CORRESPONDE EXPTE. 5855/2025

Resolución (CS) 2756/2025.-

Junín, 28 de noviembre de 2025.-

Visto,

Las presentes actuaciones relacionadas con la propuesta del Manual de Buenas prácticas para el uso de Inteligencia Artificial (IA) en UNNOBA; y,

Considerando:

Que la Directora del Sistema Institucional de Educación a Distancia y Digital (SIEDD) eleva a la Secretaría Académica propuesta del Manual de Buenas prácticas para el uso de Inteligencia Artificial (IA) en UNNOBA.

Que pone de manifiesto que el documento fue elaborado por el equipo de Educación Digital y consensuado con la ProTIC y su contenido representa una guía de orientaciones prácticas para integrar la inteligencia artificial como una herramienta de aumento cognitivo en las distintas actividades.

Que asimismo, se busca, potenciar el valor pedagógico, operativo y administrativo mientras se reducen los riesgos, abarcando las trayectorias académicas en modalidades presenciales, híbridas y a distancia. Todo ello se sostiene en la verificación humana de los resultados, el cuidado responsable de los datos y el compromiso con la equidad de acceso.

Que a fs. 2/32 obra detalle de la propuesta.

Que a fs. 33 toma intervención la Secretaría Académica.

Que a fs. 35 se expide la Comisión de Asuntos Académicos.

Que este Cuerpo trató y aprobó lo actuado en su Sesión Ordinaria del día 27 de noviembre de 2025, Acta Nro. 9/2025.

Por ello,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD NACIONAL DEL NOROESTE DE LA PROVINCIA DE BUENOS AIRES

RESUELVE:

Artículo 1: Aprobar el Manual de Buenas prácticas para el uso de Inteligencia Artificial (IA) en UNNOBA que, como Anexo I forma parte integrante de la presente.

Artículo 2: Regístrese, notifíquese, publíquese. Cumplido, archívese.-

ANEXO I

RESOLUCIÓN (CS) 2756/2025

BUENAS PRÁCTICAS PARA EL USO DE LA INTELIGENCIA ARTIFICIAL (IA) EN LA UNNOBA

educación digital

ÍNDICE

Resumen: Buenas prácticas para el uso de IA en UNNOBA 3

Buenas prácticas para el uso de IA en UNNOBA 7

1. Propósito y alcance institucional 7

2. Principios y compromisos de UNNOBA (enfoque humano) 7

3. Marco de referencia 8

3.1 Recomendaciones para usar el marco normativo: 10

4. Definiciones clave y alcances terminológicos 10

5. Gobernanza interna y roles 12

5.1. Objetivo de la gobernanza 12

5.2. Roles y responsabilidades (síntesis operativa) 12

5.3. Comité asesor y ciclo de revisión 13

5.4. Procedimiento de “pruebas pilotos” 13

5.5. Trazabilidad y rendición de cuentas 14

5.7. Capacitación y sensibilización 14

6. Selección y evaluación de herramientas 14

6.1. Criterios mínimos de adopción: ¿qué mirar antes de decidir? 15

6.2. Matriz de decisión (plantilla operativa) 16

6.3. Evaluación proporcional al riesgo: ¿cómo decidir la profundidad del análisis? 18

6.4. Prueba piloto y decisión 18

6.5. Registro y rendición de cuentas 18

6.6. Señales de alerta: ¿cuándo NO avanzar? 18

7. Privacidad, datos y seguridad 19

7.1. Principios prácticos: ¿qué debe guiar cada decisión? 19

7.2. Clasificación de datos y reglas de tratamiento 20

7.3. Controles mínimos obligatorios 20

7.4. Lo que NO debe hacerse 21

7.5. Evaluación proporcional al riesgo (cómo ajustar el nivel de control) 21

7.6. Roles y responsabilidades 21

7.7. Incidentes, registro y mejora continua 21
8. Integridad académica y evaluación 22
8.1. Principios aplicados a la evaluación 22
8.2. Limitaciones de detectores y enfoque de verificación 22
8.3. Diseño de consignas 23
8.4. Procedimiento ante dudas de autoría 23
9. Gestión de riesgos y control de calidad 23
9.1. Riesgos frecuentes 23
9.2. Controles y mitigaciones 24
9.3. Ciclo de control de calidad 24
9.4. Señales de alerta 24
10. Inclusión y accesibilidad 25
10.1. Principios aplicados 25
10.2. Requisitos mínimos en cursos y materiales 25
10.3. IA al servicio de la inclusión 25
11. Alfabetización en IA para la comunidad UNNOBA 26
12. Seguimiento y mejora continua 26
13. Usos pedagógicos recomendados 26
13.1. Familias de uso 26
14. Capacidades positivas de la IA en docencia 27
15. Usos no recomendados o prohibidos 28
Referencias bibliográficas 29

Resumen: Buenas prácticas para el uso de IA en UNNOBA

Este documento presenta una síntesis de las buenas prácticas para el uso de la inteligencia artificial en la Universidad Nacional del Noroeste de la Provincia de Buenos Aires. Su propósito es orientar a docentes, estudiantes, no docentes y equipos de gestión para integrar la IA como herramienta de aumento cognitivo, con foco en el valor pedagógico y operativo, la protección de datos y la equidad de acceso. Reúne principios, definiciones operativas y criterios de selección y evaluación de herramientas, además de pautas para la integridad académica, la inclusión y la mejora continua. Propone un modo de trabajo con evidencia, trazabilidad y revisión humana, e indica qué prácticas no se recomiendan o están prohibidas. Es un material de consulta rápida, pensado para ser adoptado por equipos docentes y áreas de la gestión y administración universitarias, y para actualizarse de forma periódica a medida que la institución aprende de su propia experiencia. A continuación se presenta el resumen organizado por temas.

1. **Propósito y alcance**
   Orientar a toda la comunidad UNNOBA (docentes, estudiantes, no docentes y gestión) en el uso responsable de la inteligencia artificial como herramienta de aumento cognitivo, maximizando el valor pedagógico y operativo y minimizando riesgos. Aplica a todas las propuestas educativas, actividades administrativas y/o de gestión, entre otras; en todas las modalidades (presencial, híbrida y distancia) No se autoriza la calificación automática sin revisión humana, el uso de detectores como única evidencia y la generación de referencias falsas.

