

FORTALEZA FINTECH: MODELOS INNOVADORES DE PREVENCIÓN Y MONITOREO

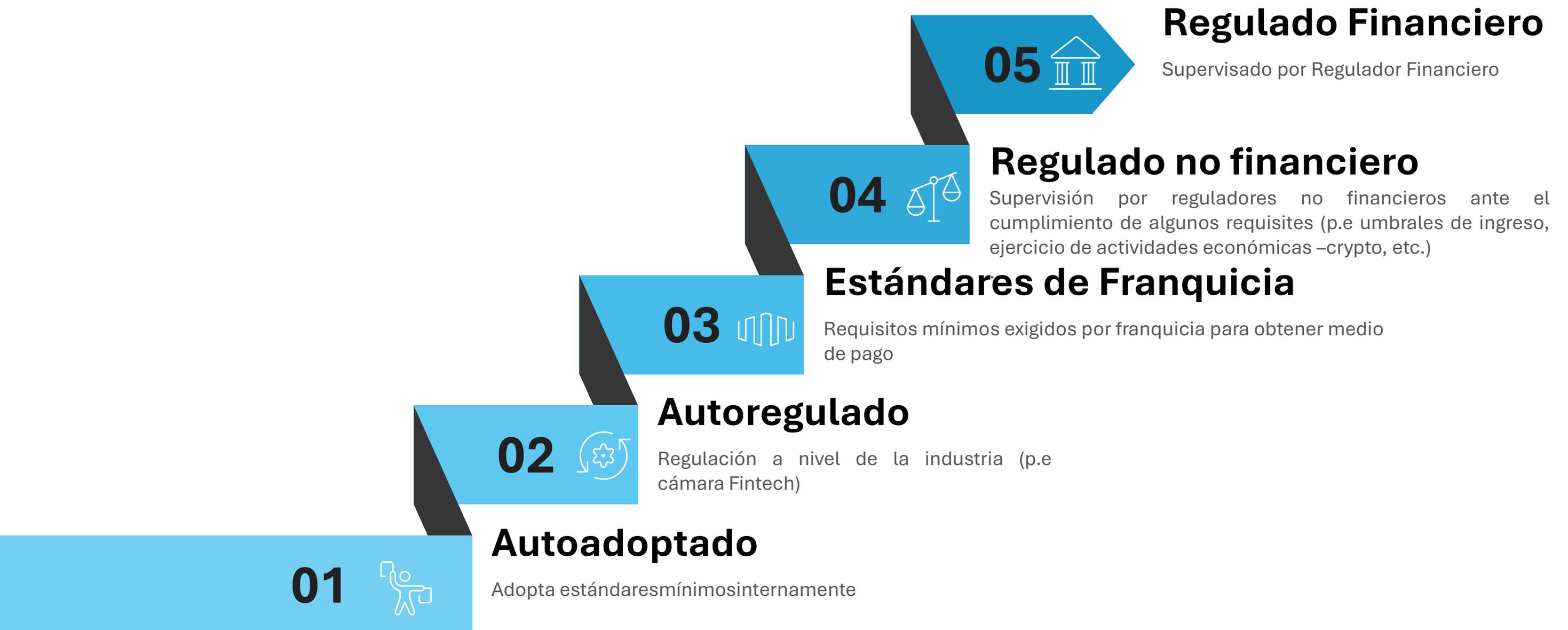
Presentado por:
Martín Franco (Uruguay)
Ing. Oscar Moratto (Colombia)

