IA aplicada a la prevención del crimen financiero

Julio Monseco – Director Global Servicios Profesionales

21 de abril de 2026

Evolución del fraude financiero:

“IA, Mitos y realidad en la prevención del fraude transaccional”

Agenda

1.
Conceptos de IA

2.
Herramientas de monitoreo transaccional para fraude

3.
Herramientas de monitoreo transaccional para AML

Lynx

Términos en
Inteligencia artificial

Lynx

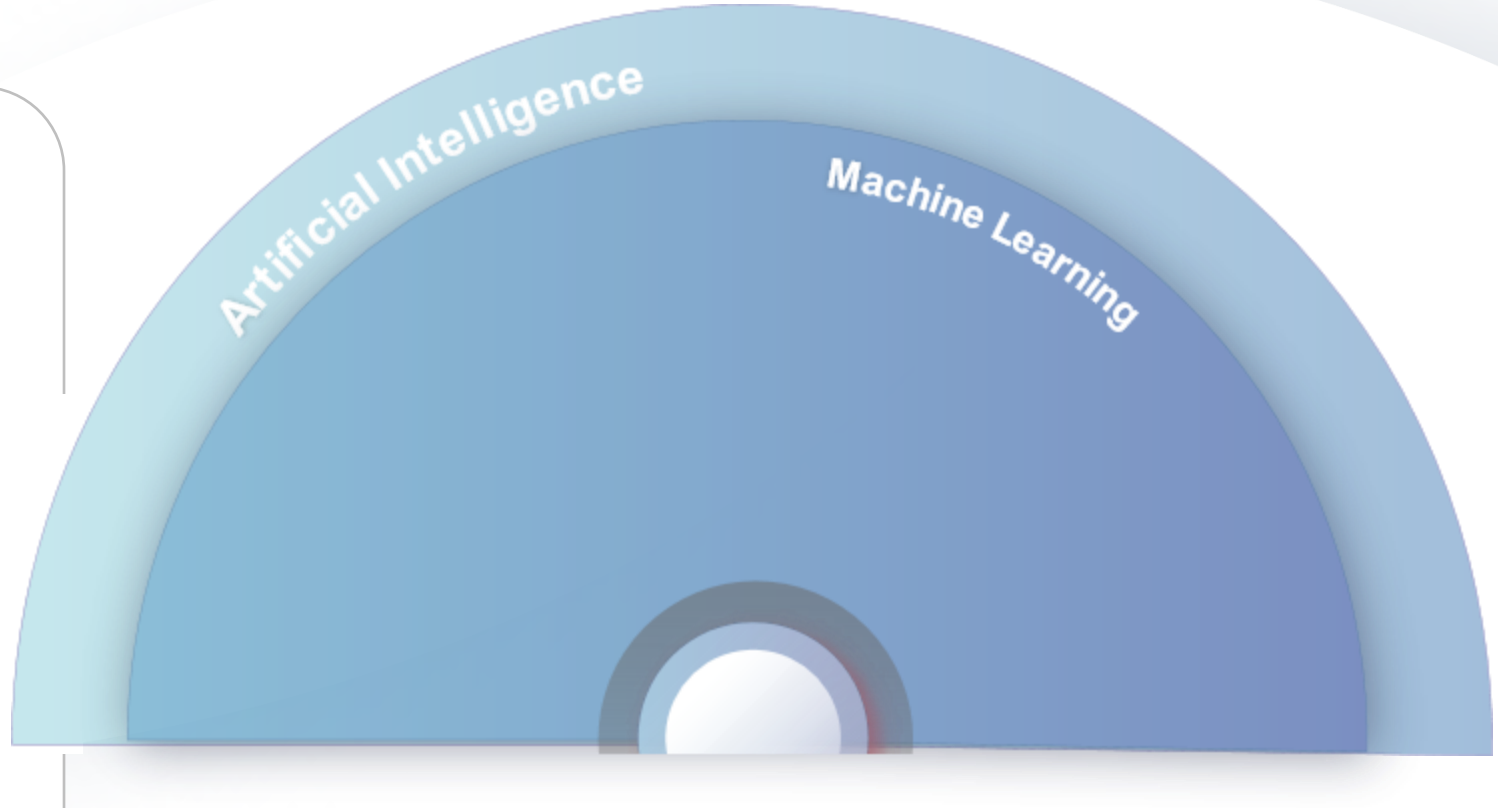
Términos en **Inteligencia artificial**

Artificial Intelligence (AI)

Lynx

Términos en **Inteligencia artificial**

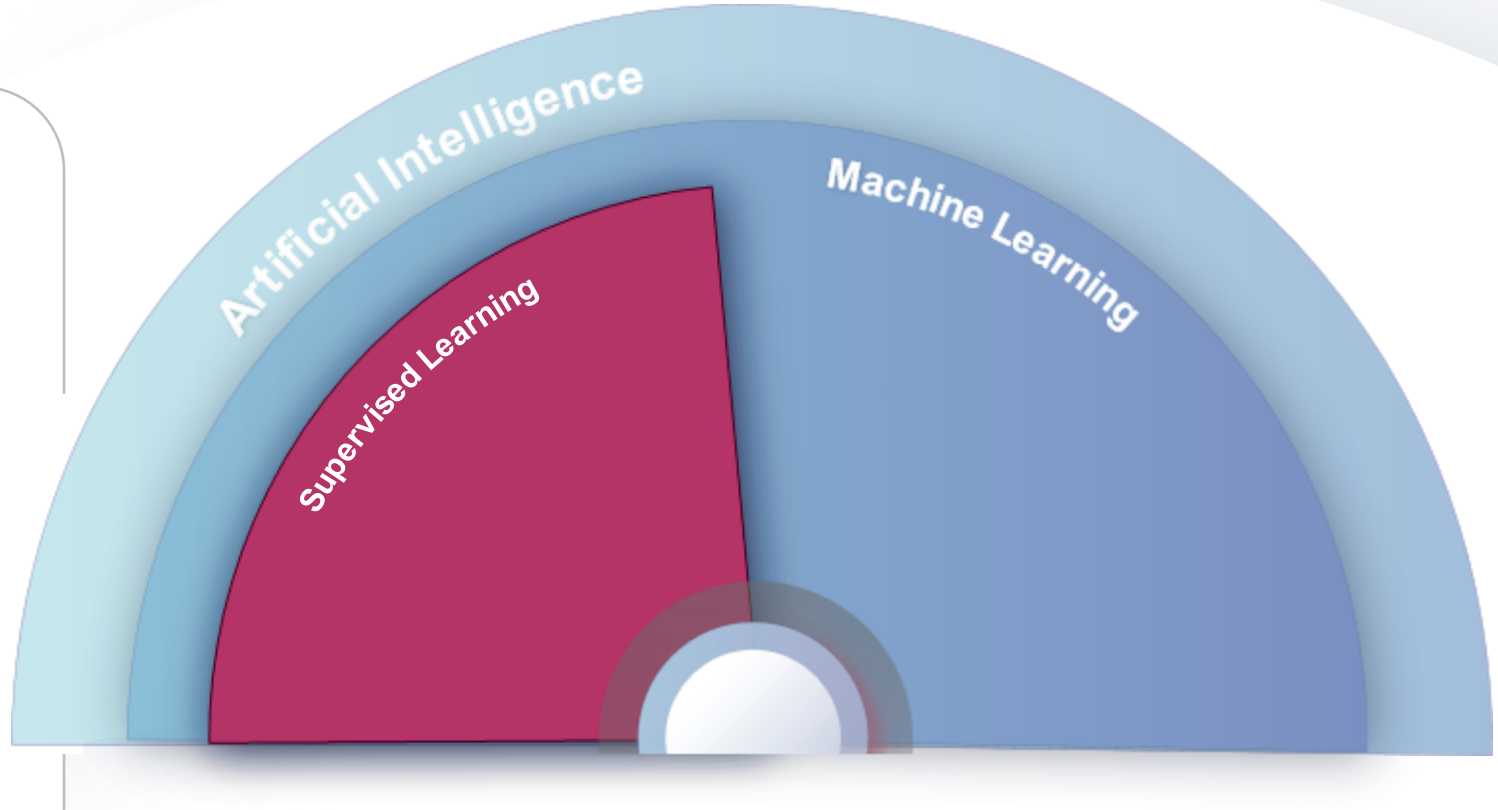
- Artificial Intelligence (AI)
  - Machine Learning (ML)