2. **Enfoque y principios**
   Las personas están primero, la inteligencia artificial no reemplaza el juicio profesional ni el aprendizaje humano. Transparencia y trazabilidad, declarar usos y conservar evidencias de proceso cuando corresponda. Responsabilidad humana en decisiones y evaluación. Privacidad y seguridad, minimización de datos, controles técnicos y acuerdos con terceros cuando aplique. Equidad y accesibilidad, alternativas de baja conectividad y criterios alineados a las Pautas de Accesibilidad para el Contenido Web (WCAG). Calidad y mejora continua, pruebas piloto acotadas con métricas antes de escalar.

3. **Marco de referencia**
   Ley 25.326 y Decreto 1558 de 2001 de la Agencia de Acceso a la Información Pública en protección de datos personales. Ley 26.653 y lineamientos del Observatorio de Accesibilidad Web para la accesibilidad digital en el sector

público. Lineamientos institucionales SIEDD, Educación Digital para la práctica local en programas, aulas, resguardo y soporte. Referencias recomendadas, UNESCO 2021 ética, NIST AI RMF 1.0 gestión de riesgos, ISO o IEC 42001 sistema de gestión para inteligencia artificial, GDPR como buena práctica en supuestos puntuales.

4. **Definiciones operativas**
   Inteligencia artificial generativa e inteligencia artificial asistiva. Modelo de lenguaje útil pero puede inventar o descontextualizar, requiere verificación. Datos personales y datos sensibles con minimización, anonimización y seudonimización. Trazabilidad de prompts, versiones y fuentes, y supervisión humana significativa. Prueba piloto, prueba acotada y documentada previa al escalado.

5. **Gobernanza y roles**
   Conducción académica y gestión definen lineamientos y aprueban políticas. Educación Digital y ProTIC brindan soporte técnico y pedagógico, acompañan pruebas piloto y asesoran en selección, evaluación y configuración segura. Asignaturas y áreas establecen políticas de curso, diseñan consignas con evidencia de proceso, resguardan datos y aseguran trazabilidad. Unidades administrativas definen objetivos, métricas y controles en procesos internos. Estudiantes declaran el uso de inteligencia artificial cuando corresponda, cuidan datos y registran el proceso. SIEDD realiza el seguimiento, coordina análisis de impacto cuando sea posible con baja carga administrativa y respeto por la privacidad.

6. **Selección y evaluación de herramientas**
   Propósito con valor educativo u operativo. Datos por tipo, sensibilidad, ubicación, accesos y minimización. Privacidad y seguridad con términos, cifrado y accesos, y acuerdo de tratamiento de datos si hay terceros. Accesibilidad alineada a WCAG, alternativas y conectividad. Calidad y explicabilidad según criticidad. Riesgos y mitigaciones con verificación de citas, coherencia y corroboración y revisión humana. Costos y sostenibilidad con licencias, soporte y escala. Plan de salida con portabilidad y sin bloqueo de proveedor. Evaluación proporcional al riesgo con semáforo, verde sin datos personales y uso individual con revisión breve, amarillo apoyo a clase y retroalimentación con matriz completa, piloto y alternativa sin inteligencia artificial, rojo datos personales o decisiones sobre personas con revisión legal, acuerdo de tratamiento de datos, piloto acotado y autorización específica.

7. **Privacidad, datos y seguridad**
   Antes de usar, verificar si el objetivo se logra sin datos personales o sensibles y, si no es posible, minimizar y aplicar controles. Si hay terceros, exigir términos compatibles, cifrado y accesos por rol y acuerdo de tratamiento de datos.

Informar y ofrecer alternativa cuando corresponda, y definir retención y borrado. Prohibido subir datos sensibles o información confidencial a servicios sin garantías contractuales y técnicas.

8. **Integridad académica y evaluación**
   Producto y proceso con evidencias de trabajo como prompts, versiones, fuentes y reflexión. Supervisión humana en calificaciones. Transparencia con declaración del uso de inteligencia artificial. Los detectores no son prueba concluyente, usar verificación de citas, coherencia y corroboración y defensas breves. Consignas resilientes a la inteligencia artificial que solicitan criterio, aplicación y transferencia.

9. **Gestión de riesgos y calidad**
   Identificar, evaluar, mitigar y monitorear con trazabilidad. Control de calidad, (planificar, ejecutar, verificar y actuar) con objetivos y métricas, piloto, revisión de resultados en calidad, equidad, accesibilidad e incidentes, y decisiones de ajuste, escalado o descarte.

10. **Inclusión y accesibilidad**
    Texto alternativo en imágenes, subtítulos y transcripciones en videos, contraste y tamaño de fuente adecuados, navegación por teclado, enlaces descriptivos y compatibilidad con lectores de pantalla. Ofrecer alternativas de baja conectividad.

11. **Alfabetización y soporte**
    Plan de formación continua por rol y canal único de consultas técnico y pedagógicas de Educación Digital. Microcredenciales y materiales de autoformación.

12. **Seguimiento y mejora continua**

13. **Usos pedagógicos recomendados**
    Planificación y guiones, ejemplos y contraejemplos, tutoría socrática, retroalimentación guiada por rúbrica, andamiaje paso a paso, bancos de ítems con revisión, metacognición, accesibilidad con transcripción, simplificación y traducción preliminar, analítica formativa sin datos sensibles y programación asistida, siempre con verificación y revisión humana.

14. **Capacidad positiva de la IA en docencia**

15. **Usos no recomendados o prohibidos**
    Delegar la autoría total en inteligencia artificial, calificar sin revisión humana, usar detectores como única evidencia, generar referencias inventadas, subir datos personales o sensibles e información confidencial a servicios sin garantías, o adoptar herramientas sin plan de salida ni portabilidad.

Buenas prácticas para el uso de IA en UNNOBA

1. Propósito y alcance institucional

Este documento ofrece a toda la comunidad de la UNNOBA (docentes, estudiantes, no docentes y equipos de gestión) orientaciones prácticas para integrar la inteligencia artificial como una herramienta de aumento cognitivo en las distintas actividades. Se busca, así, potenciar el valor pedagógico, operativo y administrativo mientras se reducen los riesgos, abarcando las trayectorias académicas en modalidades presenciales, híbridas y a distancia. Todo ello se sostiene en la verificación humana de los resultados, el cuidado responsable de los datos y el compromiso con la equidad de acceso. No se autoriza la calificación automática sin revisión humana, el uso de detectores como única evidencia y la generación de referencias falsas.

