INTELIGENCIA ARTIFICIAL, DERECHOS HUMANOS Y ÉTICA
Retos y Responsabilidades en la Era Digital

Ing. Hernán José Zepeda Castro

Experto en Cibercrimen y Ciberseguridad

CONADEH

La pregunta que debemos hacernos

- ¿Aceptaríamos que un algoritmo decidiera sobre nuestros derechos sin explicarnos cómo llegó a esa conclusión?
- ¿Quién responde cuando la inteligencia artificial se equivoca?
- ¿Puede un sistema tecnológico discriminar?
- ¿Quién controla las decisiones automatizadas?



CONADEH

Objetivos

- Comprender la relación entre IA, derechos humanos y ética.
- Identificar riesgos de discriminación, privacidad y vulneración de derechos.
- Reconocer las responsabilidades de quienes desarrollan, implementan y utilizan la IA.
- Aplicar criterios básicos para un uso responsable y seguro.
- Proponer medidas de gobernanza y supervisión humana.



CONADEH

¿Qué Entendemos por Inteligencia Artificial?

La inteligencia artificial comprende sistemas tecnológicos capaces de producir resultados como:

- Predicciones y clasificaciones.
- Recomendaciones y decisiones.
- Generación de textos, imágenes, audio y video.
- Análisis de datos y reconocimiento de patrones.

La IA procesa información y genera resultados; eso no significa que comprenda la realidad como un ser humano.

CONADEH

Tres Grandes Categorías de Inteligencia Artificial

IA predictiva

Estima resultados, detecta patrones o clasifica información.

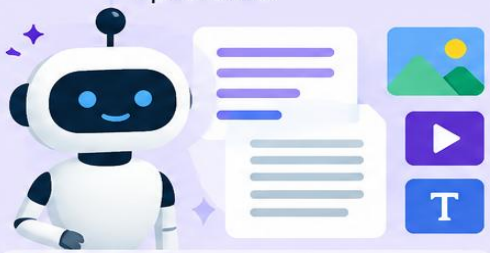


Ejemplos:

- Predecir ventas futuras.
- Detectar fraudes.
- Clasificar correos o documentos.

IA generativa

Produce contenido nuevo a partir de instrucciones y patrones aprendidos.



Ejemplos:

- Generar resúmenes de documentos.
- Crear textos, imágenes o videos.
- Redactar correos o informes.

Sistemas de decisión asistida

Proporcionan recomendaciones que pueden influir en decisiones humanas o automatizadas.



Ejemplos:

- Recomendar el mejor curso de acción.
- Sugerir tratamientos médicos.
- Apoyar decisiones de inversión.

Estos tipos pueden combinarse

Por ejemplo, una herramienta puede clasificar documentos y posteriormente generar un resumen.

1 Clasificar documentos
(IA predictiva)



2 Generar resumen
(IA generativa)



CONADEH

El ciclo de vida de un sistema de IA

Desde la definición del problema hasta su retiro, cada etapa influye en la calidad, los riesgos y el impacto del sistema.

1 Datos y definición del problema



- Identificar el problema o necesidad.
- Reunir y analizar los datos.
- Definir la finalidad y el alcance.
- Verificar la calidad, representatividad y posibles sesgos en los datos.

Ejemplo:
Datos históricos de solicitudes para detectar fraudes.

2 Diseño y desarrollo



- Seleccionar el tipo de modelo y método.
- Definir variables, criterios y arquitectura.
- Establecer medidas de seguridad y privacidad.
- Considerar requisitos éticos y legales.

Ejemplo:
Diseñar un modelo de clasificación de documentos.

3 Entrenamiento y validación



- Entrenar el modelo con datos.
- Evaluar su rendimiento y precisión.
- Detectar y corregir sesgos.
- Probar con datos de diferentes grupos y en diversos escenarios.

Ejemplo:
Validar que el modelo funcione correctamente con distintos tipos de documentos.

4 Implementación y uso



- Integrar el sistema en la organización.
- Definir roles, permisos y procedimientos.
- Capacitar al personal usuario.
- Utilizar el sistema conforme a su finalidad.

Ejemplo:
Poner en producción una herramienta que clasifica y resume documentos.

5 Supervisión y evaluación



- Monitorear el rendimiento en uso real.
- Detectar errores, sesgos o usos indebidos.
- Revisar el impacto en los usuarios.
- Auditar y documentar resultados.