Lynx

Términos en **Inteligencia artificial**

- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**

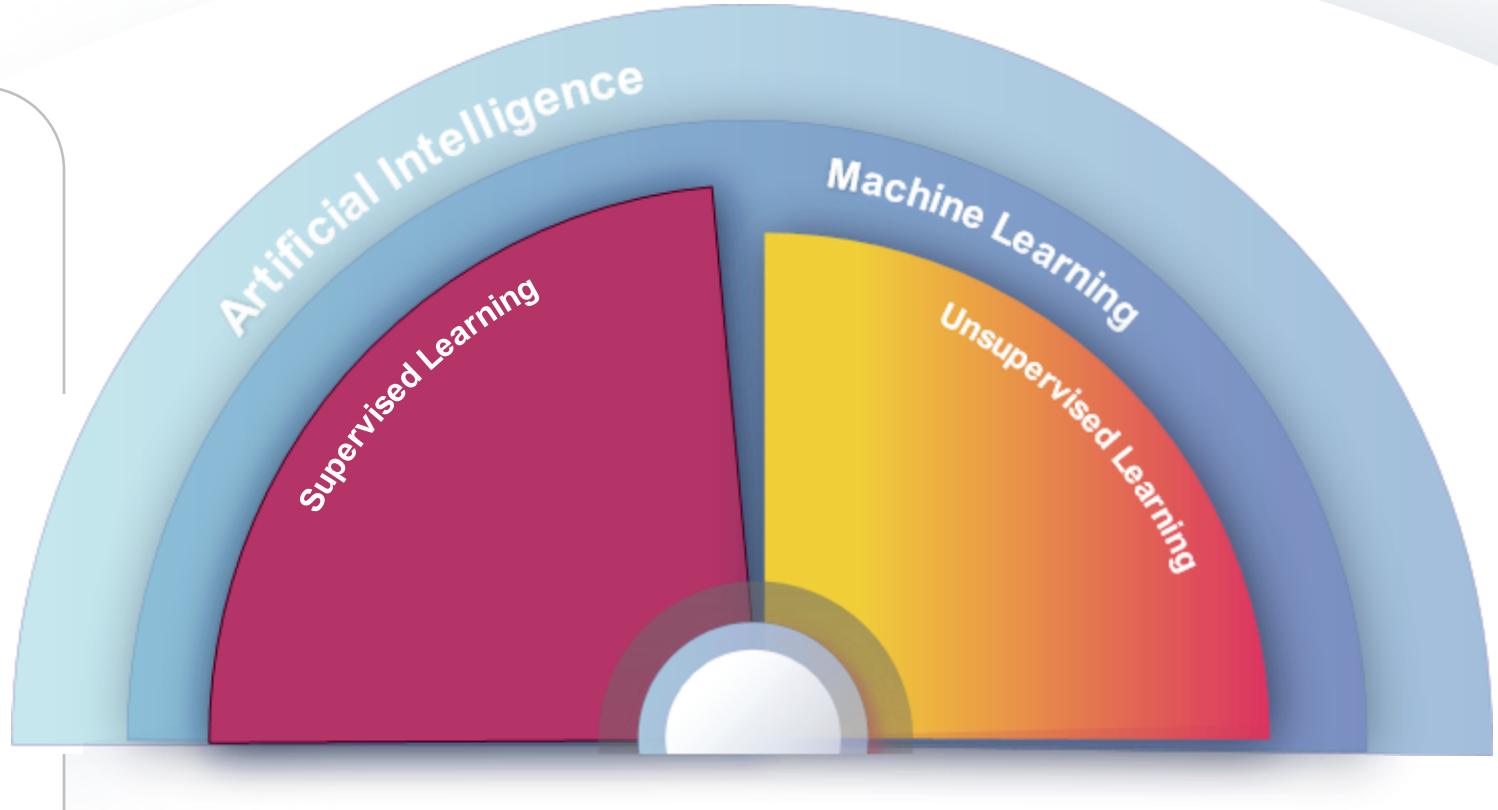


Lynx

Términos en **Inteligencia artificial**

Artificial Intelligence (AI)

- Machine Learning (ML)
  - **Supervised Learning**
  - **Unsupervised Learning**

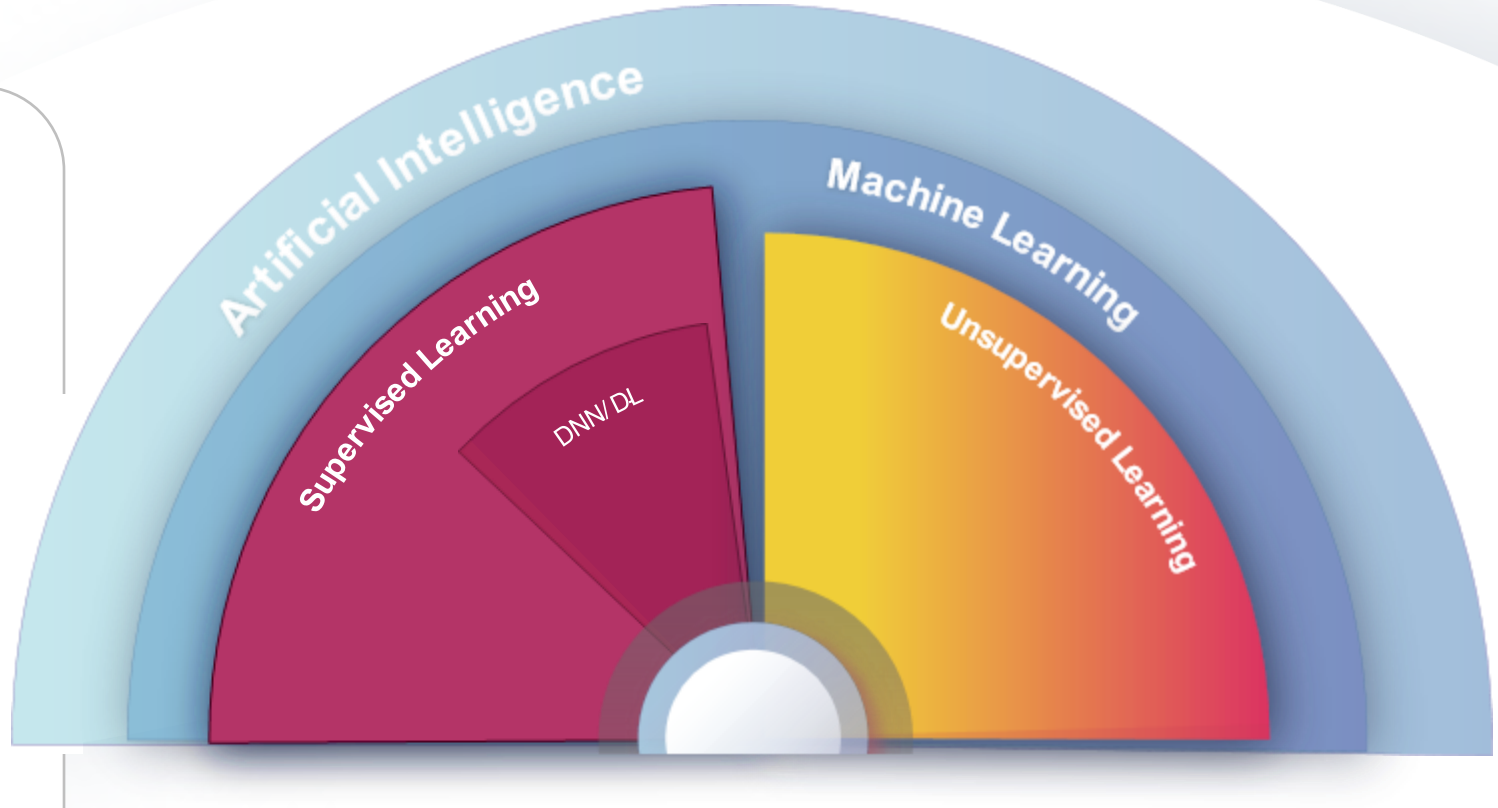


Lynx

Términos en
Inteligencia artificial

Artificial Intelligence (AI)