2. Principios y compromisos de la UNNOBA (enfoque humano)

En la UNNOBA se adopta un enfoque humanista para el uso de la Inteligencia Artificial: las personas están primero y la IA funciona como apoyo para pensar mejor, no como sustituto del juicio profesional ni del aprendizaje humano. Por eso sostenemos la transparencia y la trazabilidad (explicitar cuándo, para qué y cómo se usó la IA, dejando huellas del proceso), junto con la responsabilidad humana en las decisiones y evaluaciones; la privacidad y la seguridad mediante minimización de datos, resguardos técnicos y acuerdos adecuados; la equidad y la inclusión, garantizando alternativas accesibles y evitando brechas por conectividad, discapacidad o idioma; y la calidad pedagógica y operativa, de modo que la IA mejore la comprensión, la toma de decisiones y la eficiencia sin desvirtuar el sentido formativo. Finalmente, impulsamos la mejora continua mediante "*Pruebas pilotos*", que son explicadas con mayor detalle en el punto 4, que son pruebas acotadas y controladas, con objetivos y métricas claras, protección de datos y duración limitada; seguidos con una revisión basada en evidencia y de ajustes periódicos. Este marco se alinea con estándares y recomendaciones internacionales que ponen el foco en los derechos humanos, la dignidad y la supervisión humana significativa, por ejemplo, la *Recomendación sobre la Ética de la IA* de la UNESCO (2021) y con la normativa vigente aplicable a universidades públicas argentinas.

3. Marco de referencia

En este apartado se definen brevemente las normativas vigentes nacionales, internacionales e internas que dan fundamento a este documento, entre ellas lo que aplica a esta universidad:

- **Ley 25.326 y Decreto 1558/2001** (Protección de datos personales, autoridad AAIP).
  Qué es: el marco nacional que regula el tratamiento de datos personales en organismos públicos y privados.
  Por qué es importante: establece principios (finalidad, proporcionalidad, seguridad), derechos de las personas y deberes institucionales; exige resguardar datos y, cuando corresponda, contar con acuerdos adecuados de tratamiento con terceros.

- **Ley 26.653** (Accesibilidad de la información en páginas web del sector público) y lineamientos del Observatorio de Accesibilidad Web (ONTI).
  Qué es: la norma que obliga a los sitios y servicios digitales del Estado (incluidas universidades nacionales) a ser accesibles.
  Por qué es importante: orienta a cumplir criterios alineados a las Pautas de Accesibilidad para el Contenido Web (WCAG), por ejemplo, alternativas textuales, contraste, navegación por teclado; garantizando inclusión y no discriminación en contenidos y herramientas con IA.

- **Lineamientos y resoluciones institucionales** (SIEDD, Educación Digital y Politica de Seguridad de la informacion).
  Qué es: políticas, instructivos y procedimientos internos vigentes.
  Por qué es importante: brindan sugerencias a programas de asignaturas, aulas virtuales, resguardo de datos, soporte y canales de consulta, asegurando coherencia entre la normativa y la operación cotidiana.

Lo que referencia y da respaldo (no obligatorio, pero recomendado para buenas prácticas)

- **Recomendación sobre la Ética de la IA** (UNESCO, 2021).
  Qué es: un marco internacional de ética en IA centrado en derechos humanos, dignidad, bienestar y supervisión humana significativa.
  Por qué es importante: aporta principios transversales (justicia, transparencia, responsabilidad, diversidad, inclusión) que refuerzan nuestro enfoque humano y orientan decisiones prudentes en docencia y gestión.

- **NIST AI Risk Management Framework 1.0** (EE. UU.).
  Qué es: un marco voluntario para gestionar riesgos de IA a lo largo del ciclo

de vida (validez, seguridad, privacidad, equidad, explicabilidad). **Por qué es importante**: ofrece lenguaje común y prácticas operativas (identificar-evaluar-mitigar-monitorear) útiles para “pruebas pilotos”, adopción gradual y mejora continua.

- **ISO/IEC 42001:2023** (Sistema de gestión para IA). **Qué es**: un estándar internacional que establece procesos, roles y controles para gobernar la IA en organizaciones públicas y privadas. **Por qué es importante**: sirve como “horizonte de madurez” para ordenar responsabilidades, documentar decisiones, auditar prácticas y sostener ciclos de mejora.

- **Reglamento General de Protección de Datos de la Unión Europea** (RGPD/GDPR)
  Qué es: el marco europeo de datos personales (principios y “privacidad desde el diseño y por defecto”). **Por qué es importante:** no aplica de manera general a UNNOBA; solo podría alcanzar en supuestos puntuales de extraterritorialidad. Lo usamos como buena práctica para reforzar criterios de minimización, transparencia y resguardo.



Gráfico realizado por Educación Digital by Napkin

3.1 Recomendaciones para usar el marco normativo:

1. Para cualquier iniciativa con IA, verificar primero protección de datos y accesibilidad (Leyes 25.326 y 26.653).

2. Alinear la implementación con lineamientos internos (SIEDD y normativa vigente de Educación Digital UNNOBA).

3. Tomar como guía ética y operativa las referencias de UNESCO, NIST AI RMF e ISO/IEC 42001, especialmente en “pruebas pilotos”, trazabilidad y mejora continua.

4. Definiciones clave y alcances terminológicos

Con el objeto de asegurar una comprensión común, se presentan a continuación definiciones operativas, concisas y aplicables, que se utilizarán de manera consistente en todo el documento. Estas definiciones se alinean con marcos ampliamente reconocidos, entre ellos la *Recomendación sobre la Ética de la IA* de la UNESCO (2021) y el *AI Risk Management Framework 1.0* del NIST (2023).

- **Inteligencia artificial generativa (IA generativa)**. Es el conjunto de modelos capaces de producir contenido nuevo (texto, código, imágenes, audio o video) a partir de indicaciones. Su utilidad radica en acelerar borradores e ideas, pero sus salidas requieren verificación humana y adaptación al contexto.

- **Inteligencia artificial asistiva (IA asistiva).** Son herramientas que asisten tareas existentes (resumir, traducir, corregir, estructurar información, guiar pasos en un proceso). No “crean desde cero” necesariamente, sino que acompañan al usuario para trabajar mejor y más rápido.