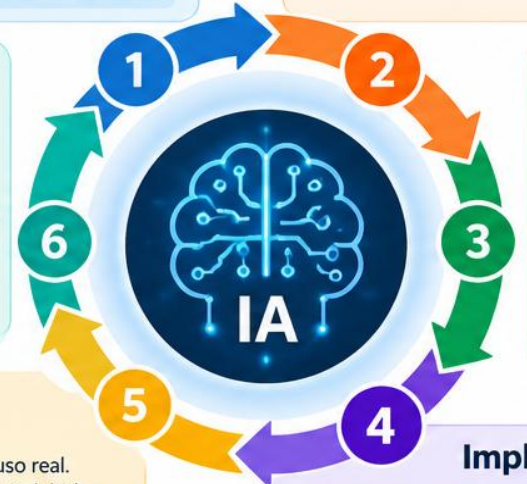
Ejemplo:
Analizar métricas de precisión y revisar casos en los que el sistema se equivoca.

6 Corrección, sustitución o retirada



- Corregir fallos y mejorar el modelo.
- Actualizar datos y controles.
- Sustituir el sistema si deja de ser adecuado.
- Retirarlo cuando genere riesgos inaceptables.

Ejemplo:
Actualizar el modelo con nuevos datos o retirarlo si ya no cumple su finalidad.



La IA debe ser desarrollada, implementada y utilizada de manera responsable, con supervisión humana, transparencia, protección de datos y evaluación continua de sus riesgos e impactos.

CONADEH

Ciclo de Vida de un Sistema de IA

El riesgo no aparece únicamente cuando alguien utiliza una herramienta. Puede originarse en los datos de entrenamiento, las decisiones de diseño, los criterios de evaluación o la forma de incorporar el sistema a una organización.

Ejemplo: una herramienta de selección de personal puede funcionar correctamente desde el punto de vista informático y, aun así, ofrecer resultados injustos porque fue entrenada con datos históricos que reflejan desigualdades.

La prevención debe cubrir todo el ciclo de vida, no solamente revisar los resultados después de que ocurra un daño.

CONADEH

¿Por Qué Necesitamos un Enfoque de Derechos Humanos?

- Las personas deben estar en el centro del desarrollo tecnológico.
- La innovación no justifica cualquier medio.
- La dignidad humana debe orientar las decisiones.
- Los riesgos deben identificarse antes de producir daños.
- Deben existir mecanismos de reclamación y reparación.

El enfoque de derechos humanos cambia la pregunta de "¿funciona esta tecnología?" a "¿funciona adecuadamente, para quién funciona y qué consecuencias puede producir?".

La Declaración Universal de Derechos Humanos aporta referencias fundamentales sobre dignidad, igualdad, privacidad, libertad de expresión y protección efectiva frente a vulneraciones. Estos principios también son relevantes cuando las decisiones están mediadas por sistemas digitales.

CONADEH

Inteligencia Artificial y Derechos Humanos

Derechos humanos que pueden verse afectados por la IA

La inteligencia artificial puede aportar grandes beneficios, pero también puede generar riesgos para los derechos fundamentales de las personas, dependiendo de cómo se utilice, qué datos se empleen y con qué finalidad.

1 Privacidad y protección de datos

Recolección, análisis, almacenamiento y reutilización de información personal.



Posibles riesgos:

- Uso de datos sin consentimiento.
- Elaboración de perfiles personales.
- Exposición de datos sensibles.
- Reutilización para otros fines.
- Filtraciones y accesos no autorizados.

2 Igualdad y no discriminación

Tratamientos desiguales derivados de datos, modelos o decisiones de implementación.



Posibles riesgos:

- Sesgos en los datos o algoritmos.
- Resultados injustos o excluyentes.
- Discriminación directa o indirecta.
- Perjuicio a grupos vulnerables.
- Falta de representatividad en los datos.



3 Libertad de expresión e información

Manipulación, moderación opaca y circulación de contenidos falsos.



Posibles riesgos:

- Difusión de desinformación.
- Manipulación de contenidos.
- Moderación automatizada sin claridad.
- Restricción indebida de opiniones.
- Uso de IA para campañas de influencia.

4 Debido proceso y acceso a la justicia

Decisiones difíciles de cuestionar y errores sin mecanismos de revisión.



Posibles riesgos:

- Decisiones automatizadas opacas.
- Falta de explicaciones comprensibles.
- Limitación del derecho de defensa.
- Uso de IA en evaluaciones de riesgo.
- Dificultad para impugnar resultados.

5 Dignidad, autonomía e integridad personal

La IA puede influir en las decisiones, comportamientos y en la vida de las personas.



