

Deepfakes: por qué su **liveness 2D** ya no es suficiente

El fraude de identidad se industrializó con IA generativa

Rostros sintéticos, inyección de cámara y agentes autónomos que **orquestan ataques completos**. Qué está pasando en América Latina, cómo operan los ataques y **por qué la biometría 3D es la respuesta técnica — y jurídica.**

El fraude que sus controles actuales no ven

LA AMENAZA

1.

La suplantación ya no requiere una cédula robada. **Con herramientas de IA disponibles públicamente**, un atacante produce un rostro hiperrealista, lo anima en tiempo real y lo inyecta en el flujo de verificación de una app.

El informe de fraude de identidad 2025-2026 de Sumsb encontró que **más del 81% de los fraudes con IA a nivel global involucraron deepfakes**; en la región los ataques crecen a triple dígito año contra año.

La escalera de sofisticación del ataque

Nivel 1



Presentación de foto

Una foto impresa o en pantalla frente a la cámara. ~31% de los intentos. Lo detecta cualquier liveness básico.

Nivel 2



Video pregrabado

Videos editados o tomados de redes sociales y streaming. ~46% de los intentos. Derrota selfies estáticas y liveness débiles.

Nivel 3



Deepfake en tiempo real

Rostros sintéticos animados en vivo, con inyección de cámara virtual. Derrota la mayoría de liveness 2D pasivos.

Nivel 4



Identidad sintética + agentes de IA

Datos reales filtrados combinados con rostros y documentos generados por IA, orquestados de extremo a extremo por agentes autónomos. Un solo perfil fraudulento llegó a vincularse a 949 identidades distintas.



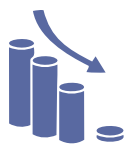
48,3%

de los casos de fraude en América Latina ya corresponde a **identidades sintéticas creadas con IA**.



1 de 5

intentos de fraude biométrico a nivel global **ya involucra deepfakes**.



US\$280K

pérdida promedio cuando un ataque con deepfakes tiene éxito (Unico / Liminal)



El ángulo regulatorio: en Colombia, la **Ley 2573 de 2026** traslada a su entidad la carga de probar que la verificación funcionó. Un deepfake que supera su liveness no es solo una pérdida por fraude: **es una vinculación cuyo cobro no podrá perseguir**.

Vector de ataque → cómo lo neutraliza Unicus

Un deepfake es, en esencia, una proyección 2D. Unicus verifica con biometría facial 3D certificada (FaceTec): reconstruye la geometría tridimensional real del rostro durante la sesión y valida señales fisiológicas en vivo. Esta es la correspondencia entre cada vector y la defensa:

Vector de ataque	Defensa <u>Unicus</u>
 Foto impresa o en pantalla	La reconstrucción 3D detecta la ausencia de profundidad real del rostro : una superficie plana no supera la sesión.
 Video pregrabado o reproducido	El análisis de sesión en vivo valida que la interacción ocurre en tiempo real , no una reproducción.
 Deepfake animado en tiempo real	La geometría 3D y las señales fisiológicas en vivo no pueden ser sintetizadas de forma consistente por una proyección generada.
 Inyección de cámara virtual	Detección de ataques de inyección en el canal de captura, más allá de lo que ve “la cámara”.
 Identidad sintética / fraude serial	Búsqueda biométrica 1:N contra el histórico : el mismo rostro no puede enrolarse con múltiples identidades.
 Documento falso o adulterado	Verificación documental de la cédula + cotejo facial 1:1 contra la foto del documento.
 Disputa posterior (¿quién se vinculó?)	Evidencia auditable por transacción : resultado, sello de tiempo y contexto — su defensa bajo la Ley 2573.



El resultado operativo: menos fraude aceptado sin castigar la conversión. La verificación toma segundos dentro de su propio flujo digital, con SDKs nativos para web, iOS, Android y React Native, y un mismo motor para enrolamiento, autenticación en operaciones sensibles y validación de edad.

Cumplir no tiene por qué costar como un proveedor global

El estándar probatorio de la Ley 2573 no distingue entre un banco grande y una fintech de 20 personas: la exigencia es la misma. Por eso Unicus fue diseñado **para que el cumplimiento sea viable a cualquier escala.**



Sin mínimos de entrada elevados

Planes de volumen graduado, volumen comprometido o usuario activo, según su operación. Empiece con un piloto y **escale con resultados.**



Costo total de propiedad menor

Integración vía API/SDK con **acompañamiento directo del equipo** de ingeniería — sin meses de consultoría facturable ni intermediarios.



Equipo local, contratación local

Soporte en español desde Bogotá, contratación en Colombia y acuerdos en moneda local posibles: **sin la volatilidad ni los sobrecostos** de un contrato 100% en USD.



Pago por verificación, no por promesas

Modelo de **tarifas escalonadas por volumen**: paga menos por transacción a medida que crece. Sin licencias de plataforma infladas.

¿Quiere ver un deepfake estrellarse contra un liveness 3D?

Agende un demo **de 20 minutos**: le mostramos en vivo cómo Unicus detecta los ataques que superan la verificación tradicional, y evaluamos su flujo de onboarding actual contra la escalera de sofisticación de esta guía.



<https://www.tekbees.com>



<https://www.linkedin.com/company/tekbees/>