

Cerrando el círculo.

IA para combatir los fraudes generados con IA





La inteligencia artificial generativa (GenAI) ha amplificado el fraude de identidad, permitiendo a los delincuentes crear deepfakes, identidades sintéticas y documentos hiperrealistas con una eficiencia alarmante. La verificación de identidad únicamente mediante *liveness* ya no es suficiente.

El

37%

de los líderes de riesgo señalan el aumento del fraude generado con IA como su principal preocupación.¹

¹Fuente: Mitek y Censuwide, Reporte de Inteligencia de la Identidad 2024

01

El fraude de identidad digital, un clásico que no deja de reinventarse

El fraude digital ya no es un fenómeno aislado; es ya una experiencia común para los consumidores españoles. Y puesto que cada vez es más sofisticado y difícil de detectar, las empresas necesitan defensas más robustas para evitarlo antes de que se produzca.

Exposición masiva

Más de la mitad de los consumidores españoles, un 52%, afirma haber sufrido algún intento de fraude digital en el último año.²

El ataque se humaniza

El principal canal de ataque ya no es el email, sino la llamada telefónica (vishing), que representa el 28% de los intentos, reflejando un movimiento hacia tácticas más humanas y personalizadas.⁴

Fraude consumado

El 9% de los intentos de fraude logra materializarse. Extrapolado a la población, esto supone que 3,7 millones de personas han podido ser objeto de fraude consumado en 2025.³



01

El fraude de identidad digital, un clásico que no deja de reinventarse

Dominio de la suplantación

2 de cada 3 fraudes se basan en la suplantación a entidades bancarias, empresas de servicios o teleoperadoras (66% de los casos), minorando enormemente la confianza del usuario (suplantación institucional)⁵

El

34%



de los fraudes consumados se materializa mediante ingeniería social: el usuario realiza personalmente la transferencia de fondos bajo engaño, lo que muestra que el cibercriminal convence a la víctima para que actúe por sí misma.⁶

^{2,3,4,5,6} Fuente: AEEFC, III Informe sobre Fraude a Consumidores en España 2025-2026

02

Puntos de ataque críticos. ¿Dónde hay más riesgo?

1

Apertura de cuentas fraudulentas en el proceso de onboarding: los atacantes usan plantillas de documentos de identidad falsos pero hiperrealistas generados con IA, datos personales robados (PII) e identidades sintéticas para superar los controles iniciales.

2

Apropiación de cuentas (ATO/login): los estafadores aprovechan las medidas de seguridad débiles o insuficientes y utilizan deepfakes y ataques de inyección para engañar a los sistemas de verificación.

3

Transacciones de alto riesgo: se utilizan técnicas de suplantación avanzadas e impulsadas por GenAI para realizar acciones no autorizadas.



El mito de la "prueba de vida" (liveness)

Una simple prueba de vida ya no es suficiente. Los deepfakes y los ataques de inyección digital han evolucionado para eludir los controles básicos de liveness, engañando al sistema para que valide que una persona real está presente cuando en realidad se trata de una imagen o video sintético.

03

Digital Fraud Defender. Cerrando el círculo de los fraudes con IA generativa

Muchos sistemas de defensa son insuficientes o quedan rápidamente obsoletos. Por ello, es necesario un escudo por capas que, además de proteger, aprenda y pueda prevenir los fraudes antes de que se produzcan, y los futuros que puedan llegar.

Digital Fraud Defender es el conjunto de funcionalidades de Mitek diseñado para superar las amenazas impulsadas con IA, protegiendo a las empresas en cada etapa del ciclo de vida digital del cliente.



Detección de ataques de inyección: estrategia multicapa que detecta la presencia de cámaras virtuales, resolución sospechosa y manipulación en el flujo de datos.



Detección de ataques con plantillas: monitorea el uso repetido de PII y retratos, identificando intentos de fraude recurrentes generados por IA



Detección de deepfakes: tecnología única de detección pasiva que analiza pistas sutiles en video o audio, sin requerir la participación activa del usuario.

03

Digital Fraud Defender. Cerrando el círculo de los fraudes con IA generativa



Defensa multicapa: utiliza IA y modelos de aprendizaje adaptativo para identificar nuevos patrones de fraude en tiempo real.



Vídeo desasistido reforzado: verificación remota con detección avanzada de deepfakes, manipulación digital e identidades sintéticas conforme a SEPBLAC.

