DOCUMENTO DE ANÁLISIS

Uso responsable de la inteligencia artificial

Qué significa, qué exige y cómo implementarlo en una organización

Buenas prácticas, componentes de un manual institucional y criterios operativos basados en los marcos del NIST, la UNESCO y la Unión Europea

Nick Perot

Abogado | Consultor en transformación digital | Docente

www.nickperot.com

Marzo 2026

1. El punto de partida: la ética no alcanza sin operación

El documento anterior de esta serie analizó los marcos éticos internacionales aplicables a la inteligencia artificial. Los principios están. El consenso existe. Pero un principio sin traducción operativa es una declaración de intenciones, no una política.

Este documento aborda lo que sigue: el uso responsable de la IA. Es decir, las prácticas concretas, los protocolos, las decisiones de gestión y los hábitos organizacionales que convierten los principios éticos en acciones verificables. No se trata de repetir los valores. Se trata de mostrar cómo se implementan.

2. Qué significa usar la IA de manera responsable

El NIST -Instituto Nacional de Estándares y Tecnología de Estados Unidos- enmarca el uso responsable de la IA como un conjunto de prácticas que promueven que los sistemas de inteligencia artificial se orienten a la confiabilidad a lo largo de todo su ciclo de vida: diseño, desarrollo, despliegue, uso y monitoreo. El AI Risk Management Framework, publicado en enero de 2023, identifica siete atributos de un sistema de IA confiable: validez y confiabilidad, seguridad, protección, rendición de cuentas y transparencia, explicabilidad e interpretabilidad, privacidad, y equidad con gestión de sesgos.

NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, enero de 2023.

La UNESCO, por su parte, plantea el uso responsable desde una perspectiva de derechos: los sistemas de IA deben respetar, proteger y promover los derechos humanos y las libertades fundamentales en todas las etapas de su ciclo de vida. La Recomendación de 2021 establece que el uso de sistemas de IA no debe ir más allá de lo necesario para alcanzar un objetivo legítimo, y que la evaluación de riesgos debe emplearse para prevenir daños.

UNESCO, Recomendación sobre la ética de la inteligencia artificial, 2021, principio de proporcionalidad.

Las dos perspectivas son complementarias. El NIST ofrece un marco técnico-organizacional: cómo gestionar riesgos. La UNESCO ofrece un marco de valores: para qué gestionarlos. Juntas definen lo que significa usar la IA de manera responsable: operar sistemas que funcionan como se espera, que no causan daño evitable, que respetan derechos y que pueden explicarse ante quienes los usan y ante quienes reciben sus efectos.

> Una organización usa la IA de manera responsable cuando puede explicar qué hace su sistema, por qué lo hace, qué datos usa, qué puede fallar y qué se hizo para prevenirlo.

3. La IA como tecnología al servicio de las personas

El AI Act de la Unión Europea, la Recomendación de la UNESCO y el marco del NIST coinciden en un punto central: la IA debe estar al servicio de las personas, no al revés. Esta afirmación, que puede sonar obvia, tiene consecuencias operativas concretas.

Significa que la supervisión humana no es opcional. El AI Act exige mecanismos de supervisión humana para todos los sistemas de alto riesgo. La UNESCO establece el principio de que los seres humanos deben poder decidir si delegan decisiones a un sistema de IA y en qué condiciones. El NIST, en su función GOVERN, requiere que las organizaciones definan roles y responsabilidades claras para la gestión de riesgos de IA, incluyendo la determinación de en qué puntos del proceso una persona debe intervenir.

NIST AI RMF 1.0, función GOVERN; Reglamento (UE) 2024/1689, artículos sobre supervisión humana; UNESCO (2021), principio de supervisión y determinación humanas.

También significa que la automatización no justifica la desatención. Que un sistema funcione de manera autónoma no exime a la organización de monitorear sus resultados, verificar su desempeño y responder por sus consecuencias. La responsabilidad no se delega a la máquina.

4. Privacidad y protección de datos

La privacidad es uno de los principios que aparece en todos los marcos internacionales analizados en esta serie. No es casual. Los sistemas de IA requieren datos para funcionar, y muchos de esos datos son personales, sensibles o ambos.

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece principios que son directamente aplicables al uso de IA: licitud del tratamiento, limitación de finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva del responsable del tratamiento. El AI Act complementa estos principios con requisitos específicos de gobernanza de datos para sistemas de alto riesgo.

Reglamento (UE) 2016/679 (GDPR), artículo 5; Reglamento (UE) 2024/1689 (AI Act), requisitos de gobernanza de datos para sistemas de alto riesgo.

