existencial, es justamente el error que aquí advertimos: la alarma puede ser legítima, pero aplicada al nivel equivocado solo produce miedo y malas decisiones.

La IA no es solamente una amenaza

También debemos evitar el extremo contrario. Muchas soluciones que hace pocos años habrían exigido equipos especializados, presupuestos altos o largos periodos de desarrollo hoy pueden construirse con ayuda de inteligencia artificial. Se están reduciendo las barreras para programar, analizar grandes volúmenes de información, automatizar procesos, generar materiales educativos, apoyar la investigación y resolver problemas concretos. En un país como el nuestro, ese potencial importa.

El problema, entonces, no es simplemente usar inteligencia artificial. El problema es **usarla sin comprenderla**. Satanizar una tecnología por desconocimiento no reduce sus riesgos: aumenta el miedo, profundiza la brecha entre quienes saben usarla y quienes no, y puede terminar dejando a instituciones y personas fuera de una transformación que ya está ocurriendo.

Antes del miedo, alfabetización

Ecuador todavía enfrenta desafíos importantes de alfabetización digital y, sobre esa brecha, estamos intentando construir una alfabetización en inteligencia artificial. Antes de preguntarnos si la IA acabará con la humanidad, deberíamos asegurarnos de que las personas comprendan qué es, qué no es, cómo funciona, cuáles son sus límites, cómo verificar sus resultados y cómo proteger sus datos.

Y alfabetización en inteligencia artificial **no significa simplemente aprender a escribir buenos prompts**. Significa comprender cuándo usarla y cuándo no. Saber que puede equivocarse. Identificar sesgos. Verificar información. Reconocer contenido sintético. Proteger datos personales e institucionales. Entender qué tareas podemos delegar y cuáles exigen necesariamente criterio y responsabilidad humana. Es una competencia

crítica, no una destreza instrumental.

Las instituciones necesitan gobernanza, no miedo

Muchas escuelas, colegios, universidades, empresas y organismos reaccionan ante la IA desde el miedo: prohibirla, bloquearla o mirar hacia otro lado. Pero la inteligencia artificial no va a desaparecer porque decidamos ignorarla. En lugar de prohibir sin comprender, necesitamos **gobernar su uso**: qué información puede introducirse en estas herramientas, qué información nunca debería compartirse, cuándo debe declararse su utilización, qué decisiones necesitan supervisión humana y cuáles son los límites de su aplicación.

Y aquí conviene ser francos sobre lo que está ocurriendo en nuestras universidades. Muchas han entrado al debate sobre la IA —permitiéndola, restringiéndola, organizando charlas, emitiendo pronunciamientos— sin haber construido primero lo básico: un código de uso ético, una política de datos, un documento base que fije las reglas del juego. **El debate llegó antes que la gobernanza.** Y cuando eso ocurre, cada facultad, cada docente y cada estudiante improvisa su propio criterio, con el consiguiente riesgo para la integridad académica y para la privacidad de los datos. Un análisis reciente sobre la educación superior ecuatoriana señala precisamente este vacío de normativas internas que regulen el uso de la IA generativa (Chamba-Eras et al., 2026). La conversación es bienvenida, pero no puede sustituir al documento que debió precederla.

Ecuador ya dio un primer paso a escala nacional con su estrategia nacional de IA 2025–2029 (Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], 2026), que reconoce la gobernanza, la alfabetización y la soberanía tecnológica como prioridades. Pero una estrategia solo cobra sentido cuando baja del papel a la práctica: a reglas internas, formación, presupuesto y capacidad técnica dentro de cada organización. Ese es el trabajo que todavía está por hacerse.

Soberanía de datos e infraestructura: una decisión, no un eslogan

Todos los días cargamos documentos, textos, imágenes, investigaciones y bases de datos en plataformas de IA que funcionan sobre infraestructuras que no controlamos. Muchas veces lo hacemos sin preguntarnos dónde se procesa esa información, qué permisos concedemos o qué ocurre cuando introducimos datos institucionales, académicos o sensibles.

La soberanía de datos no es un eslogan ni exige que Ecuador construya sus propios modelos de frontera. Es una **decisión práctica** que cada institución puede tomar, sobre un espectro de opciones según la sensibilidad de la información:

- **Cláusulas contractuales** sobre los servicios comerciales que ya usamos: residencia de datos, límites de retención y la garantía de que nuestra información no se usará para entrenar modelos ajenos. Es lo mínimo exigible.
- **Nube soberana o regional** para la información de mayor sensibilidad.
- **Modelos de pesos abiertos ejecutados en infraestructura propia** (*on-premise*) para lo más sensible, de modo que los datos se procesen sin salir hacia servidores extranjeros.

