UNIVERSIDAD ORT Uruguay
Facultad de Ingeniería
Ing. Bernard Wand-Polak

Desafíos de la Inteligencia Artificial como servicio

Explicabilidad y Privacidad

Eduardo Mangarelli
mangarelli@ort.edu.uy

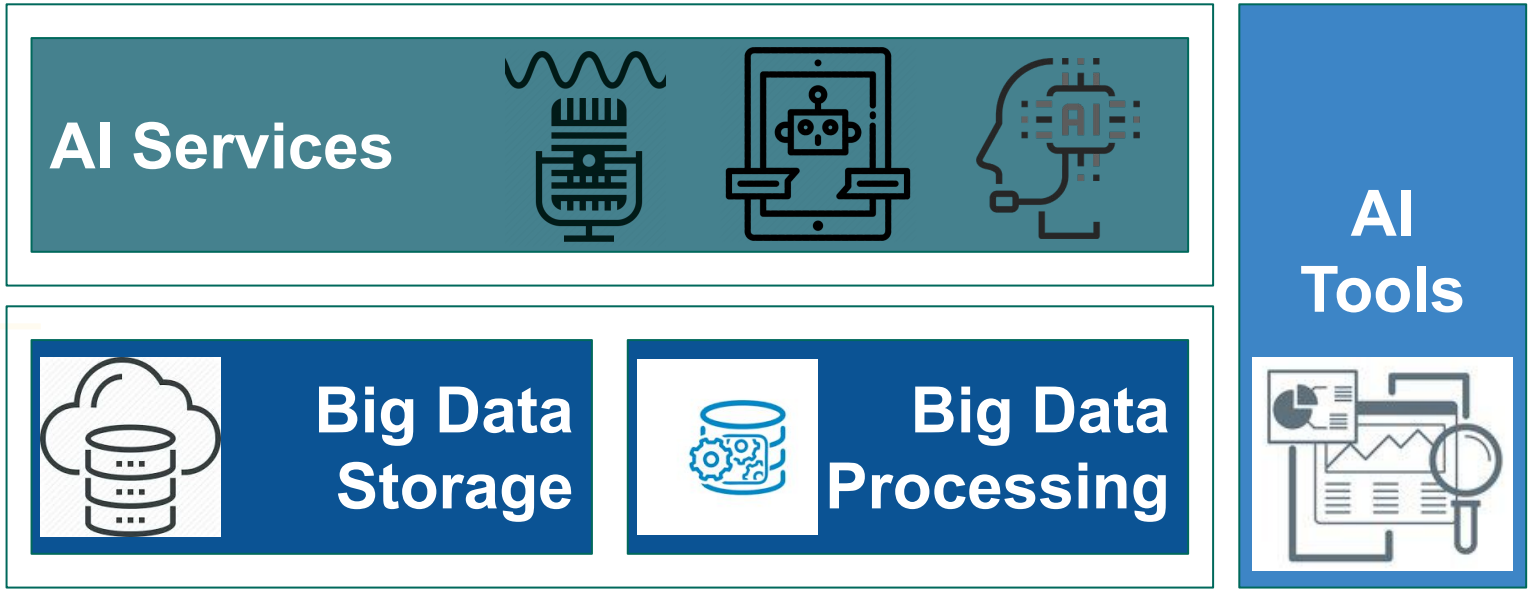
Sergio Yovine
yovine@ort.edu.uy

IA@ORT

- Grupo de investigación en IA
- Master en Big Data - https://fi.ort.edu.uy/master-en-big-data
  - Dip. Esp. en Analítica de Big Data (desde 2017)
  - Dip. Esp. en Inteligencia Artificial
- Más de 40 graduados (agosto 2019)
- Vinculación con empresas
- Cuerpo docente con académicos y profesionales
- Plataforma cloud de IA propia