Posibles riesgos:

- Manipulación del comportamiento.
- Pérdida de control sobre decisiones relevantes.
- Vigilancia y seguimiento excesivo.
- Afectación de la reputación digital.
- Vulneración de la integridad psicológica.

Grupos vulnerables y brecha digital

La IA puede generar impactos desiguales en personas y comunidades.



Posibles riesgos:

- Exclusión de servicios y oportunidades.
- Mayor afectación a niños, niñas y adolescentes.
- Impacto en personas con discapacidad.
- Desigualdad en zonas rurales.
- Perjuicio a comunidades poco representadas.

CONADEH

Amenazas Cibernéticas: Cuando la Tecnología se Utiliza para Vulnerar Derechos

Las amenazas cibernéticas pueden comprometer sistemas, datos personales e infraestructuras, causando daños económicos, sociales y jurídicos.



CONADEH

Ética y Legalidad: ¿son lo mismo?

Legalidad	Ética
Determina obligaciones y límites jurídicos aplicables.	Orienta la valoración de las decisiones y sus consecuencias.
Establece responsabilidades y consecuencias legales.	Ayuda a identificar riesgos y dilemas.
Se verifica conforme al marco normativo aplicable.	Exige deliberación, responsabilidad y mejora continua.

Cumplir la ley es indispensable, pero una decisión también debe evaluarse por sus efectos sobre las personas.

CONADEH

Ética y Legalidad: ¿son lo mismo?

Ética y Derecho no son conceptos opuestos, La ética puede orientar decisiones ante riesgos nuevos o situaciones en las que la norma no ofrece una respuesta tecnológica específica, mientras el Derecho fija obligaciones y garantías vinculantes.

La ética, por sí sola, no sustituye las obligaciones jurídicas. Tampoco es suficiente publicar un código de conducta si no existen procedimientos reales para prevenir, detectar y corregir daños.



CONADEH

Principios para una inteligencia artificial responsable

Principio	¿Qué significa?	¿Por qué es importante?	Ejemplos de aplicación
Dignidad humana Las personas en el centro.	La IA debe respetar la dignidad, los derechos y los intereses de todas las personas, sin reducirlas a simples datos o puntuaciones.	• Protege los derechos fundamenteles. • Evita el uso de la IA para fines que deshumanicen o exploten a las personas. • Promueve una tecnología al servicio del bienestar humano.	• Diseño de sistemas que prioricen el beneficio de las personas. • Evaluación del impacto en los derechos y la calidad de vida. • Consideración de las necesidades de los usuarios finales.
Equidad Prevenir la discriminación.	La IA debe tratar a todas las personas de manera justa, identificando y mitigando sesgos en datos, modelos y resultados.	• Reduce riesgos de discriminación. • Favorece la inclusión de grupos vulnerables. • Aumenta la confianza en los sistemas de IA.	• Uso de datos representativos y diversos. • Pruebas de equidad en los resultados. • Revisión periódica de posibles sesgos.
Transparencia Informar y explicar.	Debe ser posible conocer cuándo se utiliza IA, para qué se utiliza y cómo llega a sus resultados.	• Permite comprender y cuestionar las decisiones. • Facilita la rendición de cuentas. • Fortalece la confianza ciudadana.	• Información clara a los usuarios. • Explicaciones comprensibles sobre los factores relevantes. • Documentación de la finalidad, los datos y las limitaciones del sistema.
Privacidad Proteger los datos.	La IA debe garantizar la protección de los datos personales y respetar la confidencialidad de la información.	• Previene accesos no autorizados. • Reduce riesgos de uso indebido de la información. • Protege la intimidad y la autonomía personal.	• Minimización de datos. • Controles de seguridad y acceso. • Definición de tiempos de conservación y eliminación. • Cumplimiento del marco legal aplicable.
Supervisión humana Control real de las decisiones.	Las personas deben mantener la capacidad de supervisar, revisar y, cuando sea necesario, corregir o detener los sistemas de IA.	• Evita decisiones automatizadas sin control. • Permite considerar el contexto y las circunstancias particulares. • Reduce el riesgo de errores y daños.	• Revisión humana de decisiones de alto impacto. • Definición de roles y responsabilidades. • Mecanismos claros para intervenir y corregir resultados.
Responsabilidad Auditar y corregir.	Deben identificarse los actores responsables y establecerse mecanismos para prevenir, detectar, corregir y reparar posibles daños.	• Fomenta un uso ético y confiable. • Facilita la rendición de cuentas. • Permite mejorar continuamente los sistemas.	• Auditorías y evaluaciones periódicas. • Registro y documentación de decisiones. • Procedimientos para reportar incidentes. • Medidas de corrección y, cuando corresponda, reparación del daño.