- **Pruebas pilotos.**
  Son pruebas acotadas y controladas para introducir una herramienta o práctica de IA antes de escalarlas. Se realizan con alcance limitado (por ejemplo, una asignatura o curso, un proceso administrativo, entre otros), objetivos y métricas claras, resguardo de datos (sin información sensible; consentimiento si corresponde), capacitación mínima del equipo, documentación del proceso (prompts, versiones, incidencias) y duración definida. Con la evidencia resultante se decide escalar, ajustar o descartar la adopción de la herramienta. Este enfoque es coherente con la supervisión humana y la gestión de riesgos promovidas por UNESCO (2021) y el NIST AI RMF (2023).

- **Modelo de lenguaje (LLM).**
  Es un tipo de modelo que predice y genera texto según patrones aprendidos. Puede ofrecer explicaciones útiles, pero también producir respuestas inventadas o descontextualizadas; por eso pedimos fuentes, coherencia y corroboración antes de usar sus salidas en ámbitos académicos o administrativos.

- **Datos personales y datos sensibles.**
  Son aquellos que identifican o pueden identificar a una persona (nombre, DNI, correo institucional, voz, imagen, registros académicos). Los sensibles incluyen, entre otros, salud, origen étnico, convicciones u orientación sexual. En UNNOBA rige el principio de minimización (Ley 25.326): tratamos solo lo estrictamente necesario, con resguardos adecuados y, cuando corresponda, consentimiento informado.

- **Minimización, anonimización y seudonimización.**

  - **Minimización**: reducir los datos personales al mínimo indispensable para cumplir un objetivo.

  - **Anonimización**: transformar los datos para que no sea posible identificar personas (de forma razonable).

  - **seudonimización:** reemplazar identificadores por claves o códigos, manteniendo por separado la "llave" de reidentificación bajo controles estrictos.

- **Trazabilidad (del proceso con IA).**
  Es la huella que deja el trabajo con IA: prompts (indicaciones), versiones (iteraciones y cambios) y fuentes consultadas. La trazabilidad permite explicar decisiones, revisar calidad y auditar el uso de la herramienta.

- **Supervisión humana significativa (*human in the loop*).**
  Es el principio por el cual las decisiones sustantivas (sobre personas, evaluaciones, comunicaciones oficiales o datos) se revisan y validan por humanos. La IA asiste, pero no decide sola. Este enfoque es consistente con los lineamientos de UNESCO (2021) y con la gestión de riesgos propuesta por NIST (2023).

- **Confidencialidad institucional.**
  Es la obligación de no exponer información interna (por ejemplo, actas, datos académicos no públicos, documentos de gestión) en servicios sin garantías contractuales y técnicas. Toda prueba o piloto debe excluir datos confidenciales o tratarlos con acuerdos y controles apropiados.

- **Limitaciones de los "detectores de IA".** Los llamados detectores de texto/imagen "hechos con IA" estimulan probabilidades, pero no son prueba concluyente. Pueden fallar con textos breves, traducciones y materiales editados. Por lo tanto, no deben usarse como única base de sanción. En su lugar, privilegiamos evidencias de proceso (trazabilidad) y evaluación auténtica (defensas orales breves, revisiones por pares, actividades de aplicación), junto con la verificación 3C: Citas, Coherencia y Corroboración.

- **DPA: Acuerdo de Tratamiento de Datos,** por su sigla en inglés**.**

  Es el contrato que se firma con un proveedor externo que va a procesar datos personales de la universidad. Deja por escrito el "qué, cómo y para qué" de ese tratamiento, y exige medidas de seguridad y confidencialidad.

Referencias de marco: UNESCO (2021) y NIST AI RMF (2023) recomiendan mantener supervisión humana, documentar procesos, evaluar riesgos y adoptar principios de privacidad desde el diseño, coherentes con la normativa argentina de protección de datos.

5. Gobernanza interna y roles

Con el fin de garantizar un uso responsable, coherente y sostenible de la IA en la UNNOBA, se establece un modelo de gobernanza que clarifica funciones, decisiones y controles a lo largo de todo el ciclo de vida de la herramienta o práctica (desde la idea hasta la mejora continua). Este enfoque se alinea con recomendaciones internacionales que priorizan la supervisión humana significativa, la gestión de riesgos y la documentación del proceso (UNESCO, *Recomendación sobre la Ética de la IA*, 2021; NIST, *AI Risk Management Framework 1.0*, 2023).

5.1. Objetivo de la gobernanza

Asegurar que cada iniciativa con IA tenga: (a) propósito legítimo y educativo/operativo claro; (b) responsables identificados; (c) resguardos de datos acordes a la normativa; (d) mecanismos de trazabilidad y rendición de cuentas; y (e) ciclo de evaluación y mejora.

5.2. Roles y responsabilidades (síntesis operativa)

- Conducción académica y de gestión (Rectorado/Secretarías/Escuelas): define lineamientos institucionales, aprueba políticas y prioriza recursos; recibe reportes de avance e incidentes relevantes; convoca la revisión semestral del presente documento.

- Educación Digital (ED) y Prosecretaría de TIC (PRO TIC): brindan soporte, acompañan “pruebas pilotos”, asesoran en selección y evaluación de herramientas (ver punto 6), revisan configuraciones de seguridad, promueven trazabilidad y elaboran informes de uso y mejora.

- Asignaturas/Áreas (docentes y equipos): diseñan políticas de curso (cláusulas de IA en programas), formulan consignas con producto + proceso, resguardan datos, validan resultados (supervisión humana) y documentan el proceso (prompts, versiones, fuentes), capacitan a estudiantes en el uso de herramientas de IA.

- Unidades administrativas y no docentes: adoptan IA en procesos internos con objetivos, métricas y resguardos; registran procedimientos y decisiones; escalan dudas por el canal institucional.

- Estudiantes: declaran el uso de IA cuando corresponda, protegen datos propios y de terceros, mantienen trazabilidad de su trabajo y aceptan instancias de verificación (defensas breves, evidencias de proceso).

5.3. Comité asesor y ciclo de revisión

El SIEDD será el área responsable de coordinar el seguimiento del uso de herramientas de IA en la universidad cuando ello sea posible y existan datos disponibles. El objetivo es analizar, de manera sencilla y no intrusiva, el impacto pedagógico y operativo de estas herramientas (por ejemplo, mejoras percibidas, accesibilidad, incidentes y oportunidades de ajuste) y alimentar la mejora continua de esta guía y de las prácticas institucionales. Cuando corresponda, el SIEDD podrá solicitar insumos mínimos (informes, métricas básicas o lecciones aprendidas) a asignaturas o áreas, procurando siempre la baja carga administrativa y el respeto por la privacidad.