Cloud computing

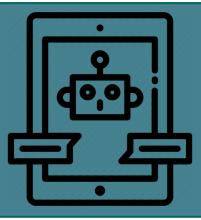
AIaaS = (I + P + S)aaS

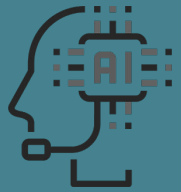


Cloud computing - Desafíos

Exposición de datos y modelos

AI Services



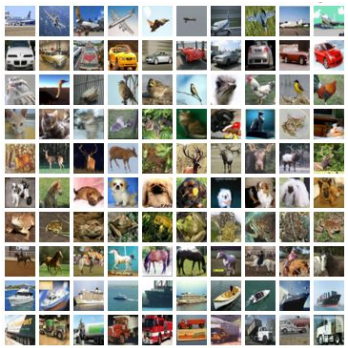


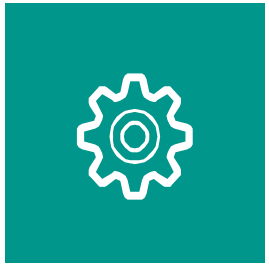
AI Tools

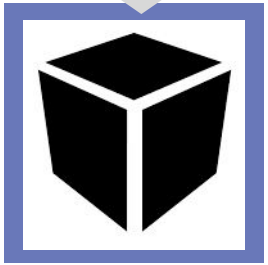
Big Data Storage

Big Data Processing

Proceso



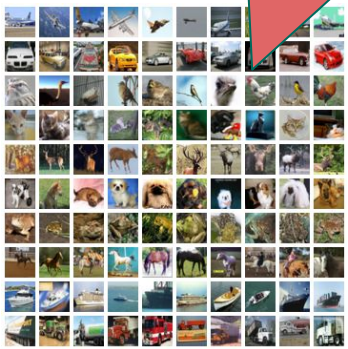




This is a Panda (p = .58)

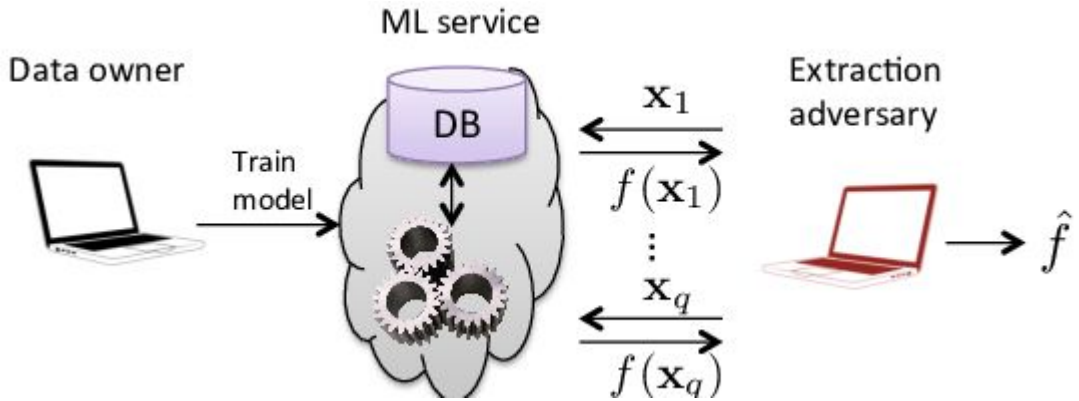
Desafío

¿Mi foto está segura?!



This is a Panda (p = .58)