El Ecosistema Fintech: heterogéneo en mercado y tamaño



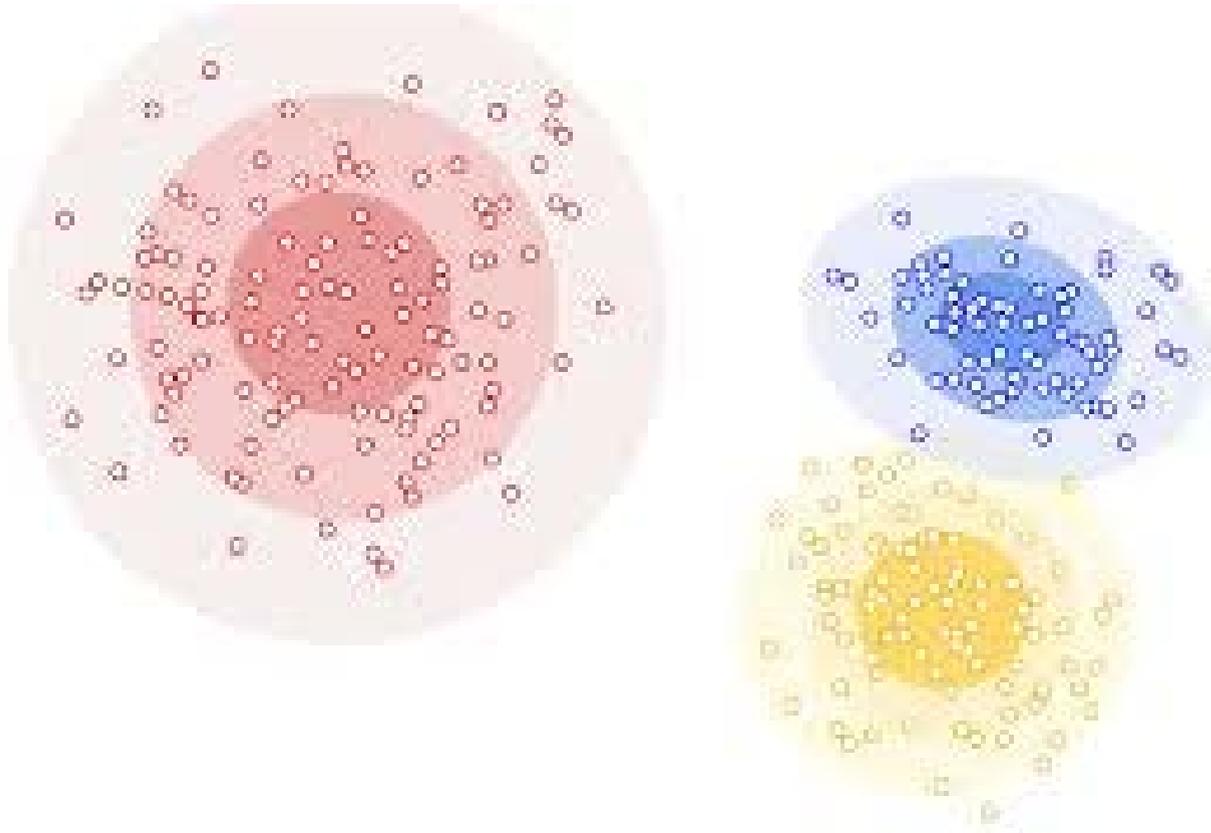
Con base en BID (2022). FinTech en América Latina y el Caribe. Un ecosistema consolidado para la recuperación

