

incode

2025

Las Fallas Ocultas en la Prevención de Fraude: Por Qué los Modelos de IA Propietaria Son el Futuro.



Introducción: Por Qué la Prevención de Fraude Tradicional Está Fallando

A medida que el fraude se vuelve cada vez más sofisticado, las empresas se están dando cuenta de que los sistemas tradicionales de verificación de identidad (IDV) son **demasiado lentos, rígidos y dependientes de tecnología de terceros** para mantenerse al día. Los cibercriminales usan IA a una escala nunca antes vista, recurriendo a deepfakes, identidades sintéticas y técnicas de fraude automatizadas para evadir los sistemas de verificación obsoletos.

¿El problema? **La mayoría de los proveedores de IDV no controlan su propia tecnología de detección de fraude.** En lugar de eso, **dependen de modelos de IA licenciados a terceros**, que tardan **meses en adaptarse** a nuevos patrones de fraude. Mientras tanto, los estafadores **iteran en días** o incluso horas.

Para combatir eficazmente las amenazas modernas de fraude, las empresas necesitan un **sistema de prevención de fraude impulsado por IA totalmente propio**, que se adapte en tiempo real, elimine la dependencia de proveedores externos y ofrezca un nivel de precisión líder en la industria.

En esta guía, revelamos las fallas ocultas en la prevención de fraude tradicional y explicamos por qué la **IA propia es el único camino a seguir**.

El Estado Deficiente de la Verificación de Identidad de Terceros

1 Adaptación Lenta al Fraude

- Los proveedores de IDV de terceros licencian sus modelos de IA a proveedores externos, por lo que no tienen control directo sobre las actualizaciones para detectar fraudes.
- Estos proveedores tardan meses en implementar actualizaciones frente a nuevas técnicas de fraude, dejando a las empresas vulnerables.
- En cambio, los cibercriminales afinan sus ataques constantemente: cada semana, o incluso cada día, surgen nuevas amenazas con deepfakes e identidades sintéticas.

2 Altas Tasas de Falsos Positivos y Negativos

- Las herramientas tradicionales de IDV usan técnicas poco precisas, lo que provoca falsos positivos (rechazo de clientes reales) y falsos negativos (fraudulentos que logran pasar).
- Ejemplo: Una fintech que usaba un proveedor de IDV de terceros vio un aumento del 15% en clientes legítimos marcados erróneamente como fraude, porque el algoritmo estaba desactualizado.

3 Poca Personalización y Adaptabilidad Sectorial

- Los modelos de IA de terceros no están diseñados para industrias específicas ni para los patrones de fraude locales.
- Una empresa que opera en Latinoamérica enfrenta retos distintos a una en Europa, pero los proveedores tradicionales ofrecen soluciones genéricas que no se adaptan al contexto.
- Sin IA propia, las empresas no pueden ajustar los modelos de detección de fraude a sus necesidades reales.

4 Falta de Agilidad en Cumplimiento Normativo

- Las regulaciones cambian constantemente (GDPR, AI Act, CCPA, actualizaciones de KYC/AML). Las empresas que dependen de IA de terceros luchan por adaptarse a tiempo.
- Las demoras en actualizar las normas pueden llevar a multas millonarias y daños reputacionales.

Conclusión Clave:

Los sistemas tradicionales de prevención de fraude carecen de agilidad, precisión y adaptabilidad para enfrentar las amenazas modernas. La única solución es una IA 100% propia.

El Poder de la IA Propietaria en la Prevención de Fraude

Por Qué la IA Propia Es el Futuro

Un sistema de prevención de fraude con IA propia se construye desde cero, lo que permite:



Real-time fraud model updates

Adaptándose a nuevas amenazas en días, no meses.



Detección de fraude específica por industria

Adaptada a fintech, e-commerce, cripto, viajes y economía gig.



Experiencia de usuario fluida

Reduciendo falsos positivos y eliminando fricciones innecesarias.



Adaptación ágil al cumplimiento normativo

Ajustándose rápido a las leyes de cada mercado.

La IA Propietaria de Incode en Acción



A diferencia de los proveedores de IDV que dependen de terceros, Incode controla el 100% de su stack de IA.

Lo que significa:

- Analizamos patrones de fraude en **tiempo real**, entrenando nuestros modelos según los desafíos específicos de nuestros clientes.
- **No esperamos a que un tercero actualice los modelos:** ajustamos las estrategias de detección al instante.
- **Nuestra detección de vida (liveness detection)** garantiza que las empresas verifiquen personas reales, no deepfakes generados por IA.



Biometric



Behavioral



Network

Resultados de Incode en Prevención de Fraude

99.65%

precisión en detección de identidades sintéticas.