5.4. Procedimiento de “pruebas pilotos”

Antes de escalar una herramienta o práctica, realizar una prueba acotada y controlada: definir alcance (una asignatura o curso), objetivos y métricas, resguardos de datos (sin información sensible; consentimiento si aplica), capacitaciones mínimas, trazabilidad (prompts, versiones, incidencias) y duración limitada. Con el informe de resultados, decidir escalar, ajustar o descartar. Este procedimiento materializa la supervisión humana y la gestión iterativa de riesgos.

5.5. Trazabilidad y rendición de cuentas

Toda iniciativa relevante con IA debe conservar evidencia suficiente para explicar decisiones y auditar: políticas de uso, prompts y versiones significativas, fuentes, configuraciones aplicadas, decisiones de corrección y criterios de evaluación. En docencia, se recomienda que el "producto" (resultado) venga acompañado de su "proceso" (bitácora/reflexión), y que las decisiones de calificación mantengan revisión humana.

5.6. Incidentes y consultas

Se define como canal único de comunicación, la oficina virtual de ED y el correo ticketed@unnoba.edu.ar para consultas sobre las herramientas y su utilización.

5.7. Capacitación y sensibilización

La gobernanza se sostiene con alfabetización continua de todos los roles: ética y riesgos, privacidad desde el diseño, diseño de consignas con evidencia de proceso, verificación 3C (Citas-Coherencia-Corroboración), accesibilidad, y criterios de selección de herramientas. Estas acciones formativas operacionalizan los principios de supervisión humana y responsabilidad promovidos por UNESCO (2021) y el enfoque de gestión de riesgos propuesto por NIST (2023).

En este sentido, se dictará una Diplomatura Universitaria de Posgrado en Estrategias Educativas con Inteligencia Artificial diseñada por ED para promover en la comunidad universitaria la comprensión crítica y el uso estratégico de la Inteligencia Artificial en los procesos educativos, favoreciendo el diseño de estrategias pedagógicas, recursos digitales y prácticas de análisis de datos que fortalezcan la enseñanza y la toma de decisiones en distintos contextos formativos.

Asimismo, se ofrecen talleres para áreas administrativas de la Universidad en relación a la aplicación de la IA en diferentes procesos.

El resultado esperado es una adopción de IA gradual, transparente y verificable, en la que las personas deciden, los datos se resguardan, y los aprendizajes de cada prueba piloto mejoran las prácticas institucionales.

6. Selección y evaluación de herramientas

Para que el uso de IA en UNNOBA sea seguro, pertinente y sostenible, la selección de herramientas debe seguir un proceso claro, documentado y proporcional al riesgo. Este enfoque se alinea con marcos internacionales que promueven supervisión humana significativa, gestión de riesgos y mejora continua.

6.1. Criterios mínimos de adopción: ¿qué mirar antes de decidir?

- **Propósito y marco institucional.** La herramienta debe responder a un objetivo educativo u operativo, conectado con resultados de aprendizaje o mejoras de proceso.
- **Datos que procesa**. Identificar qué datos requiere (personales, sensibles o no), dónde se alojan, quién accede y para qué; aplicar minimización, anonimización, seudonimización y, cuando corresponda, consentimiento informado, etc.
- **Privacidad y seguridad.** Verificar términos de uso, políticas de privacidad, cifrado, controles de acceso y, si hay transferencia a terceros, la existencia de acuerdos de procesamiento de datos adecuados.
- **Accesibilidad e inclusión**. Comprobar compatibilidad con pautas de accesibilidad (alineadas a WCAG), alternativas multiformato y funcionamiento con limitaciones de conectividad.
- **Calidad y explicabilidad.** Explorar evidencia de validez, consistencia y capacidad de revisión (registros, versiones, logs); priorizar herramientas que permitan auditar o explicar salidas en contextos críticos.
- **Riesgos y mitigaciones.** Anticipar posibles respuestas inventadas, sesgos, descontextualización o exposición de datos; definir controles (verificación 3C, revisión humana, límites de uso, restricciones de carga).
- **Costos y sostenibilidad.** Evaluar licencias, soporte, cantidad de usuarios, dependencias y condiciones de renovación; considerar alternativas libres para pilotos.
- **Plan de desactivación.** Asegurar portabilidad de datos y contenidos, y un procedimiento claro para desactivar o reemplazar la herramienta sin afectar la operación (evitar *vendor lock-in*[1]).

6.2. Matriz de decisión (plantilla operativa)

Para cada herramienta se recomienda registrar en una plantilla como la que se muestra en la Ilustración 1 (Ejemplificativa).

[1] *Vendor lock-in:* "bloqueo de proveedor" es quedar **atado** a una herramienta o empresa de tal manera que **cambiar** después resulta difícil, caro o arriesgado.

Esta matriz instrumenta la trazabilidad que recomiendan UNESCO (ética y derechos) y NIST (gestión de riesgos), y es coherente con el enfoque de sistema de gestión propuesto por ISO/IEC 42001.

Se podría implementar además, un mini “semáforo de riesgo” dentro de la plantilla:

- **Verde (bajo):** sin datos personales; uso individual; medidas básicas de verificación.
- **Amarillo (medio):** apoyo a feedback o clase; controles y alternativa sin IA; “prueba piloto”.
- **Rojo (alto):** trata datos personales o afecta decisiones sobre personas; requiere revisión jurídica, DPA[2], piloto acotado y autorización específica.

[2] DPA: Data Processing Agreement (en español: Acuerdo de Tratamiento de Datos).

Es el contrato que se firma con un proveedor externo que va a procesar datos personales de la universidad. Deja por escrito el “qué, cómo y para qué” de ese tratamiento, y exige medidas de seguridad y confidencialidad.

Título de la herramienta:
Enlace a la herramienta:
Área / Asignatura solicitante:
Fecha:

1) Objetivo y uso propuesto

.....
.....

2) Datos tratados (tipo, sensibilidad, almacenamiento)

- Tipos de datos: .....
- ¿Hay datos personales/sensibles?: Sí / No (¿cuáles?) .....
- Almacenamiento y ubicación: ..... / Retención: .....
- Accesos (quién y para qué): .....

3) Riesgos identificados y mitigaciones previstas

Riesgos: .....
Mitigaciones (verificación 3C, revisión humana, límites, etc.): .....