CONADEH

Transparencia y Explicabilidad Algorítmica

Un sistema responsable debe permitir conocer, según el contexto:

- Que la IA está siendo utilizada.
- Para qué finalidad se utiliza.
- Qué datos y criterios son relevantes.
- Cuáles son sus limitaciones.
- Cómo se revisa o cuestiona un resultado.
- Quién tiene autoridad para corregirlo.



La transparencia no consiste necesariamente en publicar todo el código fuente. En muchas situaciones, lo más importante para las personas afectadas es disponer de información comprensible sobre la finalidad, los factores relevantes, las limitaciones y las vías de reclamación.

CONADEH

¿Quién es Responsable cuando la IA se Equivoca?

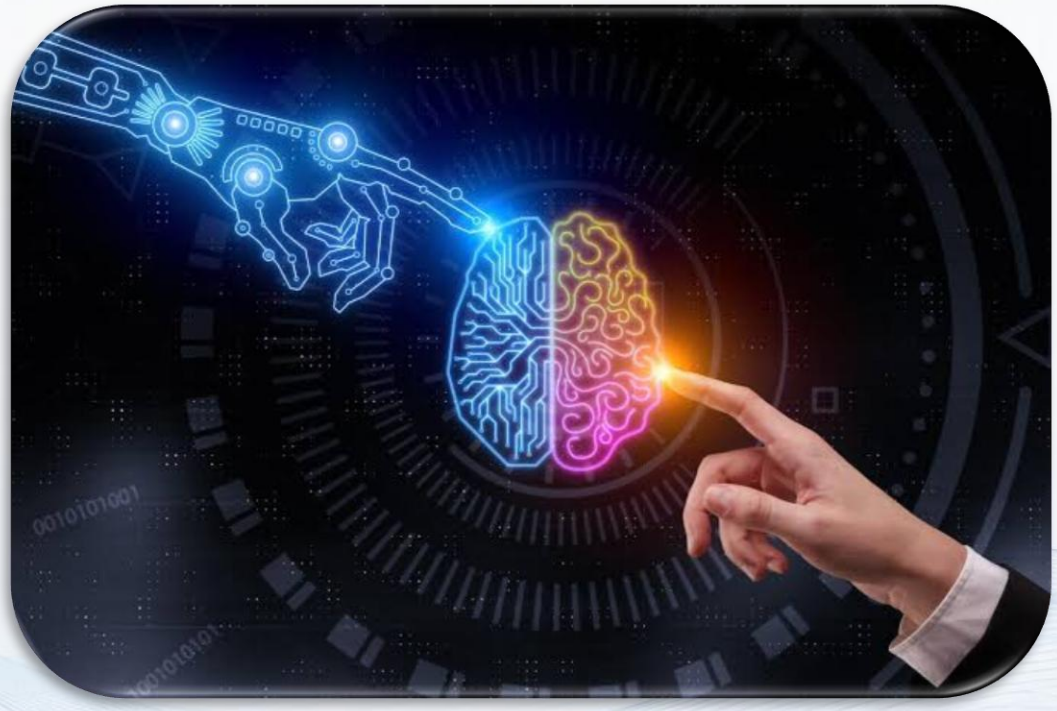
- **Desarrolladores:** diseño, pruebas, documentación y gestión de defectos.
- **Proveedores:** información sobre capacidades, límites y condiciones de uso.
- **Instituciones usuarias:** selección de herramientas, gobernanza y supervisión.
- **Operadores:** utilización competente, verificación y reporte de incidentes.
- **Autoridades competentes:** aplicación del marco jurídico y tutela de derechos según sus atribuciones.

Principio: La responsabilidad no desaparece porque intervenga un algoritmo.

CONADEH

¿Quién es Responsable cuando la IA se Equivoca?

Una institución no debería justificar una decisión perjudicial afirmando simplemente que “el sistema así lo indicó”. Debe poder demostrar por qué se utilizó la herramienta, qué controles existían, cómo se revisaron sus resultados y qué procedimiento permite corregir errores.



CONADEH

Confiabilidad, Ciberseguridad y Gestión de Riesgos

- Riesgos técnicos y operativos
- Respuestas falsas o inexactas.
- Exposición de información confidencial.
- Accesos no autorizados.
- Manipulación de instrucciones o datos.
- Cambios de rendimiento con el tiempo.
- Dependencia excesiva de los resultados automatizados.