50%

menos falsos positivos que los proveedores tradicionales de IDV.

11x

onboarding más rápidos gracias a la automatización con IA.

98.53%

tasa de verificación positiva (TPR) en comparaciones de selfies con documentos.

Ranked #1

en pruebas NIST FRVT por precisión y velocidad frente a otros proveedores.

El Rol de la **Identidad Digital (Digital Personhood)** en la Prevención de Fraude

La Evolución de la Verificación de Identidad

Antes, verificar identidad era comparar una cédula con una base de datos. **Pero las técnicas modernas de fraude superan ese enfoque.**

Identidad Digital: Más Allá de la Cédula

La identidad real incluye:

- **Patrones biométricos y de comportamiento** (expresiones faciales, movimientos).
- **Interacciones sociales y contextuales** (historial de transacciones, relaciones previas).
- **Detección de vida** — para verificar que haya una persona real, no un deepfake.

Los Riesgos de Ignorar la Identidad Digital

Sin una verificación avanzada de personalidad, las empresas corren el riesgo de:

- **Ser víctima de fraudes con deepfakes** (rostros y voces creadas por IA).
- **Perder clientes reales** por filtros de fraude mal calibrados.
- **Filtraciones y robo de identidad** al depender de bases de datos centralizadas.

Cómo Incode Potencia la Verificación de Identidad Digital

- **Detección de vida multimodal:** combinamos señales físicas, digitales y de comportamiento para detectar deepfakes, identidades falsas y bots.
- **Análisis conductual impulsado por IA:** evaluamos las interacciones en tiempo real para detectar fraudes antes de que ocurran.
- **Verificación activa y pasiva:** autenticación en tiempo real sin pedir pasos adicionales al usuario, eliminando fricciones.

Casos de Uso: Cómo la IA Propietaria Está Transformando la Seguridad



Fintech & Pagos

- Previene fraude de identidades sintéticas en créditos.
- Reduce falsos positivos en transacciones.



E-Commerce & Marketplaces

- Bloquea cuentas falsas creadas por bots.
- Previene fraudes de contracargos mediante biometría conductual.



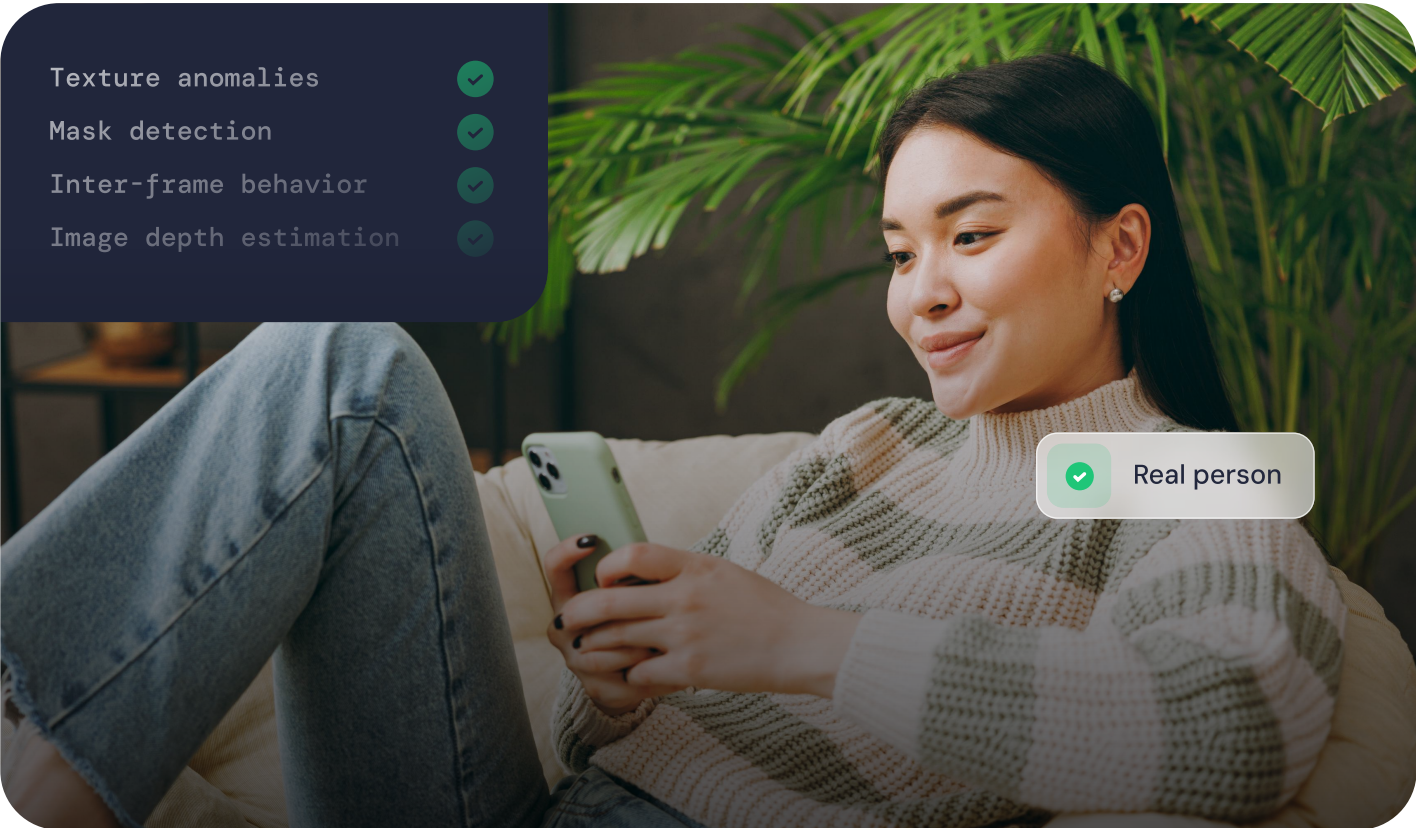
Economía Gig & Plataformas de Transporte