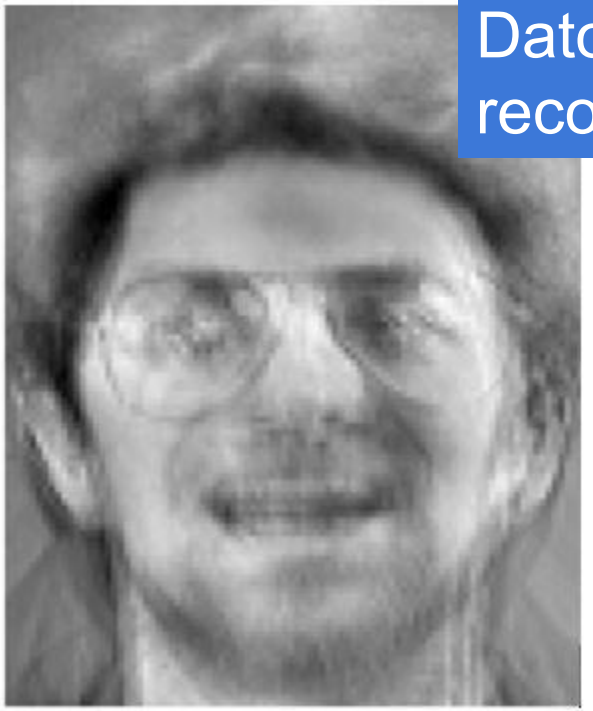
Ataques a la privacidad



Extraer información sobre los datos de entrenamiento

Ataques a la privacidad

Dato de entrenamiento



Dato reconstruido

Privacidad - Soluciones

- Privacidad diferencial en el entrenamiento
  - Proteger los datos de entrenamiento

- Generación de datos sintéticos privatizados
  - Publicar datos con valor predictivo
  - Proteger los datos reales