4) Accesibilidad y requerimientos técnicos

- WCAG / lectura fácil / subtítulos: .....
- Conectividad / dispositivos: .....
- Integración (Moodle/API/otros): .....

5) Términos / DPA y seguridad

- Política de privacidad y uso de datos: .....
- Cifrado / control de accesos / registros: .....
- ¿Existe DPA o cláusula de tratamiento con terceros?: Sí / No (detalle) .....

6) Costo / licencia y escala

- Tipo de licencia / costo estimado: .....
- N° de usuarios / soporte / renovación: .....

7) Evidencia de calidad (piloto responsable, métricas)

- Alcance del piloto: ..... Duración: .....
- Métricas (resultado, uso, satisfacción, incidencias): .....
- Lecciones aprendidas: .....

8) Decisión

□ Aprobar □ Aprobar con restricciones □ No aprobar
Condiciones/restricciones: .....

9) Plan de salida

- Exportación (formatos abiertos): .....
- Devolución/borrado de datos: .....
- Pasos y tiempos para desactivar/migrar: .....

Responsables y firmas

Solicitante: ..... Área/Asignatura: ..... Fecha: .....
ED(revisión): ..... Conducción (aprobación): ..... Fecha: .....

Ilustración 1: Matriz de decisión para la solicitud de herramientas de IA (Plantilla)

6.3. Evaluación proporcional al riesgo: ¿cómo decidir la profundidad del análisis?

- Riesgo bajo (por ejemplo, propuestas individuales sin datos personales). Revisión rápida de términos y límites de uso; incluir advertencias de verificación y no cargar información sensible.
- Riesgo medio (por ejemplo, apoyo a feedback en borradores, sin datos sensibles). Matriz completa, “prueba piloto” con trazabilidad, verificación 3C y alternativa sin IA.
- Riesgo alto (por ejemplo, tratamiento de datos personales, decisiones que afectan a personas o calificaciones). Análisis reforzado: asesoría de ED+Pro-TIC, revisión jurídica de términos/DPA, controles de acceso, registro detallado de actividad, prueba acotada y aprobación específica antes de escalar.

6.4. Prueba piloto y decisión

Antes de cualquier despliegue amplio, realizar un “prueba piloto” (revisar la definición en el punto 4): alcance limitado, objetivos y métricas claras, protección de datos, capacitación mínima, bitácora (prompts, versiones, incidencias) y duración definida. Con el informe de resultados, decidir escalar, ajustar o descartar la herramienta.

Este ciclo de “probar - evaluar - ajustar” materializa la supervisión humana y la mejora continua (UNESCO, 2021; NIST, 2023).

6.5. Registro y rendición de cuentas

Toda herramienta aprobada debe contar con: (a) ficha de evaluación (matriz), (b) configuración recomendada (privacidad y accesibilidad), (c) límites de uso (qué sí/qué no), (d) responsables, (e) canal de soporte y (f) criterios de desactivación. En docencia, las políticas de curso (cláusulas de IA) deben reflejar esas condiciones.

6.6. Señales de alerta: ¿cuándo NO avanzar?

- Términos que habilitan uso comercial de datos institucionales sin control.
- Imposibilidad de exportar contenidos/datos (sin plan de salida).
- Falta de controles de acceso, cifrado o registro de actividad.
- Dependencia total de la herramienta para funciones críticas sin alternativa o supervisión humana.

- Evidencia de sesgos significativos sin mitigación razonable.

Con este proceso, UNNOBA elige y usa herramientas de IA que agregan valor real, resguardan derechos, reducen riesgos y dejan huellas verificables para aprender y mejorar con cada iteración. La institución considera indispensable la intervención humana y análisis con criterio de la utilización de los resultados que den las herramientas.



Gráfico realizado por Educación Digital by Napkin

7. Privacidad, datos y seguridad

Para garantizar un uso de la IA en la UNNOBA que sea confiable y respetuoso de los derechos, la Universidad adopta un enfoque de privacidad desde el diseño y por defecto, junto con gestión de riesgos, aplicado de forma continua a todo el ciclo de vida de los datos y de las herramientas. Este apartado se alinea con la normativa argentina (Ley 25.326 y Decreto 1558/2001, autoridad AAIP) y con marcos internacionales que recomiendan supervisión humana significativa, documentación y controles proporcionales al riesgo (UNESCO, *Recomendación sobre la Ética de la IA*, 2021; NIST, *AI Risk Management Framework 1.0*, 2023).

7.1. Principios prácticos: ¿qué debe guiar cada decisión?

- **Licitud y finalidad clara.** Tratar datos sólo con un propósito legítimo y explícito; evitar usos secundarios no informados.
- **Minimización y proporcionalidad.** Recabar lo estrictamente necesario; preferir datos anónimos o pseudonimizados cuando sea posible.

- **Transparencia y trazabilidad.** Informar qué se hace con los datos, con qué herramienta y para qué; conservar huellas de proceso (prompts/versiones) cuando corresponda.
- **Seguridad por diseño.** Implementar controles técnicos y organizativos (cifrado, accesos, registros, retención/borrado).
- **Supervisión humana**. Mantener revisión y decisión humana en procesos que afecten a personas (evaluaciones, comunicaciones oficiales, decisiones administrativas).

7.2. Clasificación de datos y reglas de tratamiento

- **Datos sin identificación** (bajo riesgo). Ej.: consignas genéricas, textos ficticios, código no sensible. Uso permitido, sin restricciones especiales.
- **Datos personales** (riesgo medio). Ej.: nombre, correo institucional, desempeño académico. Requiere minimización, base legal (información/consentimiento si corresponde), y controles (accesos, retención).
- **Datos sensibles o confidenciales** (alto riesgo). Ej.: salud, situación socioeconómica, actas internas, expedientes. No cargar en servicios externos sin acuerdos de tratamiento (DPA) y garantías robustas; preferir entornos institucionales y, si no es imprescindible, no usarlos.

7.3. Controles mínimos obligatorios

(Antes de usar una herramienta):

- ¿Puedo cumplir el objetivo sin datos personales o sensibles?
    - Sino, ¿apliqué anonimización, pseudonimización o minimización?
- ¿La herramienta tiene términos compatibles, cifrado y DPA (si hay terceros)?
- ¿Informé a las personas involucradas y ofrecí alternativa sin IA, si corresponde?
- ¿Definí retención y borrado? ¿Quién es responsable?