Etapas de maduración en modelos de gestión de riesgo en entornos FinTech

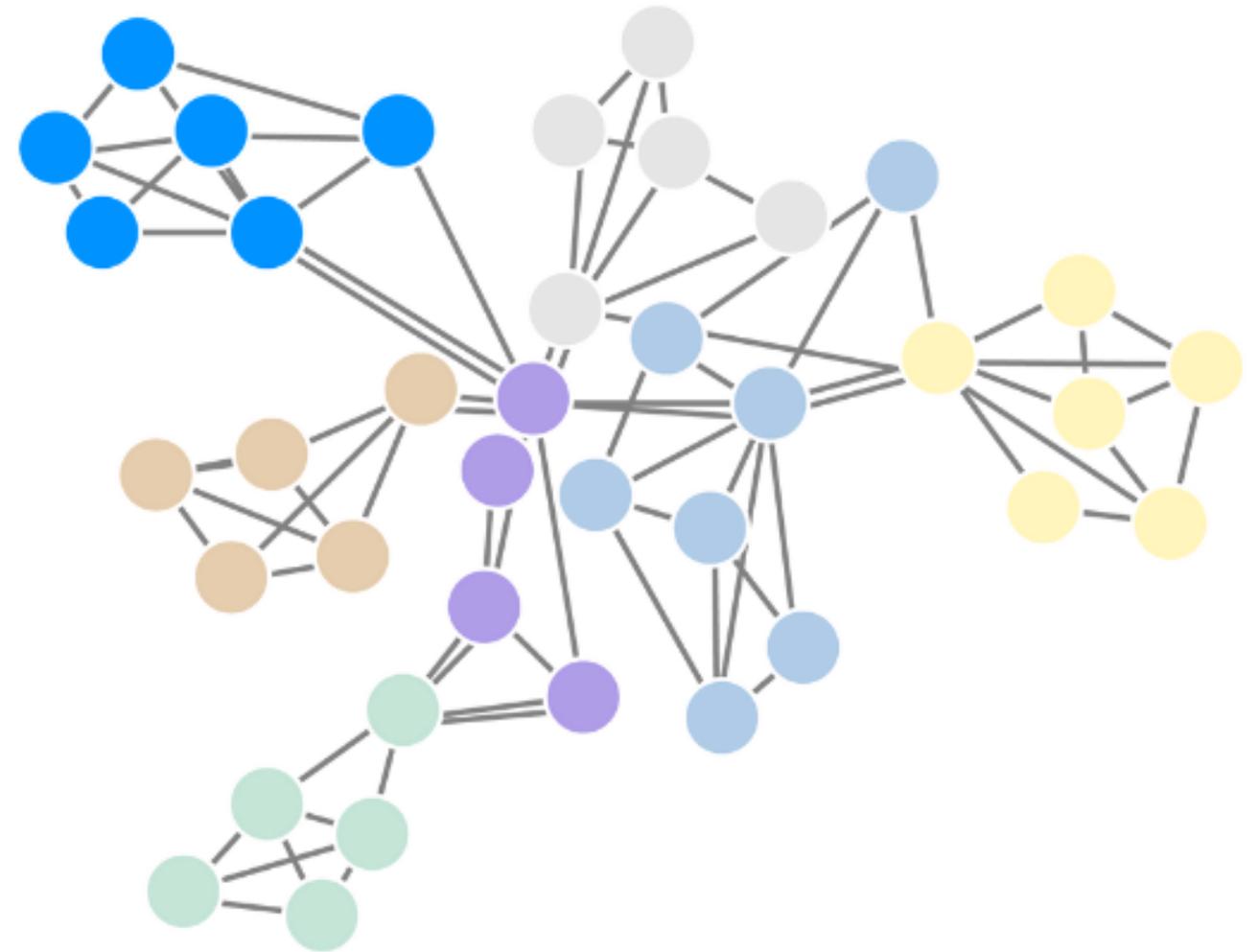


Oportunidades en cumplimiento

Segmentacion

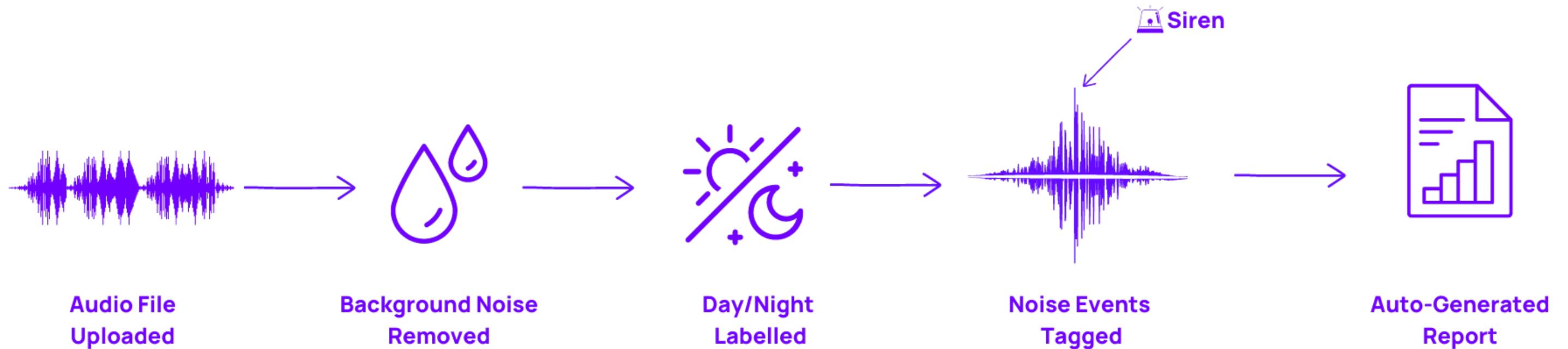


Detección de comunidades



Oportunidades en cumplimiento

Analisis de texto y audio en Comunicaciones con clientes (p.e. sentiment analysis)



Algunos Riesgos de IA e IAGen

LARAZÓN

Tecnología y consumo

NUESTRA ELECCIÓN

La terrorífica advertencia del creador de ChatGPT: "La IA ha derrotado casi todos los métodos de autenticación actuales"

Los sistemas de clonación de voz comprometen la seguridad de los usuarios y Sam Altman teme que esto provoque una "crisis de fraude"

- Chrome podrá cambiar automáticamente tus contraseñas si detecta que han sido filtradas
- Una de las plataformas más populares de Microsoft ha sido hackeada: gobiernos y empresas de todo el mundo están en problemas

Justin Leroux
@0xMidnight

AI will rapidly accelerate broad use of private key cryptography and decentralized ID.

Check out this Reddit "verification post" and ID made with Stable Diffusion. When we can no longer trust our eyes to ascertain whether content is genuine we'll rely on applied cryptography.

[Traducir post](#)

Verification post!
Workflow Included



12:52 p. m. · 5 ene. 2024 · 7.100 Reproducciones

AI Deepfake Tool ProKYC Cracks Crypto Exchange Authentication

Fake | Regulatory/Regulations

Oct. 18, 2024.

6 mins. read. 8 Interactions