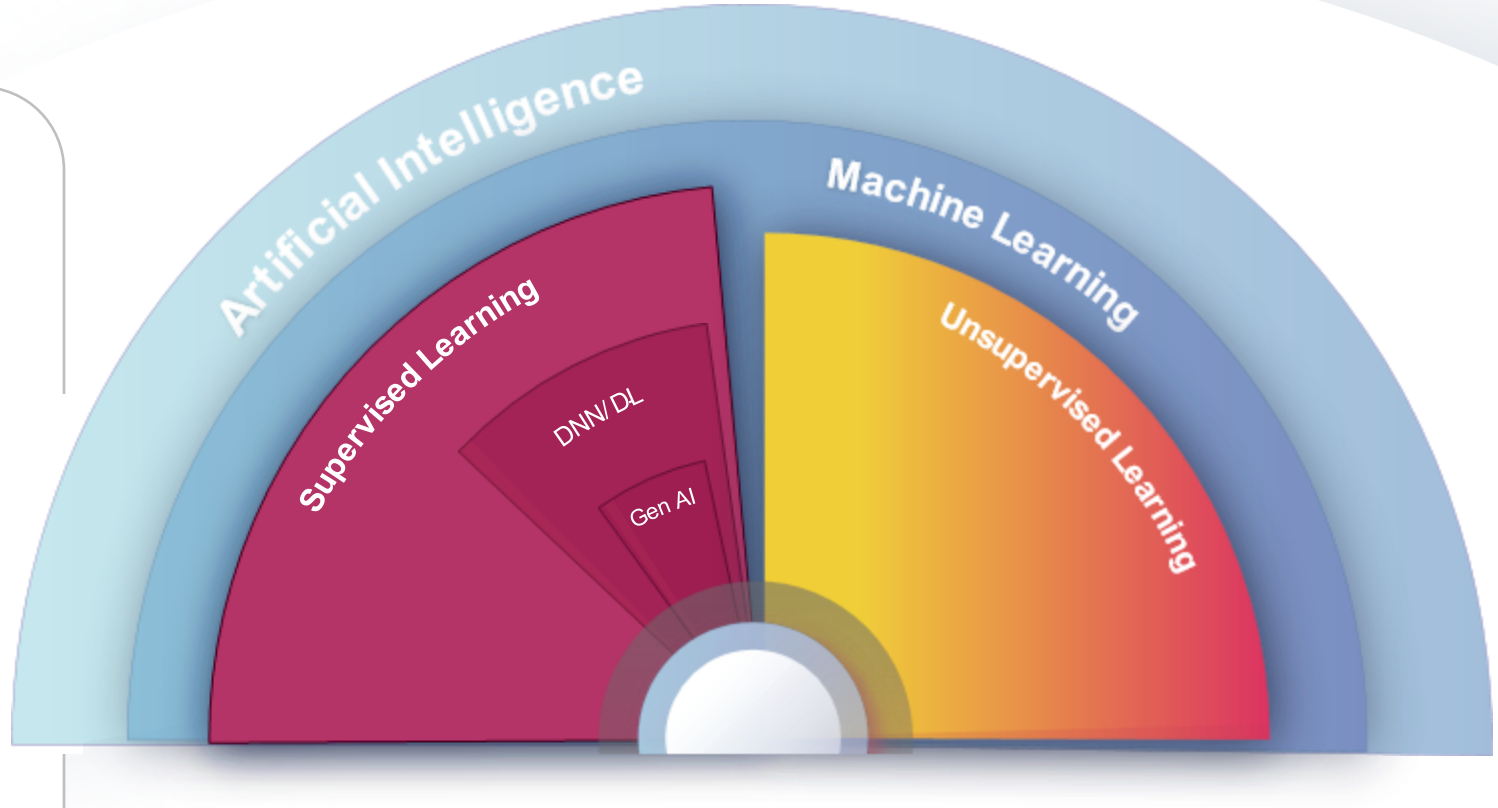
- Machine Learning (ML)
  - **Supervised Learning**
    - Deep Neural Networks / Deep Learning (DNN/DL)
  - **Unsupervised Learning**



Lynx

Términos en **Inteligencia artificial**

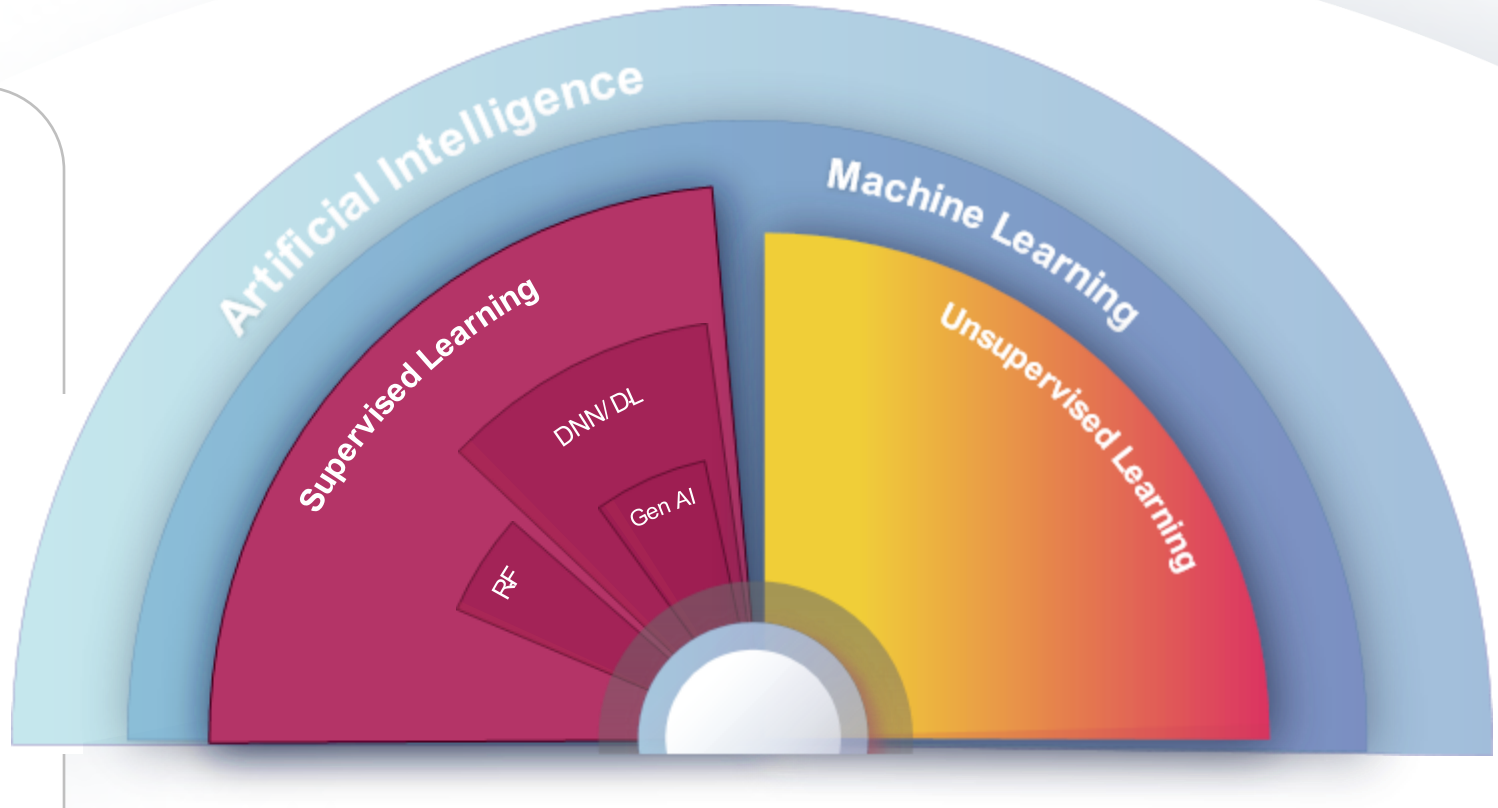
- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
    - → **Unsupervised Learning**