Controles: validación, permisos mínimos, pruebas de seguridad, registros, monitoreo y respuesta a incidentes.

CONADEH

Confiabilidad, Ciberseguridad y Gestión de Riesgos

- Riesgos técnicos y operativos
- Respuestas falsas o inexactas.
- Exposición de información confidencial.
- Accesos no autorizados.
- Manipulación de instrucciones o datos.
- Cambios de rendimiento con el tiempo.
- Dependencia excesiva de los resultados automatizados.



Controles: validación, permisos mínimos, pruebas de seguridad, registros, monitoreo y respuesta a incidentes.

CONADEH

Aplicaciones y Dilemas de la Era Digital

Inteligencia artificial en la administración pública y la justicia.

Aplicaciones de apoyo:



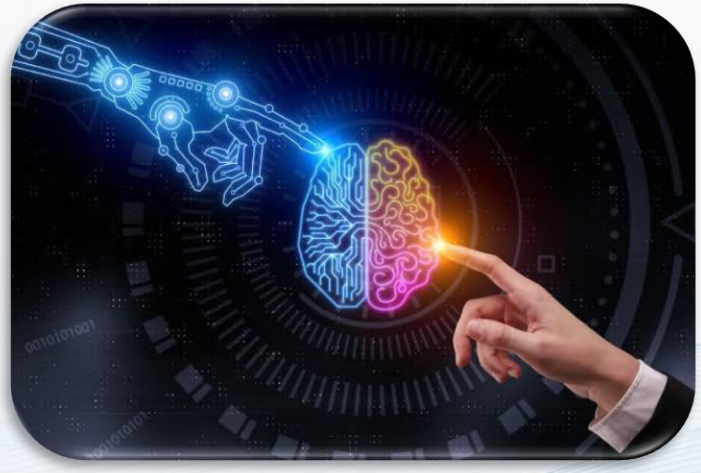
- Búsqueda y clasificación de documentos.
- Elaboración de borradores y resúmenes.
- Traducción y transcripción.
- Detección de inconsistencias documentales.
- Automatización de tareas administrativas.
- Asistencia en la investigación jurídica.

CONADEH

Aplicaciones y Dilemas de la Era Digital

Inteligencia Artificial en la administración pública y la justicia.

Una herramienta generativa puede ahorrar tiempo al localizar información o elaborar un primer borrador, siempre que exista supervisión adecuada.

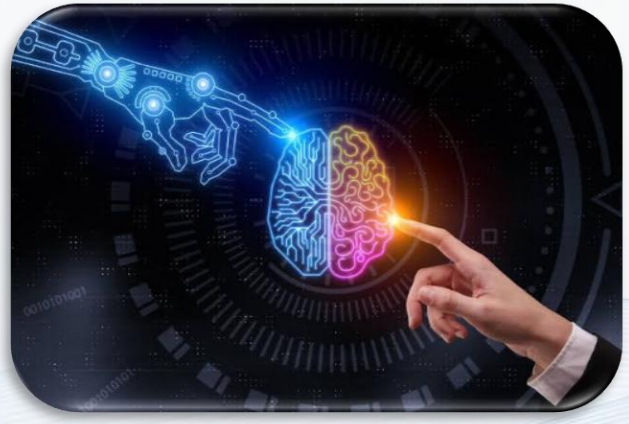


CONADEH

Aplicaciones y Dilemas de la Era Digital

Inteligencia Artificial en la administración pública y la justicia.

Por ejemplo, un funcionario puede utilizar IA para generar una primera estructura de informe. Sin embargo, debe comprobar la exactitud de los hechos, la validez de las fuentes, la normativa citada y la correspondencia del documento con el expediente.



CONADEH

Aplicaciones y Dilemas de la Era Digital

Inteligencia Artificial en la administración pública y la justicia.

Tres precauciones:

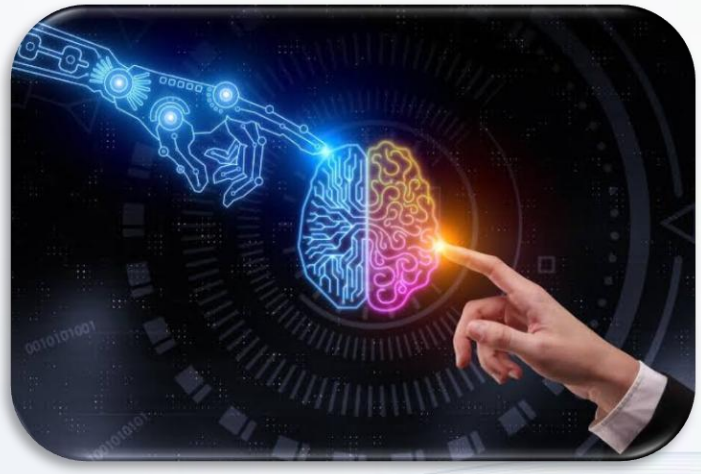
- No introducir expedientes judiciales, datos de víctimas, información de menores ni documentos confidenciales en herramientas que no hayan sido autorizadas institucionalmente.
- No confiar en citas jurisprudenciales o referencias legales generadas sin comprobarlas en fuentes fiables.
- No delegar en un sistema la valoración definitiva de la prueba, la responsabilidad profesional o la decisión que corresponda a una autoridad competente.