In a troubling development for crypto security, the AI-driven ProKYC tool exposes vulnerabilities in identity verification, potentially reshaping the landscape of digital fraud.

¡Alerta Roja! IA en el Monitoreo Transaccional Fintech

El ecosistema fintech ha revolucionado el panorama financiero, pero la creciente amenaza del lavado de activos (AML) persiste como un desafío crítico. Los sistemas de monitoreo tradicionales, a menudo obsoletos, son ineficientes: generan una avalancha de falsos positivos que no solo saturan las operaciones, sino que también comprometen la experiencia del cliente. Ante este escenario, la **Inteligencia Artificial** emerge no solo como una opción, sino como la herramienta indispensable para revolucionar el monitoreo transaccional. La IA ofrece un enfoque mucho más preciso, rápido y verdaderamente centrado en el cliente, dejando atrás las deficiencias de los métodos convencionales.



El Poder de la IA: Eficiencia y Precisión Comprobadas



Detección Temprana

La IA permite la detección y el análisis de patrones inusuales en tiempo real, operando como un "sexto sentido" financiero que anticipa anomalías y riesgos antes de que se materialicen.



Reducción de Falsos Positivos

Una drástica reducción de hasta el 70% en falsos positivos, lo que optimiza la eficiencia operativa y libera al talento humano para que se concentre en investigaciones críticas de alto impacto.



Adopción Global

Con el 91% de las empresas líderes ya integrando la IA para priorizar alertas, su adopción se ha consolidado como un nuevo estándar y una ventaja competitiva clave en la industria financiera global.

