

IA y Datos: Ética y Seguridad en un Mundo Inteligente

Cómo equilibrar innovación, privacidad y responsabilidad
en la era de la Inteligencia Artificial

Emilia Bertomeu Bertomeu– 09.06.2025 / Cisco NetaCad

Agenda de la Charla

- 1. Qué es la IA y cómo usa los datos
- 2. Riesgos en la privacidad
- 3. Ética en la IA
- 4. Ciberseguridad y amenazas con IA
- 5. Regulación y gobernanza
- 6. Buenas prácticas
- 7. Reflexión final

¿Qué es la Inteligencia Artificial?

- Sistemas que imitan el pensamiento y decisiones humanas.
- Aprende de grandes volúmenes de datos.

La IA se alimenta de datos:

- Personales: hábitos, ubicación, voz, gustos.
- Corporativos: procesos, finanzas, comunicaciones.

Privacidad bajo amenaza



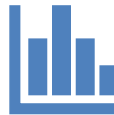
- IA que escucha, observa y predice.



- Publicidad dirigida, vigilancia, extracción de información.



- Asistentes virtuales.

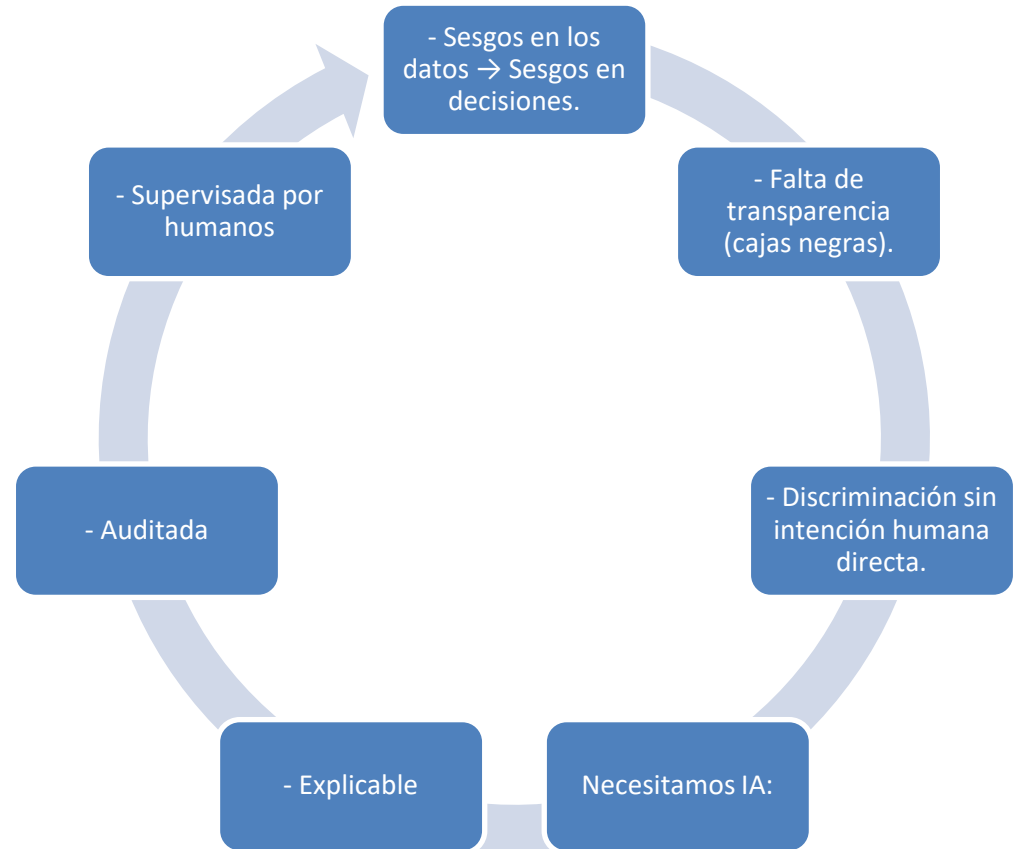


- Fugas de datos personales o corporativos.



- Análisis predictivo mal aplicado.

¿Puede un
algoritmo ser
injusto? Sí.