Lynx

Términos en **Inteligencia artificial**

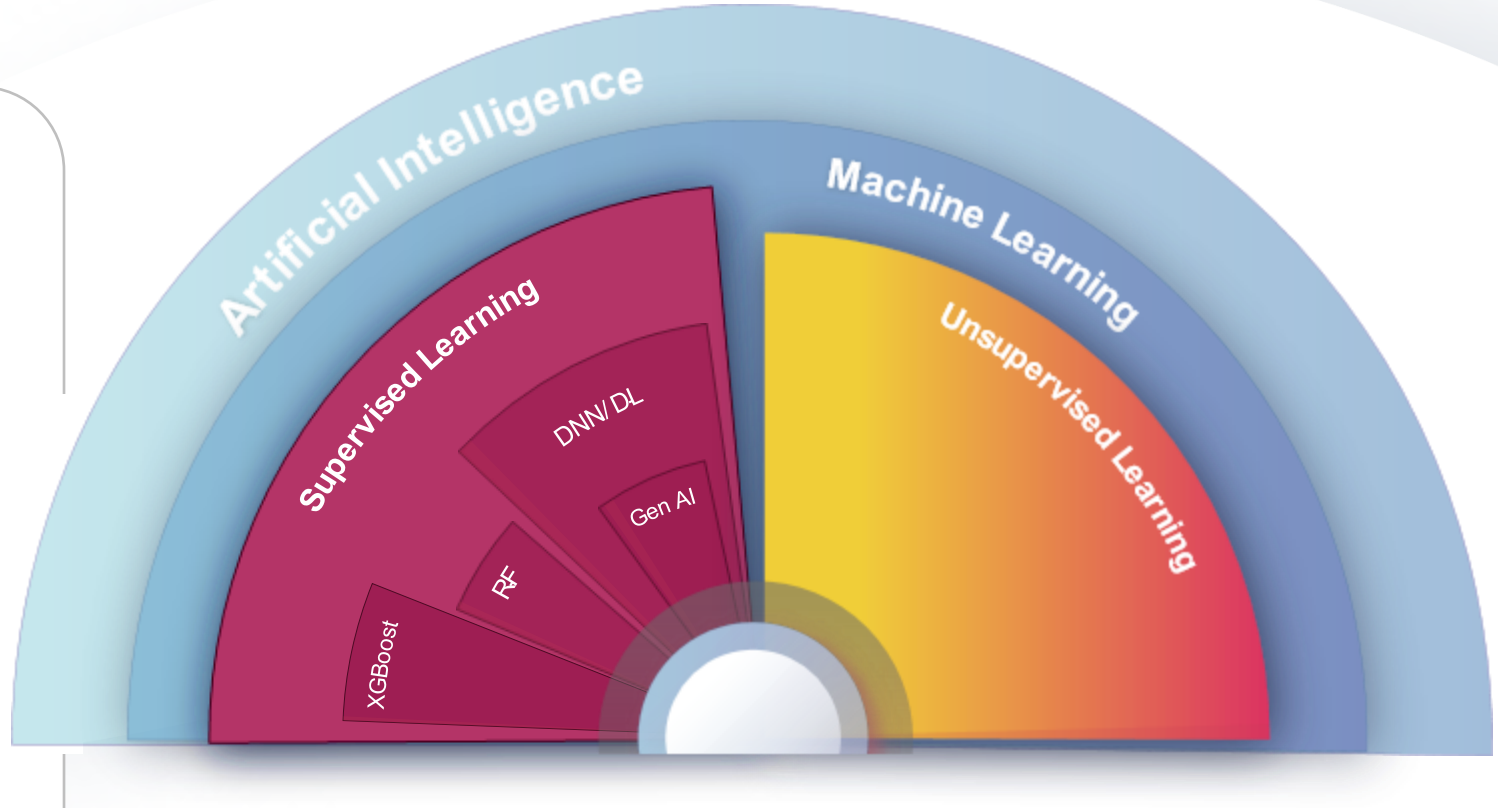
- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
      - » Random Forest (RF)
    - → **Unsupervised Learning**



Lynx

Términos en **Inteligencia artificial**

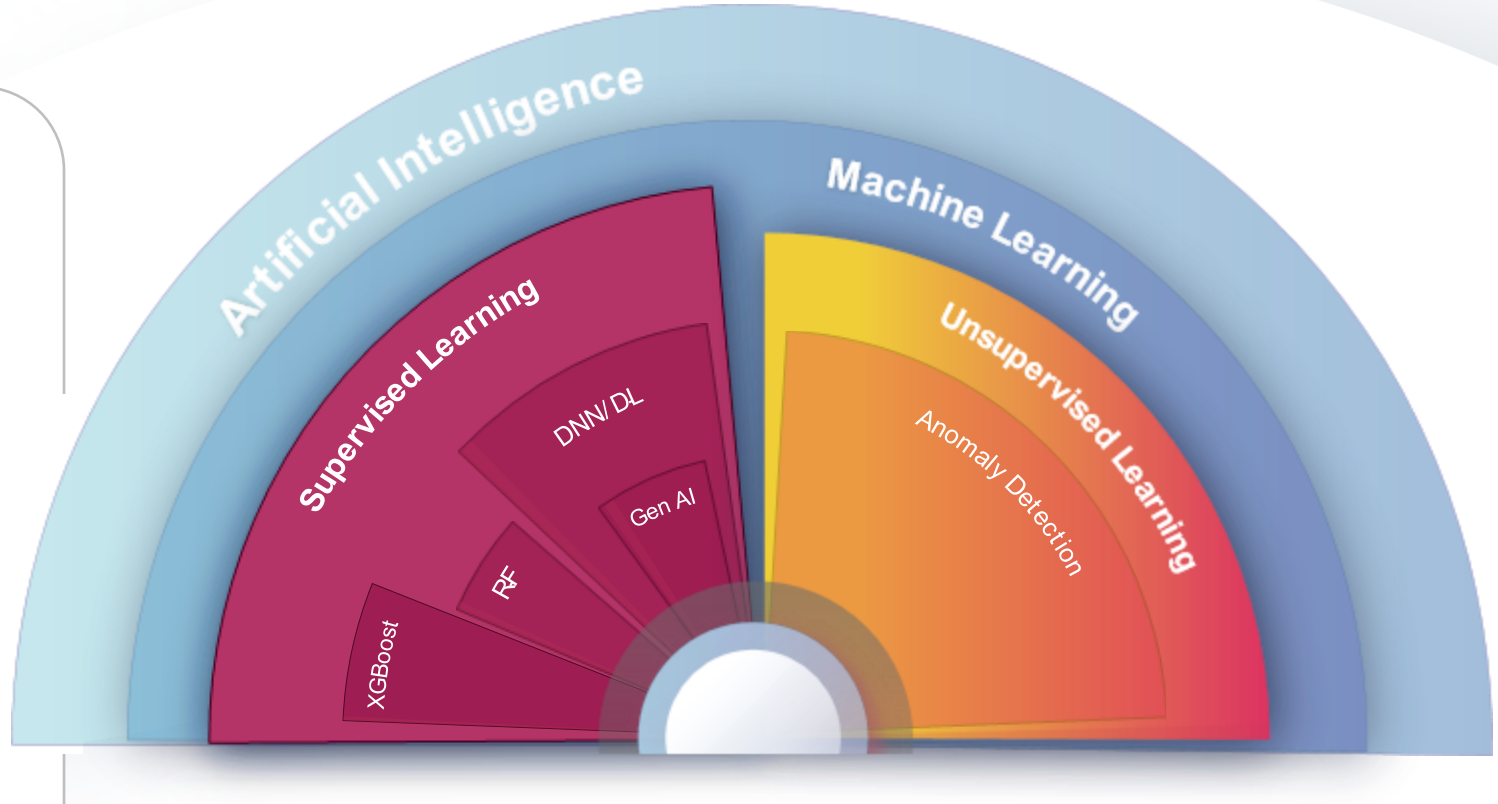
- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
      - » Random Forest (RF)
      - » XGBoost
    - → **Unsupervised Learning**



Lynx

Términos en **Inteligencia artificial**

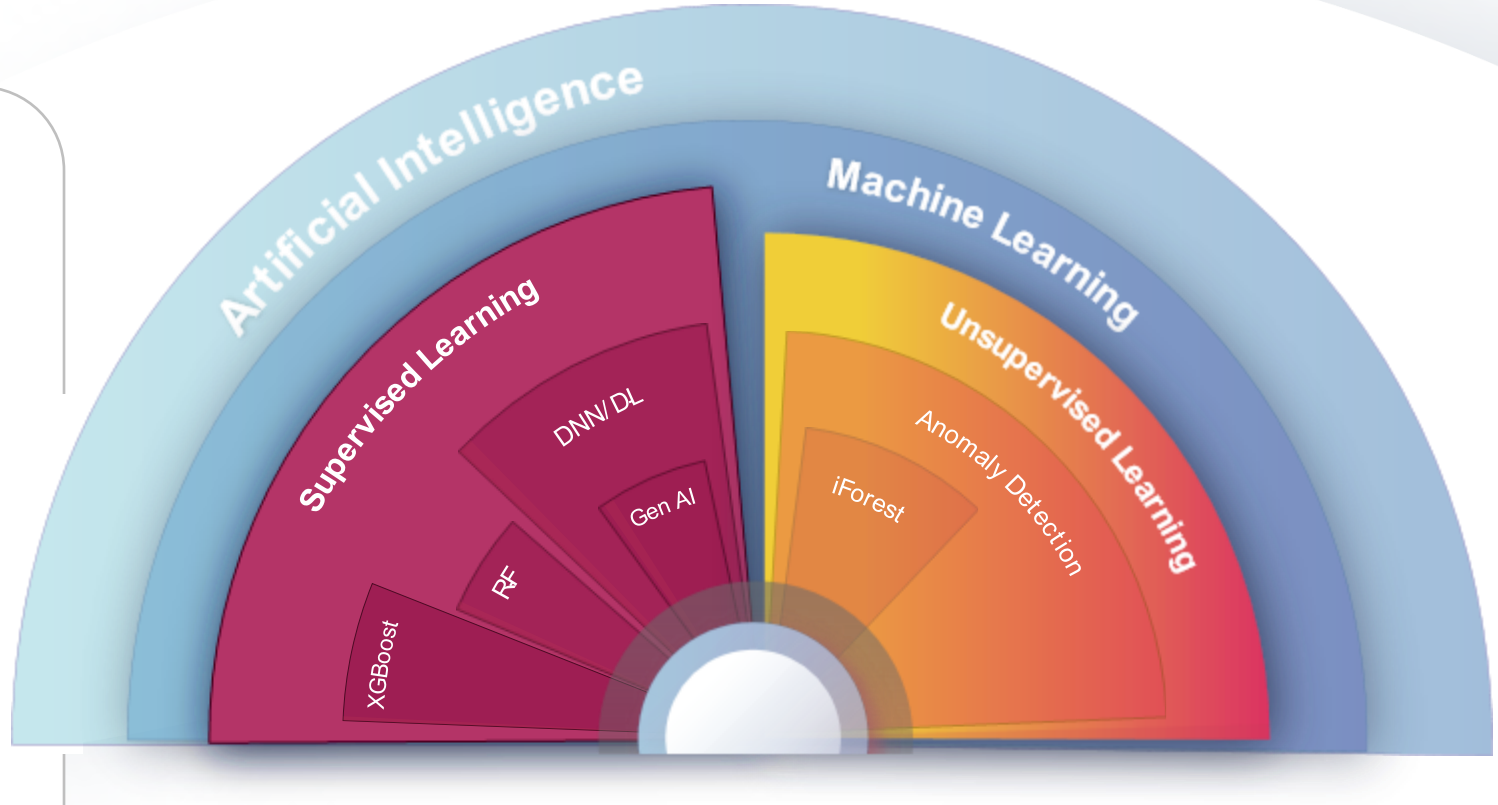
- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
      - » Random Forest (RF)
      - » XGBoost
    - → **Unsupervised Learning**
      - » Anomaly Detection



