# Inteligencia Artificial y su Aplicación en la Prevención de Fraudes Bancarios

(Informe elaborado por: Mayker Córdova Pintado – Practicante Preprofesional, Prevención de Fraude y Gobierno Operacional, Scotiabank Perú)

1. Situación actual del fraude y la Inteligencia Artificial  
El fraude financiero ha evolucionado de forma acelerada. Hoy en día, los atacantes usan Inteligencia Artificial (IA) para crear correos falsos, deepfakes e identidades sintéticas, lo que hace que las estafas sean más sofisticadas.   
Los sistemas tradicionales de reglas son insuficientes, mientras que la IA permite detección predictiva y aprendizaje continuo.   
  
Según Feedzai (2025), más del 50 % de los fraudes modernos involucran IA y el 90 % de los bancos ya la implementan. En Perú, la Ley N° 31814 impulsa su adopción ética. Mastercard y Visa han reducido hasta un 85 % los falsos positivos usando IA, y American Express mejoró su detección en 6 % con modelos LSTM (IBM, 2025).  
  
2. Tecnologías clave aplicadas al fraude  
a. Machine Learning: Aprende de datos históricos y predice comportamientos sospechosos. Un estudio (ArXiv, 2024) demostró que usando Deep Feature Synthesis se redujeron los falsos positivos en 54 %.  
b. Deep Learning: Redes neuronales que detectan secuencias anómalas. PayPal aumentó en 10 % la detección en tiempo real (IBM, 2025).  
c. NLP: Analiza lenguaje en mensajes y correos para identificar phishing. BBVA usa NLP para detectar patrones de suplantación (BBVA, 2025).  
d. Análisis de grafos: Detecta redes de lavado de dinero o colusión. PwC reporta bancos europeos que hallaron conexiones ocultas entre clientes (PwC, 2025).  
e. UEBA: Analiza comportamientos de usuarios y entidades. Santander España usa UEBA para prevenir accesos indebidos (Forbes, 2025).  
  
3. Aplicaciones en la banca  
La IA se aplica en:  
- Fraude transaccional: análisis en milisegundos. Mastercard y Visa redujeron falsos positivos en 85 %.  
- Robo de identidad: visión por computadora para validar documentos. IBM redujo fraudes de identidad en 30 %.  
- Lavado de dinero (AML): IA prioriza alertas reales, reduciendo 95 % falsos positivos (Feedzai, PwC).  
- Fraude interno: UEBA detecta accesos fuera del comportamiento normal.  
  
Scotiabank puede integrar información de distintos canales (tarjetas, banca móvil, AML) para una visión 360° del cliente.  
  
4. Beneficios estratégicos  
La IA ofrece:  
- Mayor precisión y menos fricción con clientes.  
- Procesamiento de millones de transacciones en tiempo real.  
- Reducción de pérdidas y fortalecimiento de la confianza.  
Ejemplo: CoreCard, cliente de Feedzai, redujo el fraude en 64 %.   
  
5. Desafíos y hoja de ruta  
Desafíos: calidad de datos, talento especializado, infraestructura e IA explicable conforme a las leyes N° 31814 y N° 29733.  
Hoja de ruta:  
1. Diagnóstico inicial del tipo de fraude prioritario.  
2. Proyecto piloto en e-commerce o tarjetas.  
3. Escalamiento progresivo.  
4. Capacitación en IA explicable (XAI).  
5. Centro de Excelencia en IA.  
  
6. Oportunidades futuras  
- IA generativa: crea datos sintéticos para entrenar modelos robustos.  
- Aprendizaje federado: colaboración interbancaria sin compartir datos sensibles.  
- IA adversarial: modelos resistentes a manipulación de defraudadores.  
BBVA (2025) usa IA generativa para simular escenarios de fraude y probar resiliencia.  
  
7. Conclusión  
La IA potencia al analista de fraude, no lo reemplaza. Scotiabank puede liderar la banca peruana si combina experiencia humana con modelos predictivos, asegurando transparencia y ética.  
  
Fuentes principales:  
Feedzai (2025), IBM (2025), PwC (2025), BBVA (2025), Forbes (2025), ICPF (2025), FinTech México (2025), Topaz Evolution (2025), Scotiabank México (2025).  
**Principales fuentes consultadas**

* PwC (2025). *Aplicaciones prácticas de Inteligencia Artificial en el sector bancario.*  
  👉 <https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/aplicaciones-practicas-de-inteligencia-artificial.html>
* Asociación ICPF (2025). *Estrategias de IA para la Detección y Prevención del Fraude.*  
  👉 <https://asociacionicpf.org/noticias/estrategias-de-ia-para-la-deteccion-y-prevencion-del-fraude>
* Forbes España (2025). *Así se aplica la IA en la detección de fraudes en el sector bancario.*  
  👉 <https://forbes.es/tecnologia/699969/asi-se-aplica-la-ia-en-la-deteccion-de-fraudes-en-el-sector-bancario>
* Feedzai (2025). *Tendencias de Fraude con IA 2025: Los Bancos Contraatacan.*  
  👉 <https://www.feedzai.com/es/pressrelease/tendencias-de-fraude-con-ia-2025>
* IBM (2025). *Detección de fraude con IA en la banca.*  
  👉 <https://www.ibm.com/es-es/think/topics/ai-fraud-detection-in-banking>
* FinTech México (2025). *El rol de la IA en la detección de fraude.*  
  👉 <https://www.fintechmexico.org/notices/el-rol-de-la-inteligencia-artificial-ia-en-la-deteccion-de-fraude-estadisticas-y-aplicaciones-claves>
* Topaz Evolution (2025). *Prevención de fraude: cómo proteger la operación financiera con IA.*  
  👉 <https://www.topazevolution.com/es/blog/prevencion-de-fraude-bancario>
* BBVA (2025). *La nueva era de la ciberseguridad: cómo la IA ayudará a la prevención del fraude.*  
  👉 <https://www.bbva.com/es/innovacion/la-nueva-era-de-la-ciberseguridad-como-la-ia-ayudara-a-la-prevencion-del-fraude-en-2025>
* Scotiabank México (2025). *Identifica cómo la IA es usada para hacer fraudes digitales.*  
  👉 <https://www.scotiabank.com.mx/blog/para-ti-identifica-como-la-ia-es-usada-para-hacer-fraudes-digitales>