Los consumidores españoles exigen más tecnología:

El 30%

demanda validación adicional de acceso (doble factor) y el 17% apoya el uso de la biometría facial como herramienta antifraude.⁷

⁷ Fuente: AEEFC, III Informe sobre Fraude a Consumidores en España 2025-2026

03

Digital Fraud Defender. Cerrando el círculo de los fraudes con IA generativa

Proceso SIN Digital Fraud Defender

El atacante inyecta un deepfake y bypassa el liveness básico.

La identidad sintética supera la verificación básica de documentos y biometría simple.

El delincuente se apropia de la cuenta y realiza transacciones críticas (ATO).

Fraude consumado y pérdida financiera.

Proceso CON Digital Fraud Defender

Se detecta la presencia de cámaras virtuales y se analizan flujos de datos anómalos: ataque de inyección.

Se detectan las plantillas generadas con IA, el uso repetido de PII y la manipulación digital en el documento: ataque con plantillas.

La verificación biométrica adaptativa protege el login y las transacciones críticas, con detección pasiva de deepfakes.

Usuario legítimo → Operación segura. Reducción de las vulnerabilidades en procesos de autenticación escalonada.

03

Digital Fraud Defender. Cerrando el círculo de los fraudes con IA generativa

Vídeo desasistido reforzado: una capa extra de seguridad ante la aceleración del fraude de identidad impulsado con IA

La verificación por vídeo desasistido es, desde hace tiempo, un requisito normativo para las entidades financieras y otros sectores regulados en España.

Dado que el fraude evoluciona más allá de los documentos falsos para incluir deepfakes, replays de pantalla, manipulación digital e identidades sintéticas generadas con IA, es necesario reforzar las capacidades de defensa de forma recurrente.

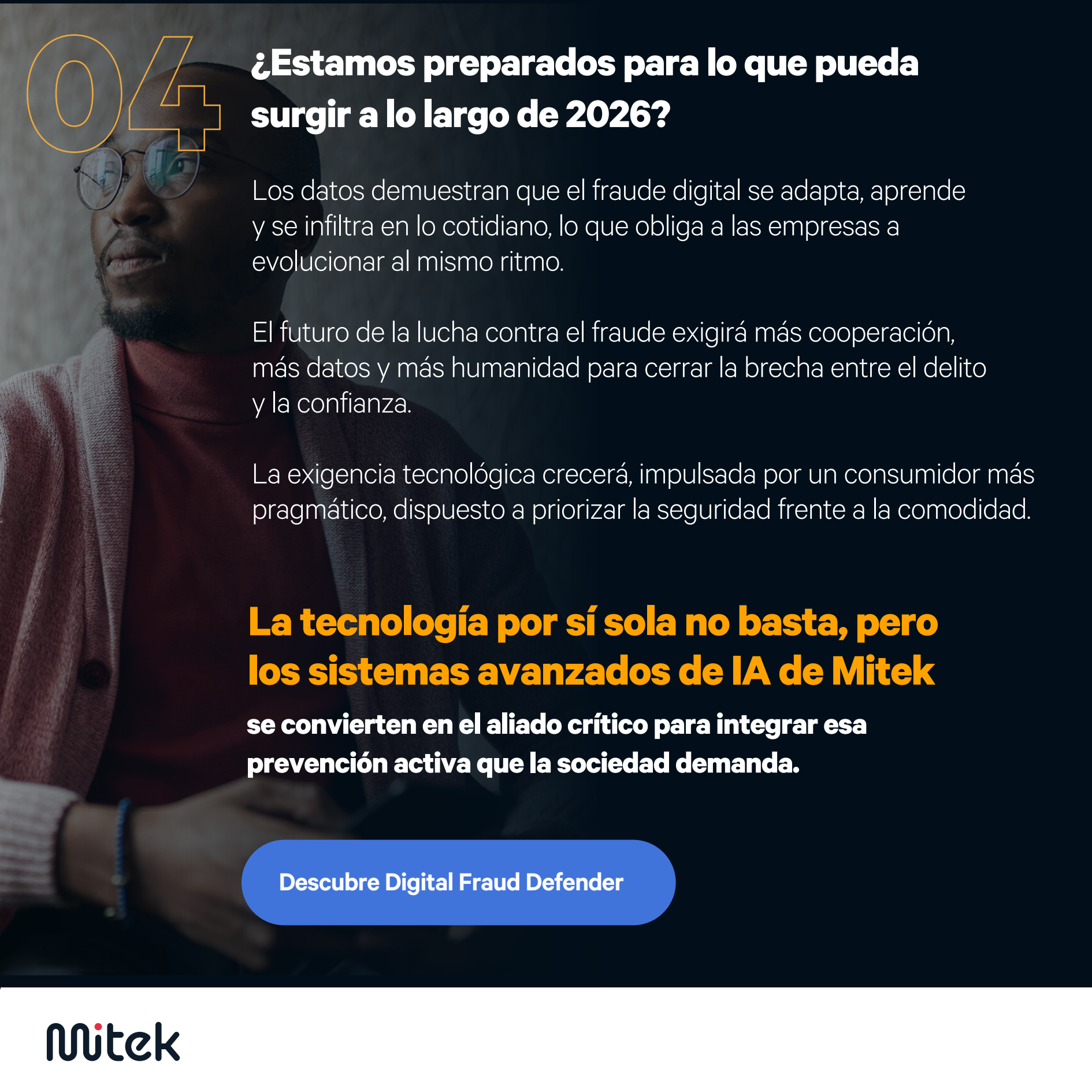
Esta capacidad está diseñada para ayudar a las entidades reguladas a defenderse frente a una ola de fraude de identidad impulsado