Lynx

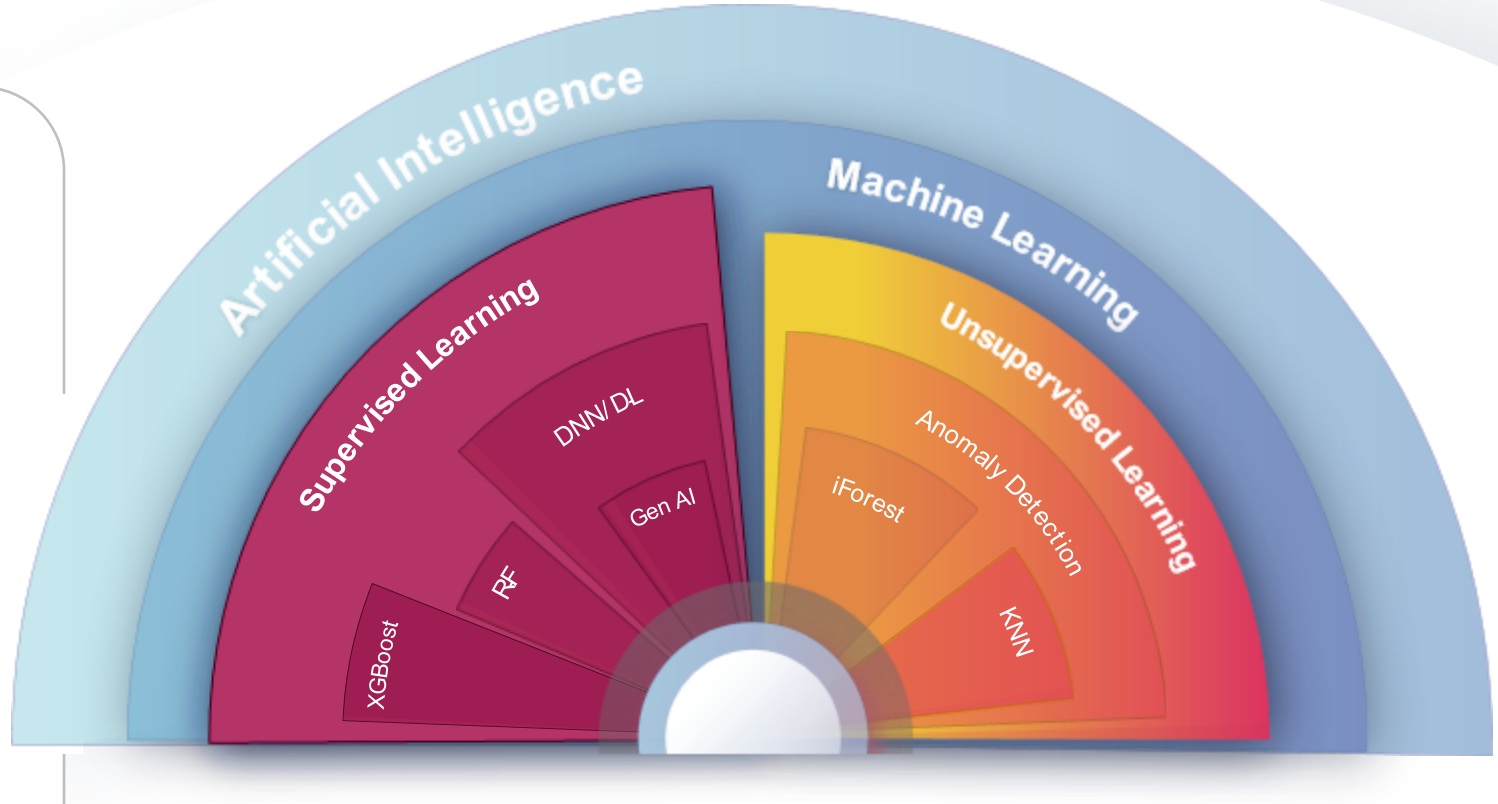
Términos en **Inteligencia artificial**

- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
      - » Random Forest (RF)
      - » XGBoost
    - → **Unsupervised Learning**
      - » Anomaly Detection
        - iForest



Términos en
Inteligencia artificial

- Artificial Intelligence (AI)
  - ↘ Machine Learning (ML)
    - → **Supervised Learning**
      - » Deep Neural Networks / Deep Learning (DNN/DL)
        - Generative AI (Gen AI)
      - » Random Forest (RF)
      - » XGBoost
    - → **Unsupervised Learning**
      - » Anomaly Detection
        - iForest
        - KNN



- Aprendizaje supervisado siempre superior al no supervisado
- **NFL -** *No free Lunch* theorem

Problemas y **soluciones**

Prevención de fraude transaccional

Aprendizaje supervisado
(XGBoost)

Biometría de comportamiento

Aprendizaje supervisado
(XGBoost)

Fraude/AML cuentas mula (análisis de flujos)

Aprendizaje supervisado
(XGBoost)

Identidad, reconocimiento facial

Aprendizaje supervisado
(DNN)

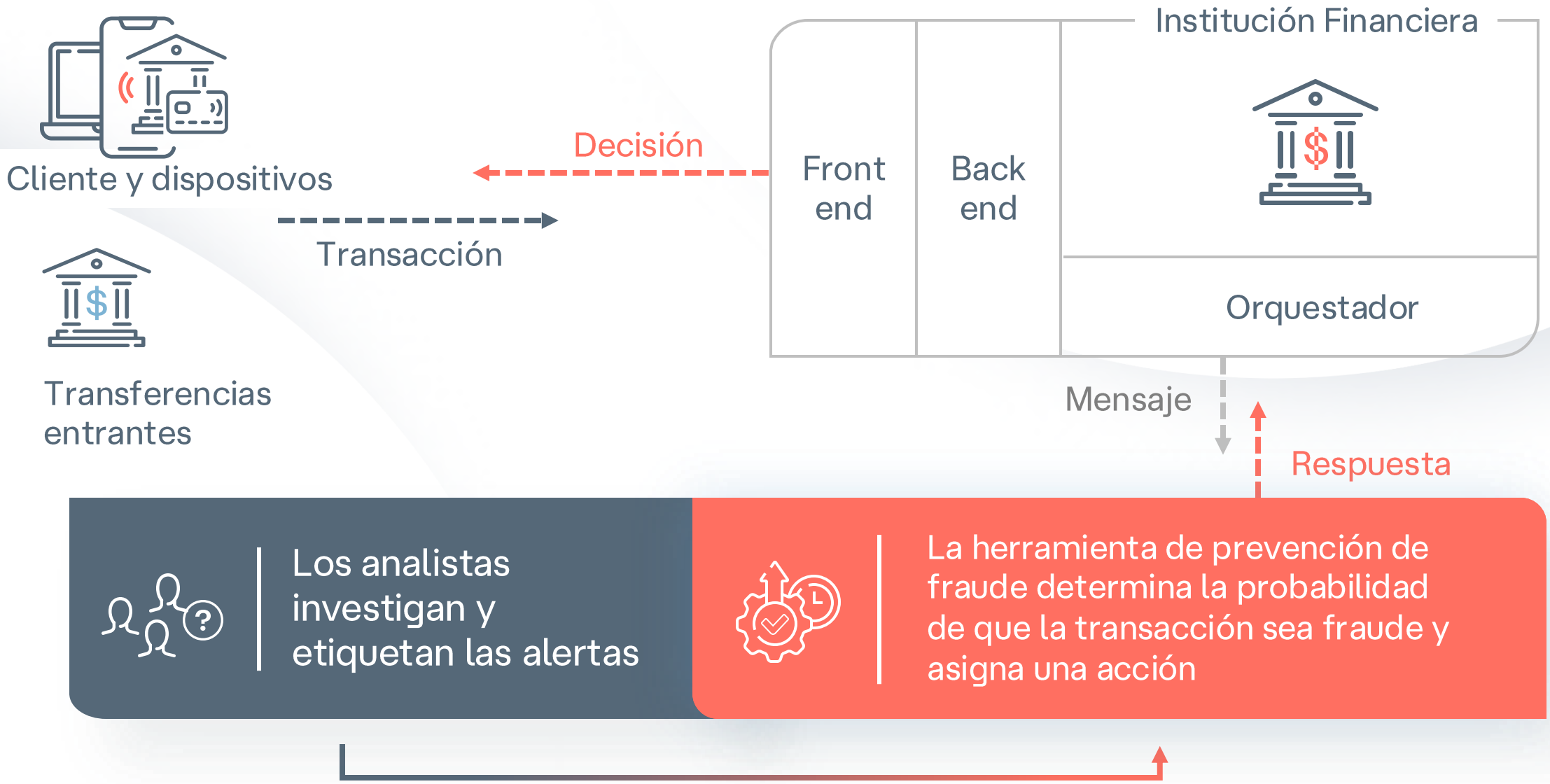
Construcción de reglas (Fraude, AML)