CONADEH

Aplicaciones y Dilemas de la Era Digital

Inteligencia Artificial en la administración pública y la justicia.

La IA debe fortalecer las capacidades profesionales, no sustituir el criterio jurídico ni diluir la responsabilidad institucional.



Aplicaciones y Dilemas de la Era Digital

Aplicaciones de alto impacto: ¿dónde debemos ser más cuidadosos?

Ámbito	Aplicaciones típicas de IA	Posible problema o riesgo	Consecuencias	Ejemplos
Contratación laboral	• Preselección de candidatos. • Análisis de currículos. • Evaluación de competencias. • Entrevistas asistidas por IA.	• Sesgos en los datos o algoritmos. • Rechazo injustificado de candidatos. • Falta de transparencia en los criterios. • Evaluación basada en datos irrelevantes.	• Discriminación laboral. • Menor diversidad y oportunidades. • Afectación a la igualdad de trato y al derecho al trabajo.	• Sistemas que asignan puntajes a currículos. • Herramientas que analizan expresiones faciales o voz. • Exclusión de candidatos por motivos indirectamente discriminatorios.
Créditos y seguros	• Evaluación de riesgo crediticio. • Análisis de historial financiero. • Detección de fraude. • Cálculo de primas de seguros.	• Uso de datos incompletos o poco representativos. • Perfiles que reproducen desigualdades. • Decisiones automatizadas sin revisión. • Falta de explicación de resultados.	• Negación injustificada de créditos. • Condiciones desiguales de acceso a seguros. • Exclusión de personas o grupos. • Afectación a la inclusión financiera.	• Algoritmos que infieren capacidad de pago con variables indirectas. • Ajuste automático de primas según perfiles de comportamiento. • Rechazo de créditos sin explicación comprensible.
Educación	• Plataformas de aprendizaje personalizado. • Evaluación automática. • Sistemas de recomendación. • Detección de riesgo de abandono.	• Clasificación inadecuada de estudiantes. • Etiquetado que afecta oportunidades. • Sesgos que perjudican a ciertos grupos. • Uso excesivo de datos personales.	• Menor acceso a oportunidades educativas. • Estigmatización de estudiantes. • Afectación al derecho a la educación y al desarrollo integral.	• Sistemas que predicen rendimiento a partir de datos históricos. • Herramientas que asignan niveles o rutas de aprendizaje automatizadas. • Identificación temprana de "riesgo" sin seguimiento humano adecuado.
Salud	• Apoyo al diagnóstico. • Análisis de imágenes médicas. • Predicción de riesgos. • Gestión de citas y recursos.	• Errores en la interpretación de datos. • Sesgos por falta de diversidad en los datos. • Decisiones automatizadas sin supervisión. • Uso inadecuado de datos sensibles.	• Diagnósticos incorrectos. • Tratamientos inadecuados o tardíos. • Desigualdad en el acceso a servicios. • Afectación al derecho a la salud y a la vida.	• Modelos que analizan radiografías o tomografías. • Sistemas que priorizan pacientes en listas de espera. • Predicción de enfermedades a partir de historiales incompletos.
Seguridad y vigilancia	• Reconocimiento facial. • Análisis de video y comportamiento. • Predicción de riesgos. • Monitoreo de espacios públicos.	• Identificación errónea de personas. • Mayor vigilancia sobre grupos vulnerables. • Uso desproporcionado de la tecnología. • Falta de controles y revisión humana.	• Restricción injustificada de libertades. • Discriminación y estigmatización. • Afectación a la privacidad, la libertad de movimiento y la presunción de inocencia.	• Sistemas de reconocimiento facial en espacios públicos. • Herramientas de análisis predictivo de delitos. • Monitoreo masivo sin criterios claros y transparentes.
Servicios públicos	• Asignación de beneficios sociales. • Evaluación de elegibilidad. • Detección de fraude. • Automatización de trámites y atención ciudadana.	• Exclusión de beneficiarios por errores en los datos. • Criterios poco transparentes. • Desigualdad en el acceso a servicios. • Falta de mecanismos de reclamación.	• Negación injustificada de ayudas. • Mayor desigualdad social. • Afectación al derecho a la protección social y a un trato equitativo. • Pérdida de confianza en las instituciones.	• Sistemas que priorizan la asignación de ayudas con base en puntajes. • Verificación automatizada de requisitos documentales. • Chatbots que rechazan solicitudes sin revisión humana.