Conviene decirlo con honestidad: los modelos abiertos todavía van detrás de los mejores modelos cerrados en varias tareas, y ejecutarlos localmente tiene costos reales de infraestructura y operación. Por eso lo sensato no es *todo local o nada*, sino **clasificar la información por niveles de sensibilidad** y asignar a cada nivel la opción adecuada. Una institución no necesita procesar internamente un correo trivial; sí debería pensarlo dos veces antes de cargar expedientes académicos, historias clínicas o datos personales de su comunidad en una plataforma externa.

Y hay una capa que en Ecuador solemos olvidar. Cuando trabajamos con información de comunidades o de pueblos indígenas, la soberanía no se reduce a *dónde están los servidores*, sino a *quién tiene autoridad sobre el dato y quién se beneficia de él*. Los principios CARE para la gobernanza de datos indígenas (Carroll et al., 2020) —beneficio colectivo, autoridad para controlar, responsabilidad y ética— nos recuerdan que la apertura de los datos debe equilibrarse con los derechos de las personas y comunidades a las que esos datos pertenecen. Para un país plurinacional, esa no es una nota al pie: es parte del centro.

Distinguir para decidir

El debate sobre los riesgos futuros de la IA es necesario. Pero no debería distraernos de los problemas y oportunidades que ya tenemos delante. Necesitamos distinguir entre **la IA que usamos, la IA que estamos construyendo y la IA que podríamos llegar a construir**. Cada una plantea preguntas diferentes.

Para Ecuador, quizá la pregunta más urgente no sea si algún día una inteligencia artificial podría escapar de nuestro control:

> *Antes de temerle a la IA, necesitamos comprenderla.*
>
> *Antes de prohibirla, necesitamos aprender a gobernarla.*
>
> *Antes de confiar ciegamente en ella, necesitamos aprender a cuestionarla.*
>
> *Y antes de entregarle nuestros datos, necesitamos decidir quién los controla y para qué pueden utilizarse.*

El mayor riesgo para Ecuador quizá no sea que la inteligencia artificial avance demasiado rápido, sino que nosotros lleguemos demasiado tarde a comprenderla, gobernarla y utilizarla para construir nuestro propio futuro.

Principios Yachay Deep para la adopción responsable de la IA

Estos principios constituyen un marco que otras instituciones pueden interpretar, implementar y evaluar. No se proponen como un modelo empíricamente validado, sino como un marco conceptual susceptible de adaptación, discusión y evaluación en distintos contextos institucionales.

1. **Proporcionalidad del riesgo.** No todos los sistemas ni todos los usos de IA presentan el mismo nivel de riesgo. Regular con la misma vara un asistente de escritura y un sistema que decide sobre personas produce normas inaplicables o injustas. La respuesta proporcional gradúa las exigencias —transparencia, supervisión y evaluación— según el impacto real de cada uso: cotidiano, sensible o de frontera.

2. **Alfabetización antes que prohibición.** Frente a una tecnología desconocida, la primera respuesta institucional debería ser desarrollar la capacidad de comprenderla, usarla y evaluarla críticamente. Prohibir lo que no se entiende no elimina el riesgo: lo empuja a la informalidad y ensancha la brecha entre quienes saben usar la IA y quienes no. Alfabetizar a docentes, gestores y estudiantes es la condición previa de cualquier política sensata.

3. **Gobernanza antes que adopción indiscriminada.** Incorporar IA exige reglas sobre usos permitidos, responsabilidades, privacidad, transparencia y supervisión. Adoptar herramientas sin esas reglas deja a cada persona improvisando su propio criterio, con riesgos para la integridad académica y la protección de datos. La gobernanza —un documento base que fije qué se puede hacer, con qué información y bajo qué controles— debe preceder al despliegue, no seguirlo.

4. **Responsabilidad humana.** Usar IA no transfiere al sistema la responsabilidad de una decisión: la máquina puede sugerir, redactar o priorizar, pero la decisión y sus consecuencias siguen siendo de quien la toma. Por eso las decisiones que afectan a personas exigen supervisión humana significativa, no una firma automática sobre lo que produjo el sistema. La responsabilidad final es siempre humana e institucional.