Aprendizaje supervisado
(ML, GenAI)

Fraude/AML cuentas mula (accesos)

Aprendizaje no supervisado
(KNN, Autoencoders, ...)

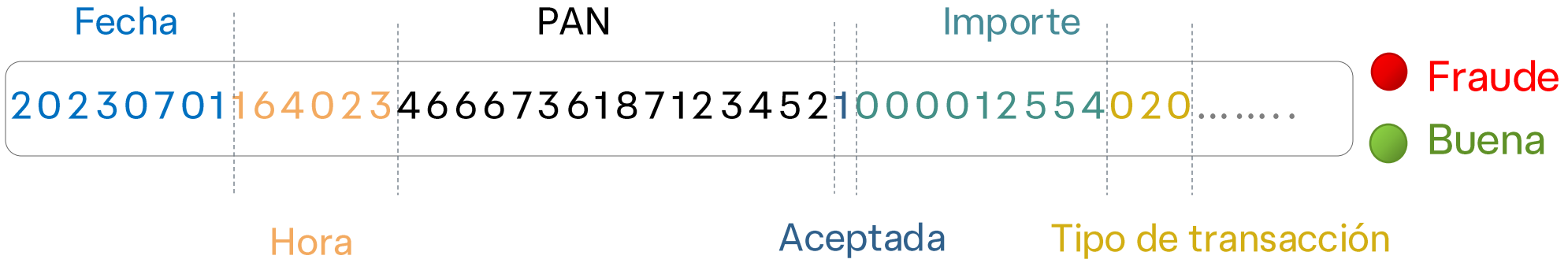
Nivel de Riesgo



Información de transacciones

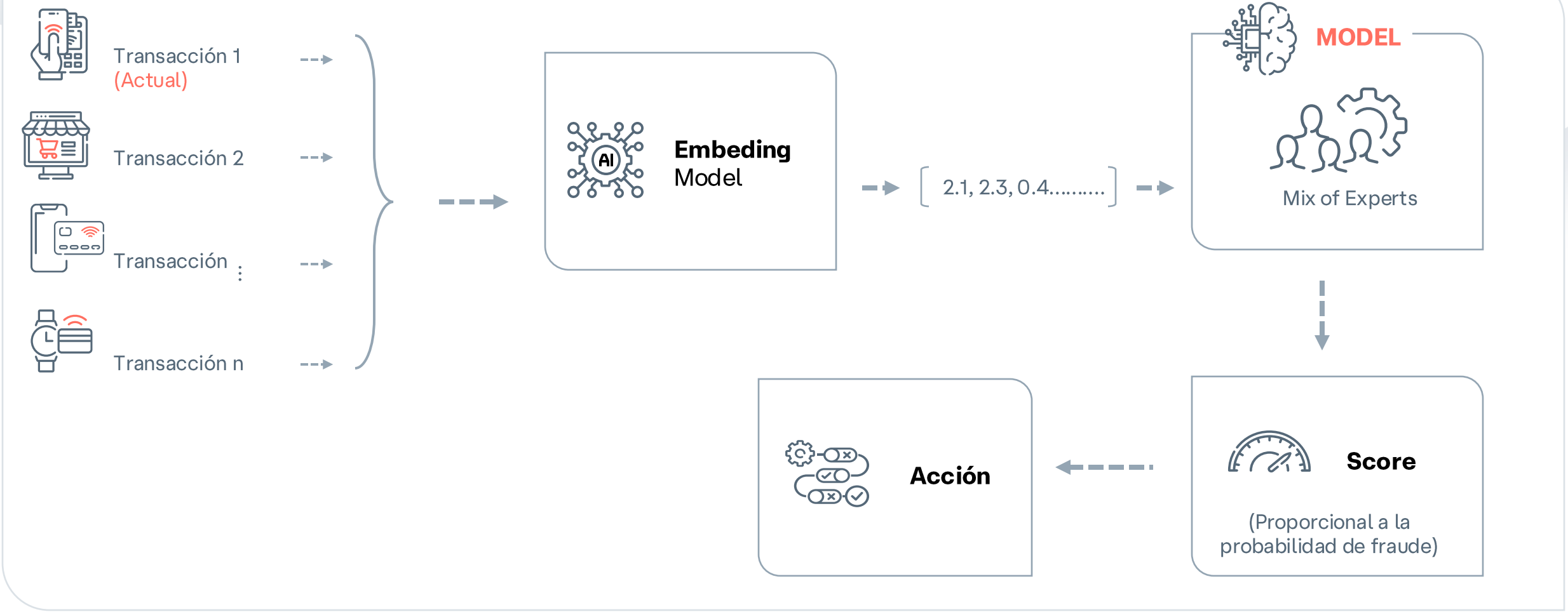
Tarjetas y transferencia con operaciones buenas y casos de fraude

Mensaje de tarjetas



Lynx

Ejecución



¿Como se define **la identidad de la una persona?**

Identidad **Biológica**

- **Identificación unívoca de la persona.**
- AND, Iris, huella dactilar, cara, ...

Identidad **Digital**

- Dispositivo que utilizamos
- Biometria de **comportamiento con los dispositivos**

Identidad **Financiera**

Tipos de operaciones y características de las operaciones financieras que realizamos

Nivel de Riesgo

Herramienta de
prevención de fraude

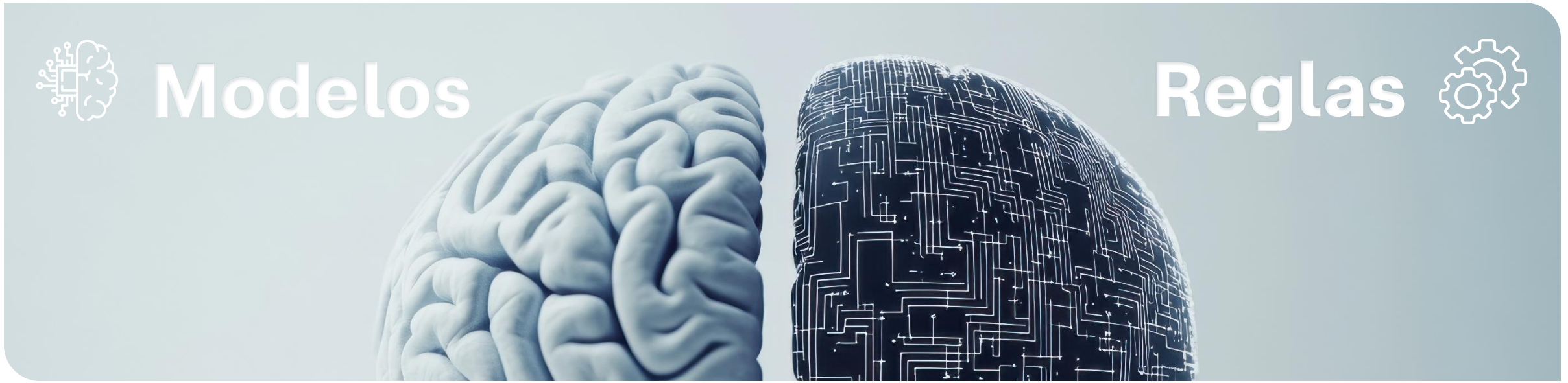
Información **transaccional**

Información **personal**

Información de **biometría de comportamiento**

Información del **dispositivo**

...