When GenAI might demonstrate less bias compared to human beings:

- **Impartial Decision-Making**
- Example: Allocating resources without favoring a particular group based on race, gender, or personal relationships.
- **Why it's better:** Unlike humans, who might unconsciously favor people they know or share similarities with, GenAI bases decisions solely on input data and rules.

When GenAI might demonstrate less bias compared to human beings:

- **Impartial Decision-Making**
- **Avoidance of Emotional Bias**
- **Consistent Application of Rules**
- **Neutral in Controversial Topics**
- **Reduced Stereotyping**
- **Consistent Standards in Moderation**

Privacy & Adversarial Use

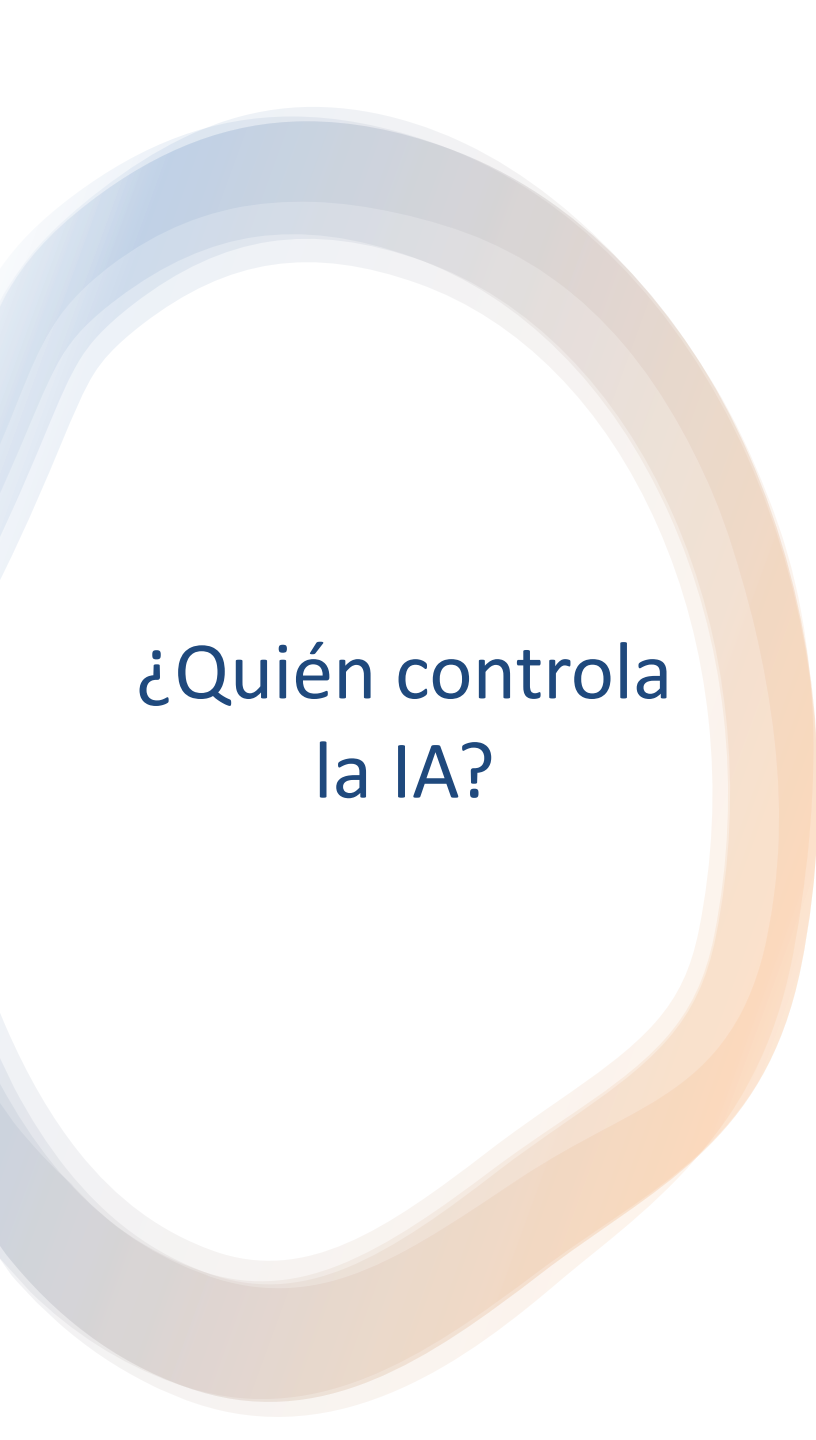
- Training the Model on Your Data
Best Practice: Opt-Out of Training, Avoid Inputting Personally Identifiable or confidential information
- Enterprise Data Protection (Copilot Chat, Copilot M365)
- Misinformation (deep fakes, fake news, financial fraud)
Best Practice: Content verification