5. **Soberanía de datos e infraestructura.** La adopción de IA debe considerar dónde se almacenan y procesan los datos, quién accede a ellos, quién se beneficia y bajo qué condiciones pueden reutilizarse. No es un eslogan ni exige construir modelos propios: es clasificar la información por sensibilidad y asignar a cada nivel la opción adecuada, desde cláusulas contractuales hasta el procesamiento local. En contextos comunitarios e indígenas, incluye decidir quién tiene autoridad sobre el dato y quién se beneficia de él.

6. **Contextualización tecnológica.** La IA no se adopta porque esté de moda; su uso debe responder a problemas reales, necesidades locales y contextos específicos. Copiar herramientas, indicadores o umbrales de otros entornos rara vez funciona: lo que se transfiere son principios, no recetas. La tecnología pertinente parte del problema de la institución, de sus recursos y de su realidad, no del catálogo del proveedor.

7. **Capacidad tecnológica propia.** Las instituciones y los países no deberían limitarse a consumir tecnologías externas: deben desarrollar la capacidad de adaptar, investigar, construir y gobernar sus propias soluciones. Depender por completo de plataformas ajenas limita la autonomía y deja decisiones importantes en manos de terceros. Formar talento y construir capacidad local, aunque sea de forma gradual, es lo que convierte a un país en actor y no solo en usuario.

Referencias

Anthropic. (2023). *Responsible scaling policy*. https://www.anthropic.com/responsible-scaling-policy

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE principles for Indigenous data governance. *Data Science Journal*, *19*(1), Artículo 43. https://doi.org/10.5334/dsj-2020-043

Center for AI Safety. (2023, 30 de mayo). *Statement on AI extinction risk*. https://safe.ai/work/statement-on-ai-extinction-risk

Chamba-Eras, L., Cumbicus Pineda, O. M., Coronel Romero, E. L., Gaona Alvarado, J. K., & Barba Guamán, L. R. (2026). *Marco IA593: Modelo de gobernanza, ética y estrategia para la integración de la inteligencia artificial en la educación superior del Ecuador*. arXiv: 2602.09246. https://arxiv.org/abs/2602.09246

Huamani, K. (2026, 9 de septiembre). *Anthropic researcher's resignation sends warning about the dangers of AI development*. PBS NewsHour.

https://www.pbs.org/newshour/science/anthropic-researchers-resignation-sends-warning-about-the-dangers-of-ai-development

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2026). *Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en el Ecuador (EFIA-EC)* (Acuerdo Ministerial N.º MINTEL-MINTEL-2025-0030; Registro Oficial, Primer Suplemento n.º 206). https://asobanca.org.ec/wp-content/uploads/2026/01/ACUERDO-Nro.-MINTEL-MINTEL-2025-0030-Estrategia-IA.pdf

OpenAI. (2025). *Preparedness framework*. https://openai.com/index/updating-our-preparedness-framework/

xAI. (2025). *Risk management framework*. https://x.ai/safety

Marcos y documentos de referencia

Documentos consultados que enmarcan la posición del texto, aunque no se citan expresamente.

Centro Nacional de Inteligencia Artificial & Comisión Económica para América Latina y el Caribe. (2025). *Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025*. CENIA; CEPAL. https://indicelatam.cl/

FLACSO Ecuador. (2025). *Abriendo la caja negra de la inteligencia artificial en Ecuador* (Boletín N.º 4). FLACSO Ecuador. https://www.flacso.edu.ec/sites/default/files/2025-08/BoletinNo.4.finalweb.pdf

OCDE. (2019). *Recomendación del Consejo sobre inteligencia artificial* (Instrumento jurídico N.º OECD/LEGAL/0449; revisada en 2024). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Stanford Institute for Human-Centered Artificial Intelligence. (2026). *Artificial Intelligence Index report 2026*. Stanford University. https://hai.stanford.edu/ai-index/2026-ai-index-report

UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial*. UNESCO. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Cómo citar. Vásconez-Paredes, C. (2026). *Antes de temerle a la inteligencia artificial, comprenderla: Manifiesto y principios Yachay Deep para una adopción responsable, crítica y soberana de la inteligencia artificial en Ecuador* (Position Paper N.º 1, versión 1.1). Yachay Deep Research Institute. https://doi.org/10.5281/zenodo.23489388

Versión 1.1. Añade los enlaces de las fuentes y ajusta las referencias a APA 7. El argumento no cambia respecto de la v1.0. Publicación original: https://www.yachaydeep.com/research/blog/riesgosIA.

Licencia. Este documento se distribuye bajo Creative Commons Atribución 4.0 Internacional (CC BY 4.0): puede compartirse y adaptarse citando la fuente.

Autor. Carlos Vásconez-Paredes, ORCID 0000-0002-1574-346X.