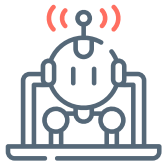


Modelos y Reglas

- Sinergia de IA y apetito por el riesgo.
- El **riesgo** preciso con un motor de decisión **configurable** dinámicamente permite respuestas **flexibles** y una **automatización** perfecta del flujo de trabajo.

Las instituciones financieras crean **capas de defensa para poder identificar, prevenir y responder a todo tipo de ataques.**

Sistemas de reglas en tiempo real. Poco eficientes en ataques complejos



Modelos de Consorcio generados con datos globales. No se ajustan al perfil de los clientes de una institución.

Modelos estáticos construidos con datos propios. Se deterioran con el tiempo y hay que reentrenarlos.

Modelos dinámicos son el último avance en Machine Learning.

Se actualizan constantemente y se ajustan a los nuevos tipos de fraude.

Aproximación Tradicional para la construcción de modelos

Estático

Las actualizaciones poco frecuentes dejan los **modelos anticuados**, incapaces de adaptarse a la evolución de las tácticas de fraude y menos eficaces con el paso del tiempo.

Recursos

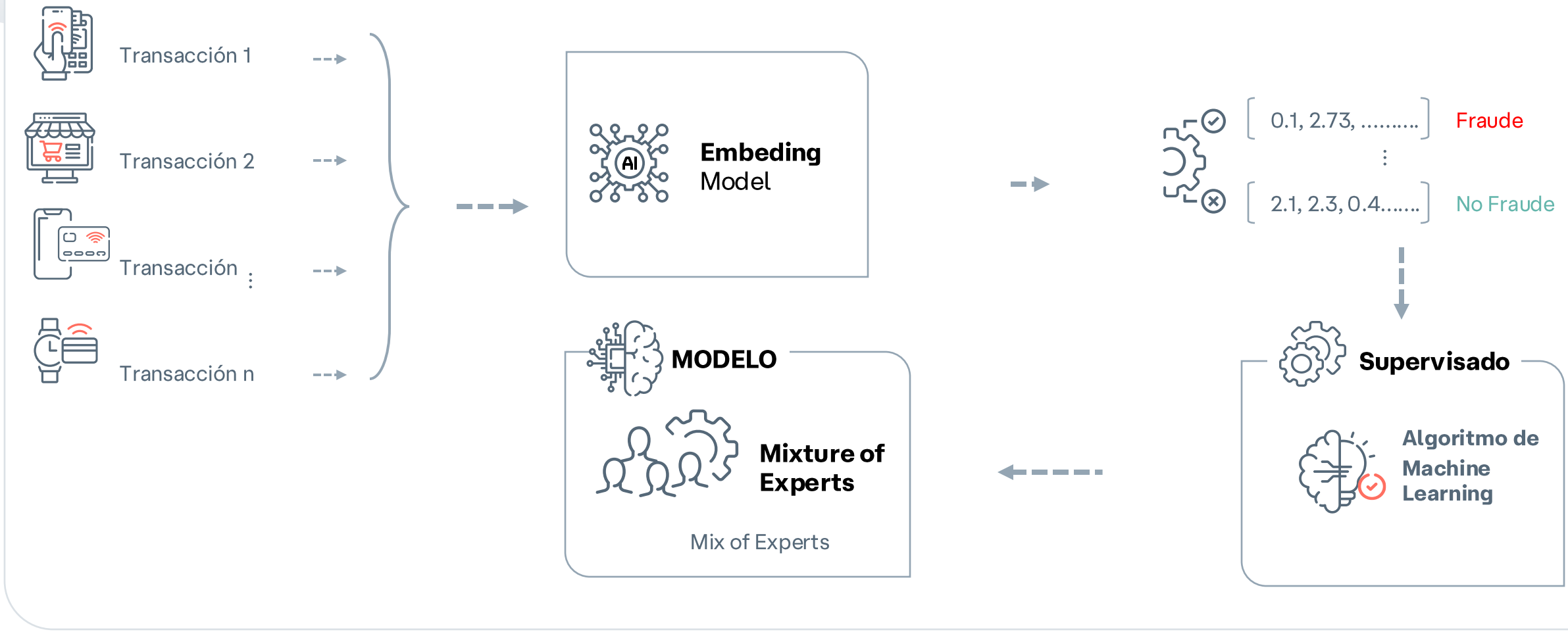
El enfoque tradicional requiere un gran esfuerzo humano, lo que **ralentiza los procesos y aumenta los costes.**

Riesgo operacional

La actualización de los modelos en producción tiene el riesgo de provocar **la inestabilidad del sistema,** por lo que el proceso lleva mucho tiempo

Lynx

Training – Información histórica



Lynx

La realidad de los **modelos estáticos**

Cambios de comportamiento

El comportamiento de los clientes evoluciona continuamente, creando nuevas pautas y tendencias.

Da lugar a **más fricción**.

Los defraudadores **se adaptan**

Los atacantes aprenden de las transacciones rechazadas y modifican sus tácticas en respuesta a las reacciones del sistema.

Da lugar a **más fraude**.

Procedimientos modernos para la construcción de modelos

Dinámico

Los modelos adaptativos diarios ofrecen actualizaciones continuas y automatizadas, lo que **garantiza que el sistema se mantiene alineado con la evolución de los datos y las tácticas de fraude**, sin intervención manual.

Eficiente

Elimina la necesidad de participación humana en el proceso de actualización y despliegue, lo que **reduce significativamente el uso de recursos y los costes asociados**

No hay riesgo operacional

Las actualizaciones diarias se producen sin interrupción del sistema ni tiempo de inactividad, lo que **aumenta la estabilidad y reduce los riesgos operativos** habituales en el reciclaje tradicional de modelos.

Problemas y **soluciones**

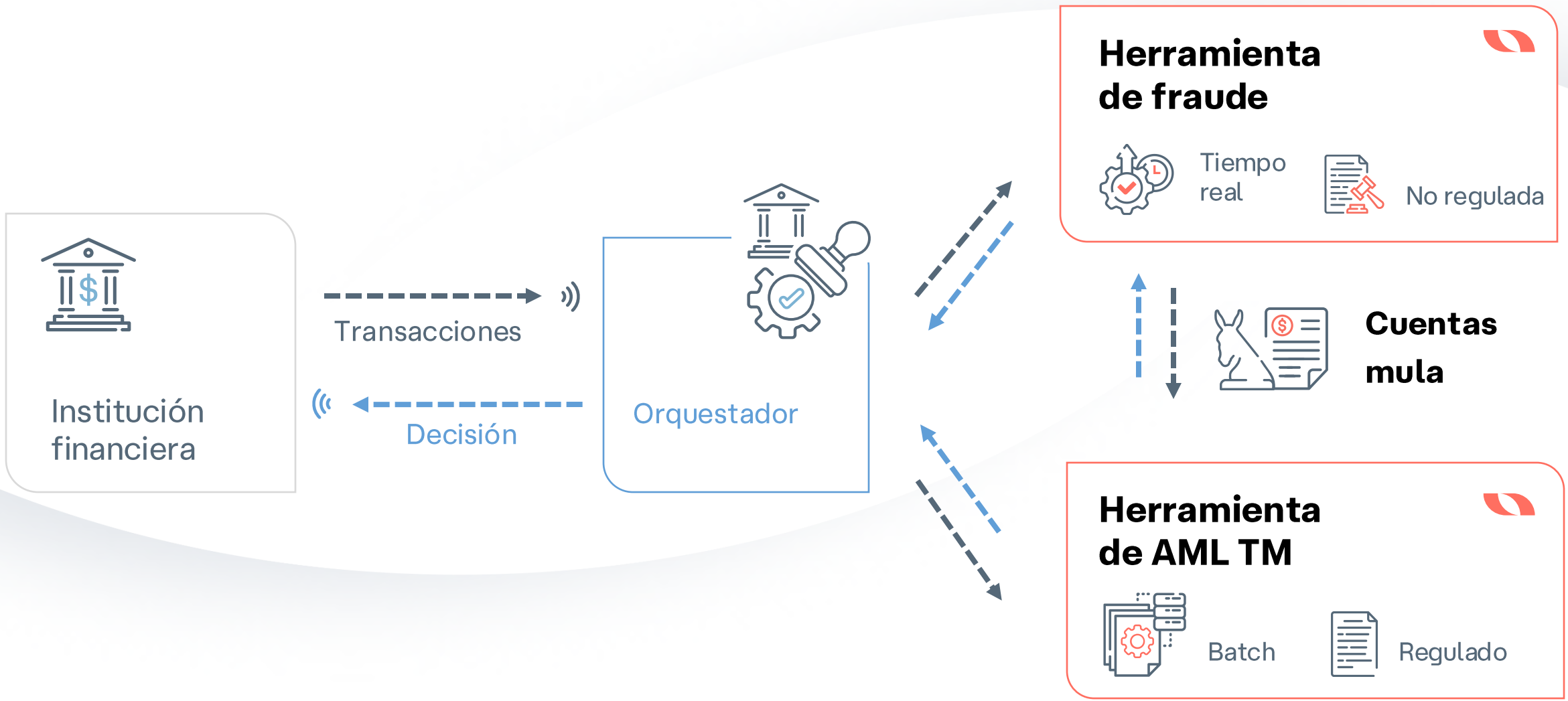
AML TM

Aprendizaje no supervisado (KNN, autoencoders, ...)