El NIST incluye la privacidad como uno de los siete atributos de un sistema de IA confiable y recomienda que las organizaciones establezcan marcos adecuados de protección de datos como parte integral de su gestión de riesgos de IA. El diagnóstico de la UNAM (2025) coincide: entre las áreas de riesgo que justifican la integración de la ética en los sistemas de IA están el control sobre los datos, la transparencia en términos de propiedad y la ciberseguridad.

Castañeda de León et al., Uso y desarrollo ético de la IA en la Universidad, DGTIC-UNAM, 2025, pp. 40–41.

Criterios mínimos de privacidad para el uso de IA en organizaciones

Consentimiento informado antes de procesar datos personales con herramientas de IA. Minimización: no ingresar a las herramientas de IA más datos personales de los estrictamente necesarios. Revisión de las políticas de privacidad y condiciones de uso de cada herramienta, especialmente las comerciales. Registro de qué herramientas se usan, con qué datos y para qué fines. Políticas claras sobre retención y eliminación de datos procesados por sistemas de IA.

5. Las cuatro funciones del NIST como estructura operativa

El AI Risk Management Framework del NIST organiza la gestión de riesgos de IA en cuatro funciones interconectadas: GOVERN, MAP, MEASURE y MANAGE. Estas funciones no son pasos secuenciales sino procesos iterativos que se aplican a lo largo de todo el ciclo de vida de un sistema de IA.

NIST AI RMF 1.0, parte 2: Core Framework.

Las cuatro funciones del NIST AI RMF

Función	Alcance
GOVERN	Cultivar una cultura organizacional consciente del riesgo. Definir roles, responsabilidades y políticas para el desarrollo y uso de IA. Aplica a todas las etapas.
MAP	Contextualizar los sistemas de IA en su entorno operativo. Identificar impactos potenciales en personas, organizaciones y ecosistemas. Evaluar propósito y alcance.
MEASURE	Evaluar riesgos con métodos cuantitativos y cualitativos. Medir desempeño, sesgos, precisión y confiabilidad. Monitorear de manera continua.
MANAGE	Responder a los riesgos identificados. Priorizar acciones de mitigación. Implementar controles técnicos y procedimentales. Documentar decisiones.

Fuente: NIST AI RMF 1.0, NIST AI 100-1, enero de 2023.

Lo que hace valioso a este marco para organizaciones que no son empresas tecnológicas es su adaptabilidad. El NIST lo diseñó como un instrumento voluntario, no sectorial y no vinculado a un caso de uso específico. Una universidad, un estudio jurídico o una organización de la sociedad civil pueden aplicar sus funciones con el mismo rigor que una empresa de software, ajustando la escala al tamaño y los recursos disponibles.

6. Qué debe contener un manual de uso responsable de IA

Un manual de uso responsable de IA no es un documento de principios generales. Es un instrumento operativo que traduce los marcos éticos y regulatorios en reglas claras, aplicables y verificables dentro de una organización específica. A partir de los marcos analizados en esta serie, un manual institucional debería contener al menos los siguientes componentes.

Alcance y definiciones

Qué se entiende por IA dentro de la organización. Qué herramientas están alcanzadas. Qué actividades se regulan. La definición de la OCDE (2024) ofrece un punto de partida sólido: sistema basado en máquinas que infiere a partir de datos y genera resultados que pueden influir en entornos físicos o virtuales.

Inventario de herramientas y sistemas de IA

Un registro actualizado de las herramientas de IA que se usan en la organización, con qué datos operan, quién las usa, para qué fines y con qué nivel de supervisión humana. El NIST recomienda este inventario como parte de la función GOVERN.

> *NIST AI RMF 1.0, GOVERN 1.6: mecanismos para inventariar sistemas de IA.*

Políticas de datos y privacidad

Reglas sobre qué datos pueden ingresarse a herramientas de IA, cómo se protegen, quién autoriza su uso y cómo se garantiza el cumplimiento de la normativa de protección de datos aplicable. Incluye consentimiento informado, minimización de datos y revisión de condiciones de uso de herramientas comerciales.

Transparencia y documentación del uso

Criterios para declarar cuándo se usó IA en un producto de trabajo. Cómo se documenta el uso: qué herramienta, qué prompt, qué resultado, qué intervención humana se aplicó sobre el resultado. El diagnóstico de la UNAM recomienda que tanto docentes como estudiantes incluyan evidencia de prompts y capturas de pantalla del contenido sintético.

> *Castañeda de León et al. (2025), pp. 45–46 (recomendaciones al docente) y pp. 46–47 (recomendaciones al alumno).*

Supervisión humana y responsabilidad

Definición de en qué puntos del proceso una persona debe revisar, validar o corregir los resultados de un sistema de IA. Quién es responsable del producto final. La regla básica, consistente con los tres marcos internacionales, es directa: la responsabilidad del resultado es siempre de la persona, no de la herramienta.