7.4. Lo que NO debe hacerse

- Subir datos sensibles o información confidencial a servicios sin garantías contractuales y técnicas.
- Delegar decisiones sustantivas a la IA sin revisión humana.
- Usar “detectores de IA” como única evidencia para sanciones.
- Adoptar herramientas que impidan exportar datos/contenidos o que carezcan de DPA cuando corresponda.

7.5. Evaluación proporcional al riesgo (cómo ajustar el nivel de control)

- **Bajo** (Propuestas con datos ficticios): aviso de buenas prácticas + límites de uso (no subir datos reales).
- **Medio** (apoyo a feedback, sin datos sensibles): “prueba piloto” con trazabilidad, revisión 3C (Citas–Coherencia–Corroboración), alternativa sin IA, configuración segura.
- **Alto** (datos personales, decisiones sobre personas): asesoría de ED y de ProTIC, revisión jurídica de términos(DPA), controles reforzados, prueba acotada, autorización específica antes de escalar.

7.6. Roles y responsabilidades

Se mantienen los roles y las responsabilidades definidos en el punto 5.2.

7.7. Incidentes, registro y mejora continua

- Registro de incidentes: cada evento (por ej. exposición de datos, salida discriminatoria, entre otros) debe documentarse con fecha, alcance, datos comprometidos (si los hubiera), acciones correctivas y observaciones.
- Ciclo de mejora: Cuestiones a tener en cuenta para nuevas actualizaciones.
- Formación continua: incluir recomendaciones de capacitación.

8. Integridad académica y evaluación

Con el fin de sostener una cultura de honestidad, aprendizaje auténtico y responsabilidad compartida, la UNNOBA entiende que la IA es un apoyo al trabajo intelectual, no un sustituto de la autoría ni del criterio profesional. En consecuencia, las actividades y evaluaciones deben promover la transparencia del proceso, la verificación humana significativa y la trazabilidad del trabajo (UNESCO, *Recomendación sobre la Ética de la IA*, 2021; NIST, *AI RMF 1.0*, 2023).

8.1. Principios aplicados a la evaluación

- **Producto + proceso**. Toda entrega relevante debe incorporar evidencias del cómo: prompts, versiones significativas, fuentes utilizadas y breve reflexión crítica.
- **Supervisión humana.** Las decisiones de calificación son humanas y deben considerar la comprensión y la capacidad de justificar el resultado.
- **Transparencia**. El uso de IA se declara (herramienta, fecha, versión, alcance del apoyo).
- **Autenticidad y defensa.** En evaluaciones con calificaciones numéricas, se recomiendan instancias orales o prácticas breves para acreditar comprensión y autoría.
- **Proporcionalidad**. Las consignas deben pedir criterio, aplicación y transferencia, no mera reproducción.

8.2. Limitaciones de detectores y enfoque de verificación

- Los detectores de “texto hecho con IA” no constituyen prueba concluyente; pueden errar con textos breves, traducciones o materiales editados.
- Se prioriza la verificación 3C: Citas (fuentes verificables), Coherencia (con la consigna y el curso) y Corroboración (chequeo cruzado de afirmaciones y datos).

8.3. Diseño de consignas

- Solicitar aplicación contextualizada al contexto, uso de datos o criterios propios, toma de decisiones justificada y defensa breve.

- Incluir restricciones de uso de IA (qué sí y qué no) y alternativas para quienes no puedan o quieran usarla.
- Evaluar con rúbricas que consideren: pertinencia del uso de IA, integridad y/o citación, verificación, reflexión y resguardo de datos.

8.4. Procedimiento ante dudas de autoría

1. Revisión 3C y análisis del proceso entregado.
2. Solicitud de aclaraciones y/o defensa breve.
3. Registro del caso y acciones formativas (no sólo punitivas), privilegiando el aprendizaje sobre la mera sanción.

Con esta implementación se espera que las evaluaciones sean más auténticas y formativas, con decisiones transparentes, trazables y centradas en la comprensión.

9. Gestión de riesgos y control de calidad

Dada la naturaleza probabilística de muchos sistemas de IA, la gestión de riesgos debe ser continua, documentada y proporcional. Este apartado adopta el ciclo identificar,evaluar, mitigar y monitorear recomendado por marcos internacionales (NIST, 2023) y lo combina con principios de ética, derechos y supervisión humana (UNESCO, 2021).

9.1. Riesgos frecuentes

- **Respuestas inventadas y descontextualización.** Contenidos aplicables pero incorrectos o fuera de contexto.
- **Sesgos y trato desigual.** Salidas que reproducen estereotipos o discriminación.
- **Exposición o derivación de datos.** Filtración, entrenamiento no deseado o uso secundario de información.
- **Falta de explicabilidad o auditoría**. Dificultad para entender o revisar cómo se generó un resultado.
- **Dependencia tecnológica**. Imposibilidad de migrar contenidos o datos sin pérdida.

9.2. Controles y mitigaciones

- Verificación 3C y supervisión humana en decisiones sustantivas.
- Trazabilidad sistemática (prompts, versiones, fuentes, configuraciones).
- Privacidad por diseño: minimización, anonimización, pseudonimización, acuerdos de tratamiento (DPA) cuando aplique.
- Evaluación proporcional al riesgo (bajo/medio/alto) y “pruebas pilotos” antes de escalar.
- Revisión por pares y listas de chequeo previas a la publicación o al uso en clase.

9.3. Ciclo de control de calidad

1. **Planificar**: definir objetivos, métricas y límites de uso de la herramienta.
2. **Hacer**: ejecutar “prueba piloto”con documentación.
3. **Verificar**: medir resultados (calidad, equidad, accesibilidad, satisfacción, incidentes).
4. **Actuar**: ajustar, escalar o descartar; actualizar la matriz (Ver punto 6) y esta guía.

Este ciclo es coherente con la gestión de riesgos del NIST y con el enfoque de mejora continua recomendado por la UNESCO.

9.4. Señales de alerta

- Términos que permiten reutilizar datos con fines comerciales.
- Imposibilidad de exportar datos/contenidos a formatos abiertos.
- Ausencia de controles de acceso, cifrado o logs.
- Evidencia de sesgos sin respuesta del proveedor ni mitigación viable.

Realizando esta gestión de riesgos y de calidad, se espera lograr decisiones informadas y trazables, reducción de incidentes y aprendizaje institucional acumulativo.