La inteligencia Artificial como Herramienta para Promover los Derechos Humanos

La IA puede contribuir a:

- Mejorar la accesibilidad para personas con discapacidad.
- Facilitar la traducción y la comunicación.
- Identificar posibles amenazas de ciberseguridad.
- Detectar patrones de fraude y anomalías.
- Facilitar la búsqueda de información jurídica.
- Apoyar la investigación científica y la educación.
- Mejorar el acceso a determinados servicios públicos.

Principio: Innovar para ampliar derechos, no para reducir garantías.

CONADEH

La inteligencia Artificial como Herramienta para Promover los Derechos Humanos

La inteligencia artificial no es intrínsecamente buena o mala; sus efectos dependen de la manera en que se diseña, implementa y utiliza.

Una herramienta de reconocimiento de voz puede facilitar el acceso a un servicio para alguien que tiene dificultades para escribir. Un sistema de apoyo a la lectura puede ayudar a personas con discapacidad visual. La IA también puede apoyar la detección de amenazas cibernéticas o ayudar a organizar grandes volúmenes de información.

Sin embargo, los beneficios deben comprobarse en condiciones reales y no asumirse únicamente porque el proveedor los anuncie. Es necesario evaluar accesibilidad, precisión, seguridad, costos, efectos sobre los derechos y mecanismos alternativos para quienes no puedan utilizar la solución.

CONADEH

Gobernanza Responsable y Contexto Hondureño

¿Cómo evaluar el impacto de un sistema de IA?



CONADEH

Responsabilidades: del desarrollo al uso institucional

La gobernanza de la IA no puede recaer exclusivamente en el departamento informático de una institución.

Requiere colaboración entre dirección institucional, asesoría jurídica, especialistas en seguridad, responsables de datos, personal usuario y órganos de control pertinentes.

Cuando se adquiere una herramienta comercial, la institución debería conocer sus capacidades y limitaciones, el tratamiento de datos, las condiciones de actualización, las medidas de seguridad y los procedimientos para informar incidentes.

También es importante definir quién autoriza el uso, quién revisa las decisiones de alto impacto y quién debe actuar si se detecta una vulneración.

Una gobernanza efectiva distribuye funciones sin utilizar esa distribución para eludir responsabilidades.

CONADEH

Responsabilidades: del desarrollo al uso institucional

Actor	Responsabilidades principales
Estado y autoridades	Normas, supervisión y protección de derechos en el ámbito de sus competencias.
Institución usuaria	Justificar el uso, establecer controles y evaluar resultados.
Proveedor tecnológico	Documentar capacidades, límites, pruebas y riesgos relevantes.
Personal operador	Verificar resultados y comunicar errores o incidentes.
Organismos de control	Examinar cumplimiento, atender reclamaciones y promover correcciones según sus atribuciones.