Evaluación de riesgos y sesgos

Procedimientos para identificar sesgos en las herramientas de IA utilizadas y para monitorear sus resultados. La función MEASURE del NIST propone evaluar sesgos, precisión y confiabilidad de manera continua. El AI Act exige un sistema formal y documentado de gestión de riesgos para sistemas de alto riesgo.

Capacitación y alfabetización

Programas de formación que incluyan tanto aspectos técnicos como éticos del uso de IA. El AI Act incluye obligaciones de alfabetización en IA exigibles desde febrero de 2025. La UNAM recomienda que la capacitación aborde el uso crítico, reflexivo y creativo de las herramientas.

> *Reglamento (UE) 2024/1689, obligaciones de alfabetización; Castañeda de León et al. (2025), p. 46, recomendación 5.*

Revisión periódica y actualización

Un manual que no se revisa queda obsoleto antes de publicarse. El NIST recomienda monitoreo continuo y revisión periódica del proceso de gestión de riesgos. La tecnología cambia. Las herramientas cambian. Las condiciones de uso cambian. El manual debe acompañar esos cambios.

> *NIST AI RMF 1.0, GOVERN 1.5: monitoreo continuo y revisión periódica.*

7. Buenas prácticas para organizaciones

A partir de los marcos analizados, las siguientes prácticas ofrecen un punto de partida operativo para organizaciones que quieran implementar un uso responsable de la IA sin esperar regulación local.

Antes de implementar

Realizar un diagnóstico de competencias digitales del equipo. Evaluar qué tareas se beneficiarían del uso de IA y cuáles no. Revisar las condiciones de uso y políticas de privacidad de las herramientas disponibles. Definir quién decide qué herramientas se adoptan y bajo qué criterios.

Durante el uso

Documentar el uso de IA en los productos de trabajo. Verificar los resultados antes de utilizarlos. No ingresar datos personales, sensibles o confidenciales sin autorización explícita. Declarar el uso

de IA cuando el contexto lo requiera: investigación, docencia, comunicaciones institucionales, documentos legales.

Después de implementar

Medir resultados. Evaluar si la herramienta cumple el propósito para el que se adoptó. Registrar incidentes. Actualizar políticas. Capacitar de manera continua. La gestión de riesgos de IA no es un proyecto con fecha de cierre. Es un proceso permanente.

> El uso responsable no se declara. Se demuestra con decisiones documentadas, datos protegidos, resultados verificados y personas que entienden lo que la herramienta hace y lo que no puede hacer.

8. Consideraciones finales

El uso responsable de la IA es el puente entre los principios éticos y la práctica cotidiana. Sin ese puente, los marcos internacionales quedan en el territorio de las declaraciones. Con él, se convierten en políticas operativas que protegen personas, datos y resultados.

Los instrumentos para construir ese puente ya existen. El NIST ofrece una estructura de cuatro funciones adaptable a cualquier organización. La UNESCO ofrece los valores y principios que orientan las decisiones. El AI Act ofrece categorías de riesgo que permiten priorizar esfuerzos. El diagnóstico de la UNAM ofrece recomendaciones específicas para contextos educativos.

Lo que falta, en la mayoría de las organizaciones, no son los marcos. Es la decisión de sentarse a escribir un manual propio, adaptado a su realidad, y la disciplina de revisarlo periódicamente. Esa decisión no requiere legislación. Requiere criterio.

> Un manual de uso responsable de IA no es el final del proceso. Es el comienzo de una conversación institucional que, si se hace bien, no termina.

Referencias

Castañeda de León, L.M., Ramírez Molina, A.Y., Castillejos Reyes, J.M. y Ventura Miranda, M.T. (2025). *Uso y desarrollo ético de la Inteligencia Artificial en la Universidad: docencia e investigación.* México: DGTIC-UNAM. ISBN 978-607-587-954-3.

NIST (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* NIST AI 100-1. Gaithersburg: National Institute of Standards and Technology.

NIST (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.* NIST AI 600-1. Gaithersburg: NIST.

OCDE (2024). *Explanatory memorandum on the updated OECD definition of an AI System.* OECD Artificial Intelligence Papers, N.º 8.

UNESCO (2021). *Recomendación sobre la ética de la inteligencia artificial.* París: UNESCO. unesdoc.unesco.org/ark:/48223/pf0000381137_spa.

Unión Europea (2016). *Reglamento (UE) 2016/679 — Reglamento General de Protección de Datos (GDPR).* Diario Oficial de la UE.

Unión Europea (2024). *Reglamento (UE) 2024/1689 — Ley de Inteligencia Artificial (AI Act).* Diario Oficial de la UE, 13 de junio de 2024.