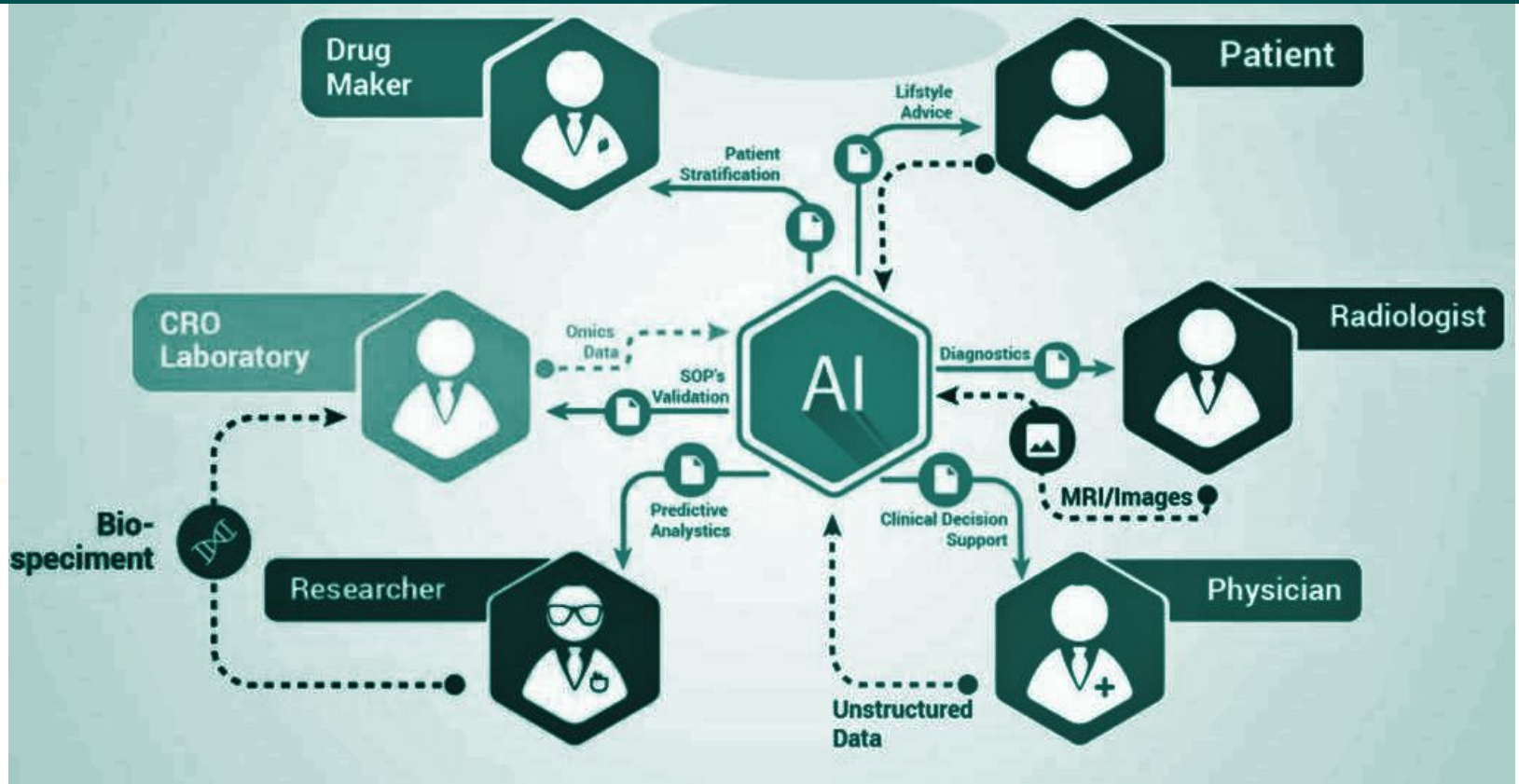
ANII

UNIVERSIDAD ORT Uruguay

ICT4V
Information and Communication Technologies for Verticals

agesic

Aplicación

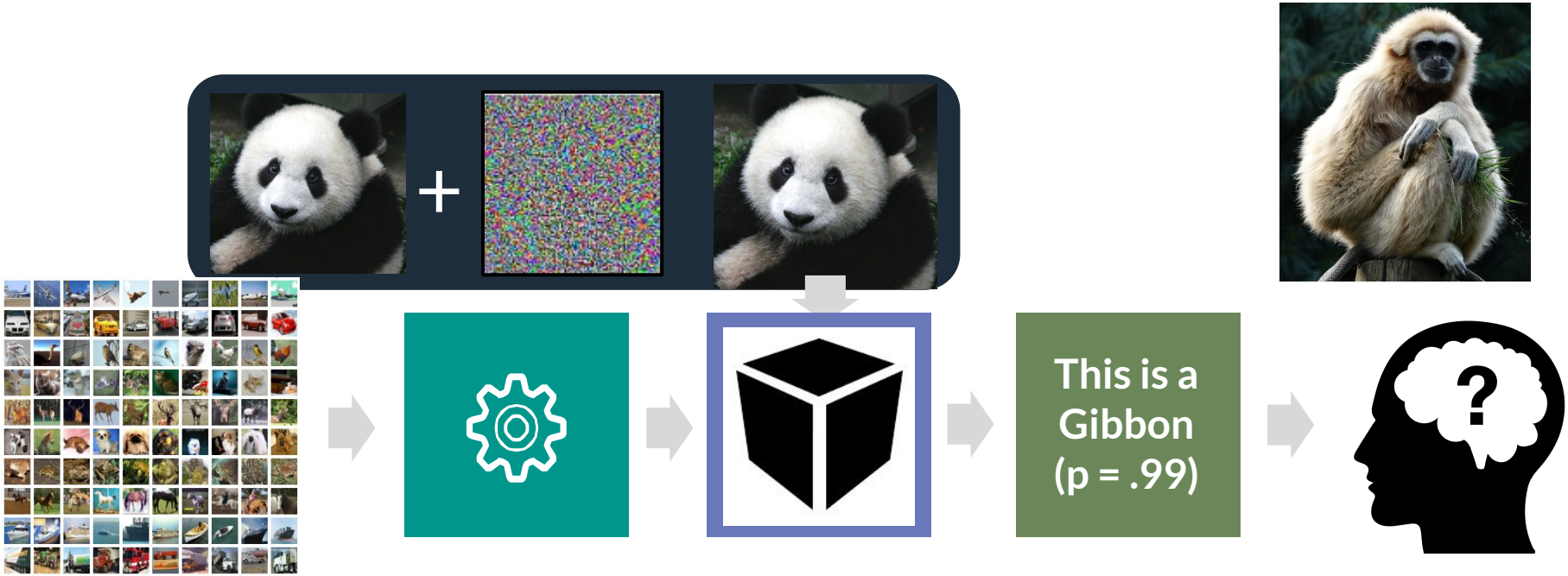

Drug Maker
Patient
Lifstyle Advice
Patient Stratification
CRO Laboratory
Omics Data
SOP's Validation
AI
Diagnostics
Radiologist
MRI/Images
Predictive Analystics
Clinical Decision Support
Bio-speciment
Researcher
Physician
Unstructured Data