CONADEH

Hacia una Inteligencia Artificial Centrada en las Personas - Conclusiones

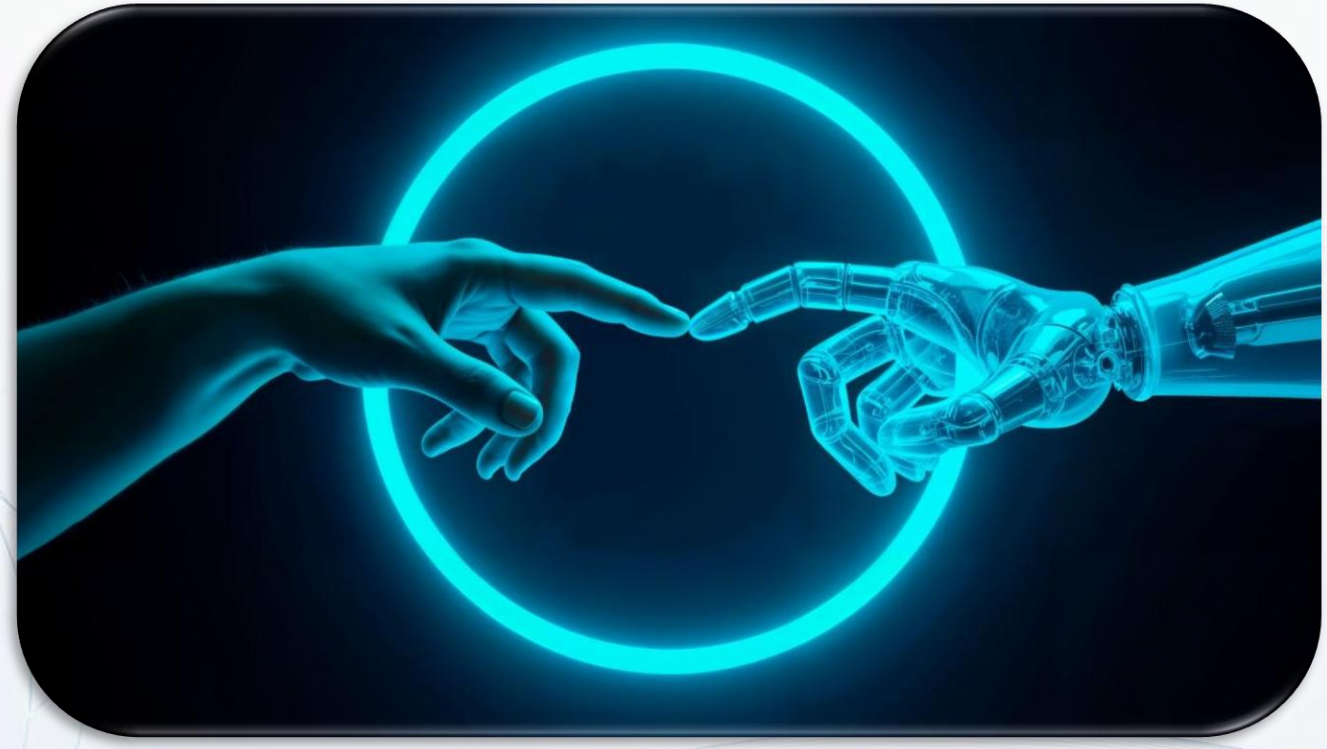
Cinco compromisos para una IA responsable

- Proteger la dignidad humana: la tecnología debe estar al servicio de las personas.
- Prevenir la discriminación: revisar datos, criterios y resultados.
- Respetar la privacidad: proteger los datos durante todo su ciclo de vida.
- Mantener el control humano: supervisar y cuestionar decisiones de alto impacto.
- Asumir responsabilidades: documentar, auditar, corregir y reparar los daños cuando corresponda.

CONADEH

Hacia una Inteligencia Artificial Centrada en las Personas - Conclusiones

La innovación tecnológica debe avanzar acompañada de responsabilidad jurídica, ética y social.



Reflexión Final –¿Qué Tipo de Futuro Digital Queremos Construir?

La inteligencia artificial puede ayudarnos a analizar información, anticipar problemas y encontrar soluciones. Pero no debe convertirse en una excusa para abandonar nuestro juicio, debilitar nuestras garantías ni trasladar la responsabilidad humana a una máquina.



El avance y la evolución tecnológica serán verdaderamente valiosos cuando no solo nos permita hacer más cosas y hacerlas más rápido, sino también hacerlas de manera más justa, segura y respetuosa de la dignidad humana.

CONADEH

Referencias y Fuentes de Consulta

1. UNESCO. Recomendación sobre la Ética de la Inteligencia Artificial (2021).

Marco internacional de principios para el desarrollo y el uso responsable de la IA.

2. Naciones Unidas. Declaración Universal de Derechos Humanos (1948).

Referencia fundamental para la dignidad, la igualdad, la privacidad, la libertad de expresión y la protección efectiva de los derechos.

3. Consejo de Europa. Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (2024).

Referencia internacional sobre garantías, transparencia, responsabilidad y gestión de riesgos durante el ciclo de vida de la IA. Su aplicación jurídica depende de las condiciones correspondientes a cada Estado parte.

4. National Institute of Standards and Technology (NIST). AI Risk Management Framework 1.0 (2023).

Guía para identificar, evaluar y gestionar riesgos relacionados con los sistemas de inteligencia artificial.

5. Constitución de la República de Honduras. Decreto n.º 131-1982.

Marco constitucional de referencia para los derechos y garantías analizados (Artículos 76, 100 y 182).



CONADEH

GRACIAS POR SU ATENCIÓN



CONADEH