AML TM revisión de alertas

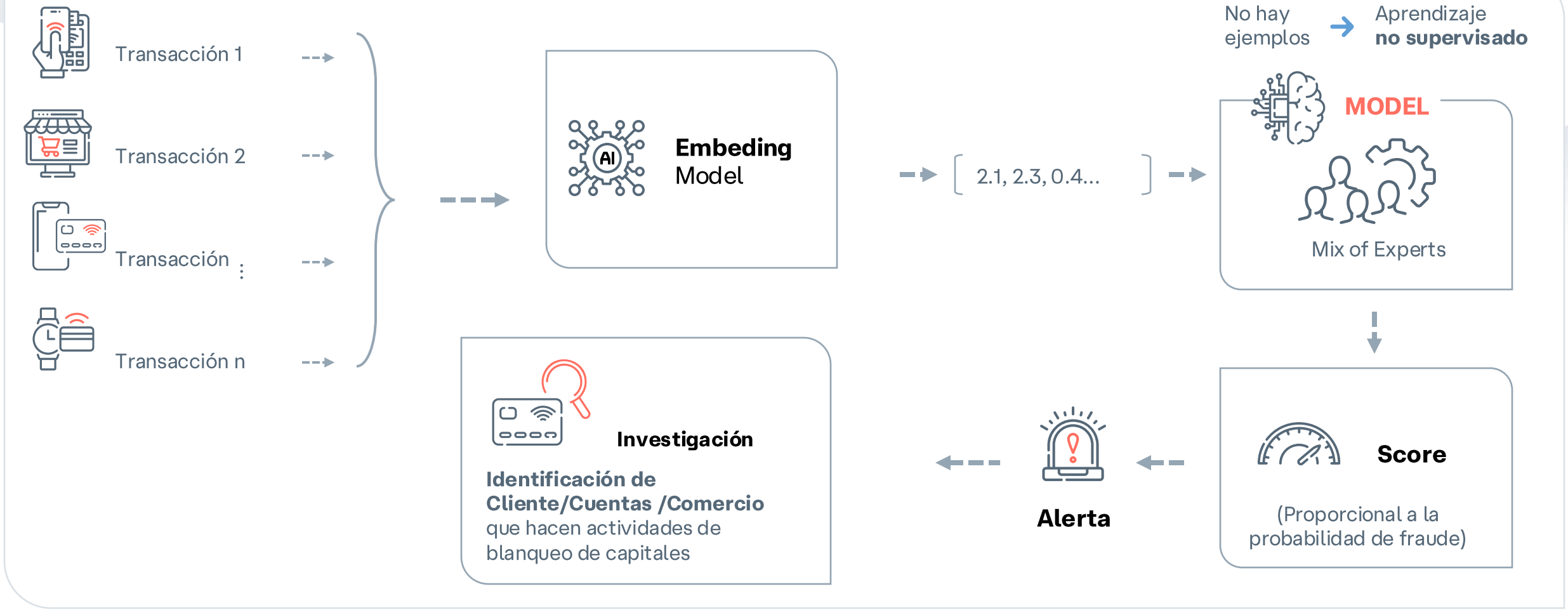
Aprendizaje supervisado (ML, GenAI)

Arquitectura de Fraude y AML TM



Lynx

AML - Transaction Monitoring (TM)

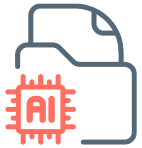


Lynx

Explicabilidad

Transparencia en los procedimientos y datos
usados para el entrenamiento de los modelos de IA.

Capacidad de un sistema de Inteligencia Artificial (IA) para **ofrecer explicaciones claras y comprensibles** sobre cómo llegó a una decisión o predicción.

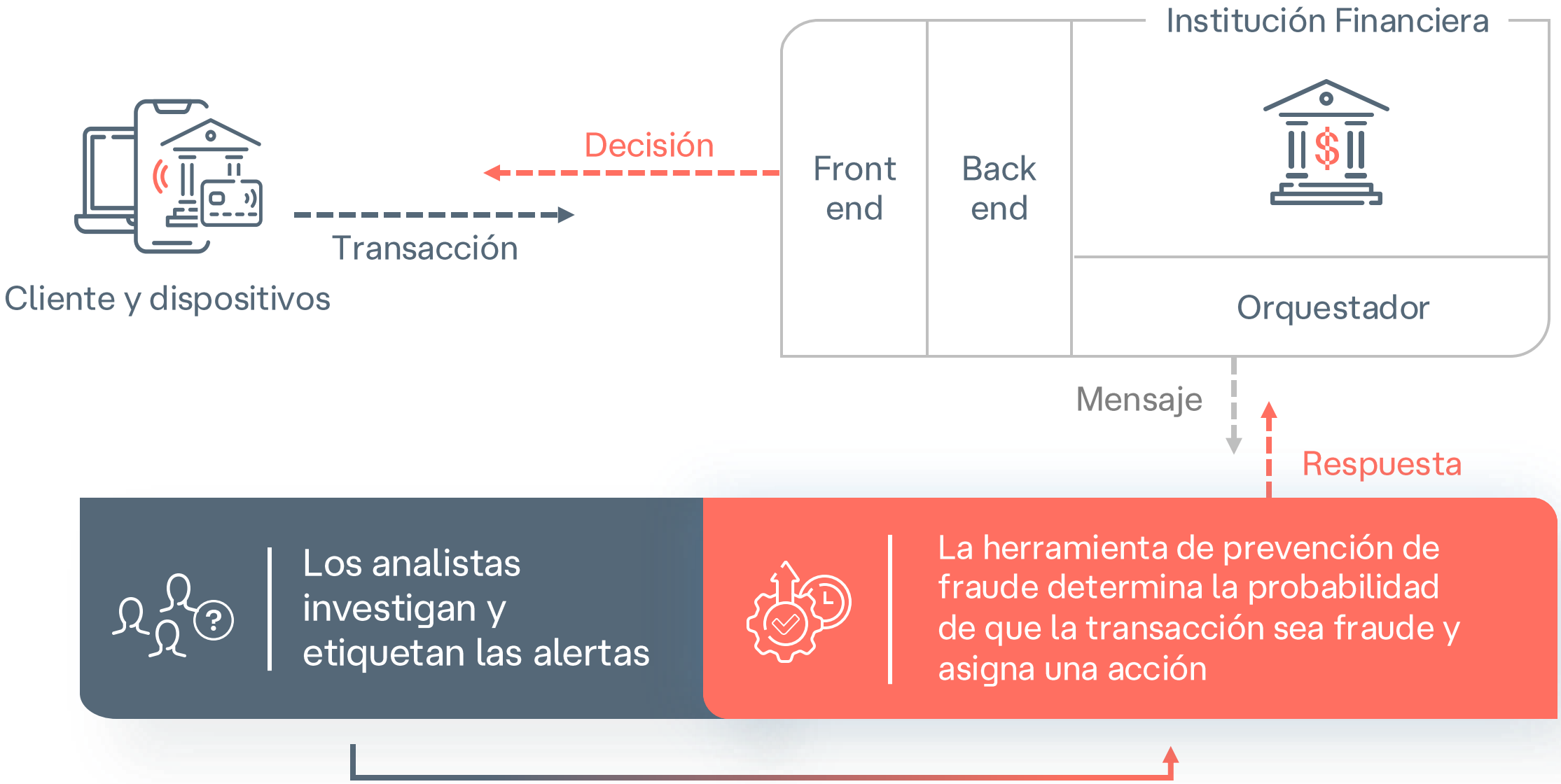


Lynx

Todo gira en torno a las personas,
a la relación entre tecnología,
talento y excelencia.

Gracias

Lynx


Institución Financiera
Front end
Back end
Orquestador
Decisión
Transacción
Cliente y dispositivos
Mensaje
Respuesta
Los analistas investigan y etiquetan las alertas
La herramienta de prevención de fraude determina la probabilidad de que la transacción sea fraude y asigna una acción