- Detecta perfiles falsos de conductores.
- Usa detección de vida para evitar cuentas falsas masivas.



Cripto & Web3

- Evita fraudes KYC con deepfakes.
- Asegura cumplimiento normativo con IA.



Las empresas líderes no permiten que los obstáculos de seguridad y cumplimiento frenen su crecimiento. Invierten en **tecnología escalable y propia** que elimina los riesgos de fraude y optimiza la experiencia del cliente.

El **Futuro** de la Prevención de Fraude: Lo Que las Empresas Deben Hacer



Eliminar proveedores de IA de terceros

Auditar tu sistema actual: ¿dependes de IA externa?



Implementar detección de fraude en tiempo real

Adoptar una solución nativa en IA que actualice sus modelos en días, no meses.



Usar verificación de identidad por capas

Combinar detección de vida, forense de documentos y biometría conductual.



Priorizar cumplimiento y experiencia de usuario

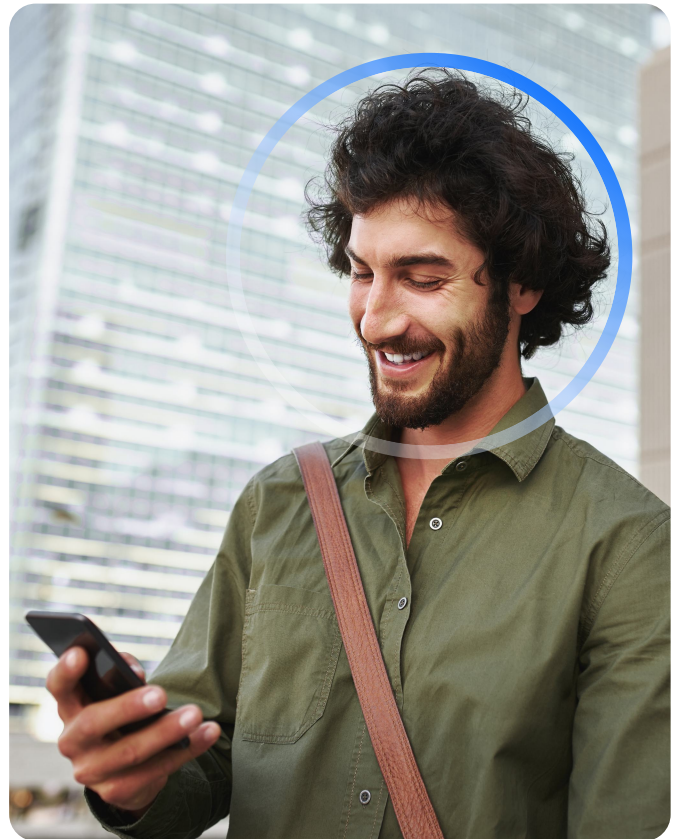
Evitar fricciones innecesarias para clientes legítimos.

Conclusión: Por Qué Incode es el Futuro en Prevención de Fraude con IA

En Incode, controlamos el 100% de nuestra IA, lo que nos permite:

- Adaptarnos al fraude en días, no meses.
- Ofrecer verificación de identidad automatizada y sin fricciones.
- Mantener a nuestros clientes protegidos sin limitaciones de terceros.

El futuro de la prevención del fraude pertenece a las empresas que invierten en soluciones de inteligencia artificial patentadas y en tiempo real.



Recibe más información

Sobre estrategias modernas contra el fraude, visita incode.com

Solicita un demo hoy