10. Inclusión y accesibilidad

La inclusión es un compromiso ético y una obligación legal para universidades públicas argentinas. La accesibilidad digital en UNNOBA se alinea con la Ley 26.653 y con pautas internacionales WCAG 2.1/2.2, reforzando el principio de no discriminación y el derecho a aprender y trabajar con igualdad de oportunidades (UNESCO, 2021).

10.1. Principios aplicados

- Diseño para todas las personas. Contenidos comprensibles, perceptibles, operables y robustos (POUR de WCAG).
- Equidad de acceso. Alternativas no digitales o de baja conectividad cuando haga falta; opciones de lectura fácil y apoyos multiformato (texto, audio, video, subtítulos, transcripciones).
- Interoperabilidad educativa. Compatibilidad con la Plataforma de Educación Digital (Moodle) y tecnologías de asistencia.

10.2. Requisitos mínimos en cursos y materiales

- Imágenes y gráficos con texto alternativo; tablas etiquetadas.
- Videos con subtítulos y, cuando sea posible, transcripción.
- Contraste suficiente y tamaño de fuente legible; evitar solo color para transmitir información.
- Navegación por teclado, foco visible y enlaces con texto descriptivo (“Descargar guía”, no “clic aquí”).
- Documentos y evaluaciones compatibles con lectores de pantalla; evitar formatos escaneados sin OCR.

10.3. IA al servicio de la inclusión

- Transcripción y subtitulado preliminar de clases virtuales.
- Simplificación de lectura y resúmenes accesibles (con verificación humana).
- Apoyo multilingüe inicial (traducción preliminar + revisión humana).
- Generación de alternativas (descripción de imágenes, versiones de “lectura fácil”), entre otras.

11. Alfabetización en IA para la comunidad UNNOBA

Con el propósito de asegurar un uso competente, ético y seguro de la IA en todos los estamentos universitarios, la UNNOBA impulsa un plan de alfabetización continua que articula conocimientos, habilidades y actitudes. Este enfoque integra la idea de supervisión humana significativa y la gestión de riesgos durante todo el ciclo de vida de los proyectos (UNESCO, 2021; NIST, 2023).

Como se menciona en el punto 5.2, desde Educación Digital se ponen a disposición cursos y capacitaciones para fomentar el buen uso de la IA en la Institución.

Se prevén microcredenciales por tema/rol, con materiales de autoformación abiertos, y un canal único de consultas técnico-pedagógicas (ED) para acompañar implementaciones y resolver incidentes.

12. Seguimiento y mejora continua

A fin de sostener una adopción gradual, transparente y verificable, se establecerá un esquema de seguimiento con indicadores, revisión periódica y acciones de mejora, en línea con los ciclos de calidad sugeridos por marcos internacionales (NIST, 2023; UNESCO, 2021).

13. Usos pedagógicos recomendados

El uso pedagógico de la IA debe agregar valor al aprendizaje, no reemplazarlo. Por ello, se priorizan usos que mejoran la comprensión, el andamiaje y la retroalimentación, manteniendo la supervisión humana y la verificación 3C (UNESCO, 2021; NIST, 2023).

13.1. Familias de uso

- **Planificación y guionado** de clases y materiales.
- **Generación de ejemplos/contraejemplos** y **tutoría socrática** para el razonamiento.
- **Andamiaje y feedback** en borradores (texto, código, presentaciones).
- **Bancos de ítems** para evaluación (con revisión humana previa).
- **Metacognición** (explicar el proceso, detectar supuestos).

- **Accesibilidad** (transcripción, simplificación, traducción preliminar).
- **Analítica formativa ligera** (sin datos personales/sensibles).
- **Programación asistida** (explicación de errores, pruebas y refactor).



Gráfico realizado por Educación Digital by Napkin

14. Capacidades positivas de la IA en docencia

Para orientar la práctica cotidiana, se reconocen doce capacidades que, con verificación y adaptación local, suelen elevar la calidad del trabajo docente y del aprendizaje:

1) Lluvia de ideas. 2) Reformulación clara. 3) Ejemplificación múltiple. 4) Tutor. 5) Feedback según rúbrica. 6) Andamiaje paso a paso. 7) Generación de ítems (con revisión). 8) Accesibilidad (transcripción/lectura fácil). 9) Detección de falencias. 10) Programación asistida. 11) Organización ágil (guiones/checklists). 12) Analítica formativa ligera (sin datos sensibles).



Gráfico realizado por Educación Digital by Napkin

Siempre con **supervisión humana** y **verificación 3C** antes de publicar, evaluar o comunicar resultados.

15. Usos no recomendados o prohibidos

Para proteger la integridad académica, los derechos de las personas y la calidad institucional, se establecen las siguientes restricciones:

- **Delegación total de autoría** en IA para trabajos evaluables.
- **Calificación automatizada** sin **revisión humana**.
- Uso de **detectores de IA** como **única evidencia** de sanción.

- **Referencias inventadas** o citas no verificables.
- Carga de **datos personales/sensibles** o **información confidencial** en servicios sin **garantías contractuales/técnicas** (ni DPA cuando aplique).
- Adopción de herramientas sin **plan de salida** ni **portabilidad** de datos/contenidos.

Ante situaciones poco claras, se aplicará el principio de prudencia, con “pruebas pilotos”, trazabilidad y revisión por pares antes de escalar.

Referencias bibliográficas

- Agencia de Acceso a la Información Pública. (s. f.). *Protección de datos personales*. https://www.argentina.gob.ar/aaip/datospersonales
- Argentina. (2000). *Ley 25.326 de Protección de Datos Personales*. Boletín Oficial de la República Argentina.
- Argentina. (2001). *Decreto 1558/2001. Reglamentación de la Ley 25.326*. Boletín Oficial de la República Argentina.
- Argentina. (2010). *Ley 26.653 de Accesibilidad de la Información en las Páginas Web*. Boletín Oficial de la República Argentina.
- ISO/IEC. (2023). *ISO/IEC 42001:2023—Artificial intelligence management system*. International Organization for Standardization. https://www.iso.org/standard/42001
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework
- UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://unesdoc.unesco.org/ark:/48223/pf0000380455

- W3C. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*. World Wide Web Consortium. https://www.w3.org/TR/WCAG22/

TAMARIT Guillermo Ricardo
Rector UNNOBA
02/12/2025 13:55
hora estándar de Argentina

PASSARELLO Mariana Vanesa
Secretaria General
02/12/2025 10:44
hora estándar de Argentina