Aplicación - Desafíos

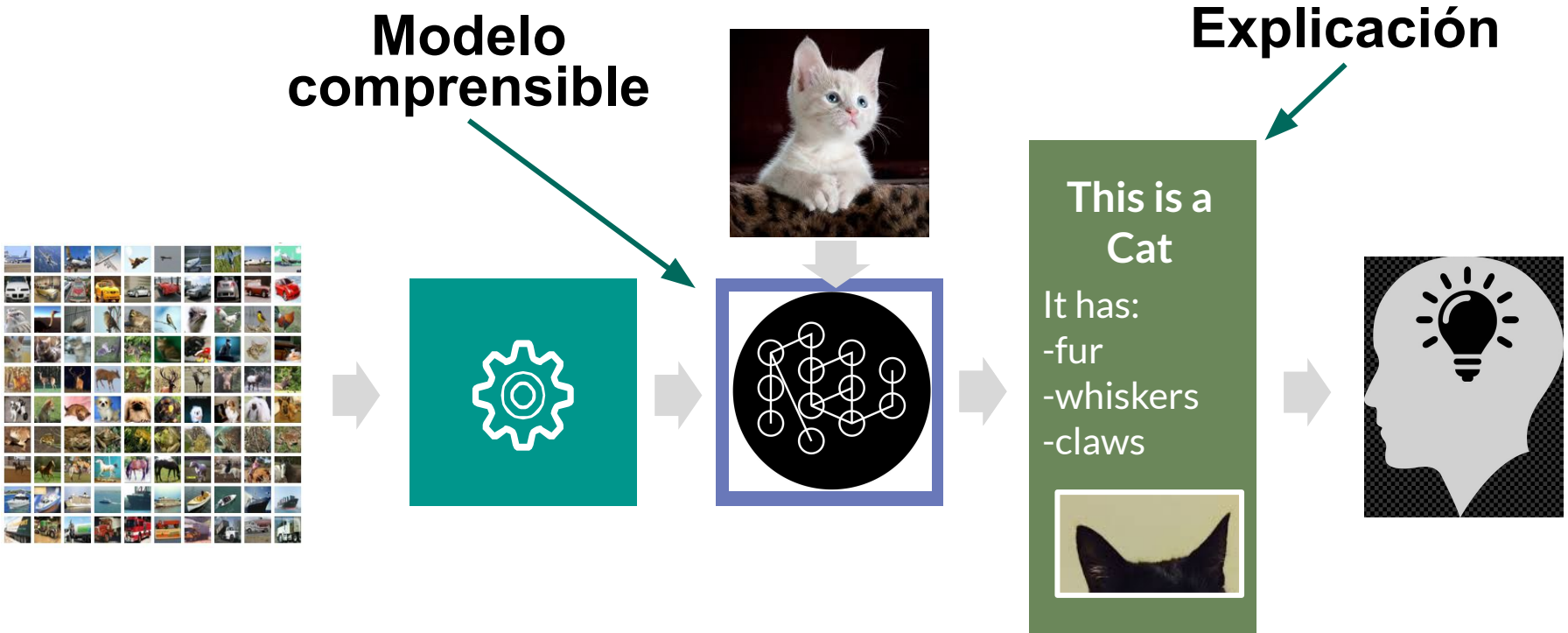
Exposición de datos y modelos

Interpretabilidad de los resultados

Desafíos



Explicabilidad



Soluciones para la explicabilidad

- Modelos interpretables
  - Bajo poder predictivo
- Explicar los modelos
  - Generar una derivación
  - Caja blanca
- Inducir un modelo interpretable
  - Aprendizaje activo (Q&A)
  - Caja negra

ICT4V
Information and Communication Technologies for Verticals

UNIVERSIDAD ORT Uruguay

AlaaS - Conclusiones

- Desafíos
  - Privacidad de los datos
  - Explicabilidad / Interpretabilidad / Verificación
- Proyectos en curso para abordarlos