por IA que crece rápidamente, y refuerza la solución de verificación por vídeo desasistido de Mitek, ampliamente utilizada en España para la verificación remota de identidad conforme a SEPBLAC, incluyendo:

- ✓ **Detección de deepfakes faciales**
- ✓ **Análisis de manipulación digital y replays de pantalla**
- ✓ **Protección frente a ataques de inyección**
- ✓ **Análisis de galerías faciales para detectar ataques repetidos o coordinados**

Reforzamos la protección frente al fraude con IA sin fricción innecesaria para los clientes legítimos.

Reforzar el vídeo desasistido es clave para proteger el onboarding, el principal objetivo de los ataques impulsados por IA.



04

¿Estamos preparados para lo que pueda surgir a lo largo de 2026?

Los datos demuestran que el fraude digital se adapta, aprende y se infiltra en lo cotidiano, lo que obliga a las empresas a evolucionar al mismo ritmo.

El futuro de la lucha contra el fraude exigirá más cooperación, más datos y más humanidad para cerrar la brecha entre el delito y la confianza.

La exigencia tecnológica crecerá, impulsada por un consumidor más pragmático, dispuesto a priorizar la seguridad frente a la comodidad.

La tecnología por sí sola no basta, pero los sistemas avanzados de IA de Mitek

se convierten en el aliado crítico para integrar esa prevención activa que la sociedad demanda.

[Descubre Digital Fraud Defender](#)

Pide más información sin compromiso

Toma medidas hoy evaluando tus defensas actuales contra el fraude y descubre cómo las soluciones impulsadas por IA de Mitek pueden ayudarte a mantenerte un paso por delante de los estafadores mientras ofreces una experiencia superior al cliente.

Pide más información

Sobre Mitek

Mitek (NASDAQ: MITK) es líder global en acceso digital, fundado para conectar los mundos físico y digital. Las avanzadas tecnologías de verificación de identidad de Mitek y su plataforma global hacen que el acceso digital sea más rápido y seguro que nunca, proporcionando a las empresas nuevos niveles de control, facilidad de implementación y operación, mientras protege todo el recorrido del cliente. Confiado por el 99 % de los bancos de EE. UU. para depósitos móviles y por 7.900 de las mayores organizaciones del mundo, Mitek ayuda a las empresas a reducir riesgos y cumplir con los requisitos regulatorios. Más información en miteksystems.com/es.

Síguenos

Lee los últimos artículos del blog de Mitek aquí:

miteksystems.com/es/blog



Una empresa de NASDAQ® | miteksystems.com/es Copyright © 2025 Mitek Systems, Inc. Confidencial. Todos los derechos reservados.

Este documento tiene fines informativos generales y no pretende ser ni debe considerarse como asesoramiento legal o regulatorio sobre hechos o circunstancias específicos. Toda la información proporcionada en este documento se ofrece "tal cual" sin garantías de ningún tipo, ya sean explícitas o implícitas. El contenido de este documento no puede citarse ni referirse para ningún propósito sin el consentimiento previo por escrito de Mitek o sus afiliados.