Copyright & Adversarial Use

- Copyright and Plagiarism
Best Practice: Prefer services that assume legal responsibility for any claims (e.g., Microsoft)
- The legal area is still trying to figure out the specifics of copyright laws related to generative AI. Currently, there are ongoing lawsuits, and some rulings have leaned towards considering content generated by AI as fair use. However, these rulings are being appealed, and the final decision is yet to be made by higher courts.

Ciberamenazas potenciadas por IA

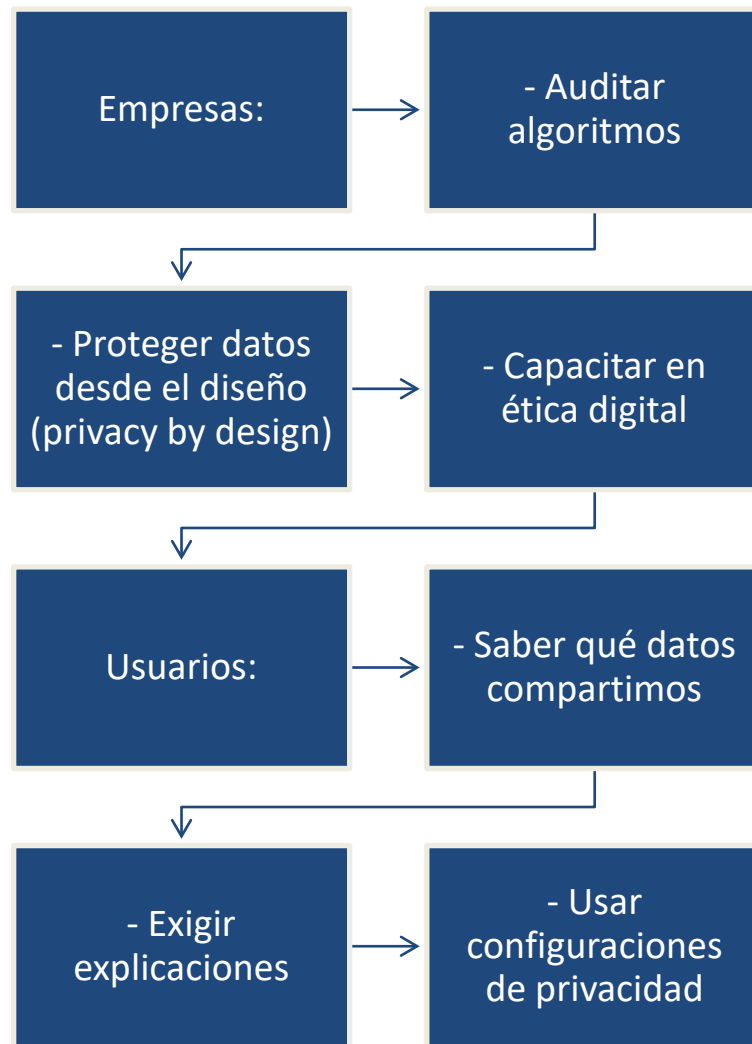
- - Phishing inteligente
 - - Deepfakes que suplantan identidad
 - - Automatización de ataques cibernéticos
-
- - Detección de fraudes
 - - Monitorización de amenazas
 - - Respuestas automáticas ante incidentes



¿Quién controla la IA?

- Regulaciones existentes:
 - - GDPR (UE)
 - - Ley de IA de la UE
- Vacíos legales aún en muchos países.
- Responsabilidad corporativa:
 - - Crear comités éticos
 - - Aplicar auditorías internas
 - - Establecer límites claros

Buenas prácticas



Reflexión final



Gracias por su
atención!



[LinkedIn | Emilia Bertomeu](#)