Este cambio de paradigma no solo mejora la seguridad, sino que también promete un potencial de ahorro masivo, estimado en aproximadamente \$3.13 billones anuales a nivel mundial en la lucha contra el Lavado de Activos y Financiamiento del Terrorismo (LA/FT).



Capacidades Avanzadas de la IA en Fintech



Análisis de Documentos

La IA automatiza el procesamiento y análisis de documentos clave, reduciendo drásticamente los errores humanos y acelerando los procesos operativos críticos.



Detección de Comunidades

Identifica conexiones ocultas y grupos de riesgo que serían imposibles de detectar de forma manual, fortaleciendo significativamente la capacidad de prevención de fraude.



¡Precaución! Los Riesgos de la IA Generativa



Deepfakes y Suplantación Biométrica

La IA generativa facilita la creación de identidades sintéticas casi imposibles de diferenciar de las reales, lo que representa una grave amenaza para los sistemas de verificación tradicionales.



Vulnerabilidad en la Autenticación

Como ha advertido Sam Altman, la inteligencia artificial ya puede eludir y superar una gran variedad de métodos de autenticación, incluyendo aquellos basados en comportamiento, reconocimiento facial y de voz.



Sintetización y Clonación de Voz

Con tan solo una pequeña muestra del audio original, la IA es capaz de sintetizar y clonar voces, lo que permite la suplantación de identidad en llamadas telefónicas o mensajes de audio.



Modelos de IA en Acción: Mejores Prácticas Fintech



Gradient Boosting Machines

Estos modelos combinan múltiples árboles de decisión para clasificar transacciones con alta precisión, **minimizando los falsos positivos y optimizando la detección de fraudes.**



Redes Neuronales Profundas

Capaces de detectar patrones intrincados en vastos volúmenes de transacciones, **revelan anomalías que los sistemas tradicionales no pueden identificar.**



Clustering No Supervisado

Identifica automáticamente comportamientos atípicos y nuevas clases de fraude sin necesidad de datos etiquetados previamente, **adaptándose a amenazas emergentes.**

Estrategias de Mitigación de Riesgos



Autenticación Multicapa

Implementación de una combinación robusta de factores biométricos, comportamentales y contextuales para una verificación de identidad integral.



Monitoreo Continuo

Evaluación proactiva y constante del comportamiento del usuario a lo largo de toda la sesión, no solo en el punto de inicio.



Detección de Anomalías en Tiempo Real

Identificación inmediata de desviaciones significativas del patrón de comportamiento habitual del usuario para prevenir actividades sospechosas.



Análisis de Metadatos

Análisis exhaustivo de metadatos (dirección IP, tipo de dispositivo, geolocalización) para validar la legitimidad y el contexto de las transacciones.

**GUARANTEED
SECURITY**

Conclusiones Clave



IA como Imperativo Estratégico

La IA es un pilar fundamental para un monitoreo AML (Anti-Lavado de Dinero) efectivo y eficiente en el sector fintech.



Doble Impacto

La IA impulsa la eficiencia operativa mediante la reducción de falsos positivos y optimiza la experiencia del usuario a través de la personalización y la transparencia.



Innovación Responsable

Es crucial abordar proactivamente los riesgos de la IA (como deepfakes y desafíos de autenticación) mediante el desarrollo de sistemas éticos y en constante evolución.



Hacia un Futuro Seguro

La IA es clave para la maduración de la gestión de riesgos y el fortalecimiento de la integridad en el ecosistema financiero.



Su Próximo Movimiento Estratégico

La Inteligencia Artificial es la clave para transformar su estrategia de prevención de lavado de dinero y financiamiento al terrorismo.

Ahora es el momento de integrar esta capacidad en su organización para construir una defensa financiera inexpugnable, que sea intuitiva para el usuario y totalmente adaptada al entorno digital.

¿Cuál será su próximo movimiento?

