

XXIII ENCUENTRO CLARCIEV

HONDURAS 2026

GOBIERNO DE LA REPÚBLICA DE HONDURAS

RNP
JUNTOS SOMOS PATRIA

CLARCIEV
CONSEJO LATINOAMERICANO Y DEL CARIBE DE REGISTRO CIVIL, IDENTIDAD Y ESTADÍSTICAS VITALES

OEA

UNHCR ACNUR
La Agencia de la ONU para los Refugiados



La próxima gran crisis de confianza

Lo que aprendimos protegiendo más de
7 mil millones de verificaciones en 195 países

Iñigo Castillo
Incode General Manager LATAM

La amenaza

El fraude que ya no se ve como fraude

Este documento parece real.
La identidad detrás de él, no.

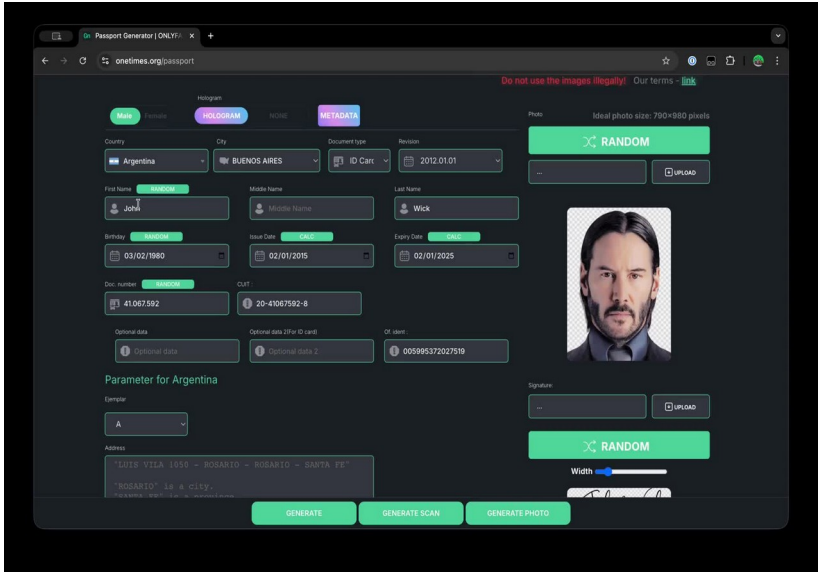
En 2026, el fraude de identidad ya no se detecta a simple vista. Se ve como una persona normal, con un documento auténtico, presentada por una identidad fabricada.



La barrera de entrada desapareció

Un documento hiperrealista por 7 dólares en menos de 7 minutos

En mercados clandestinos, basta con subir una foto, elegir un país y pagar con criptomonedas para recibir un documento de identidad falso, sin conocimientos técnicos



Un rostro sintético que coincide con el documento

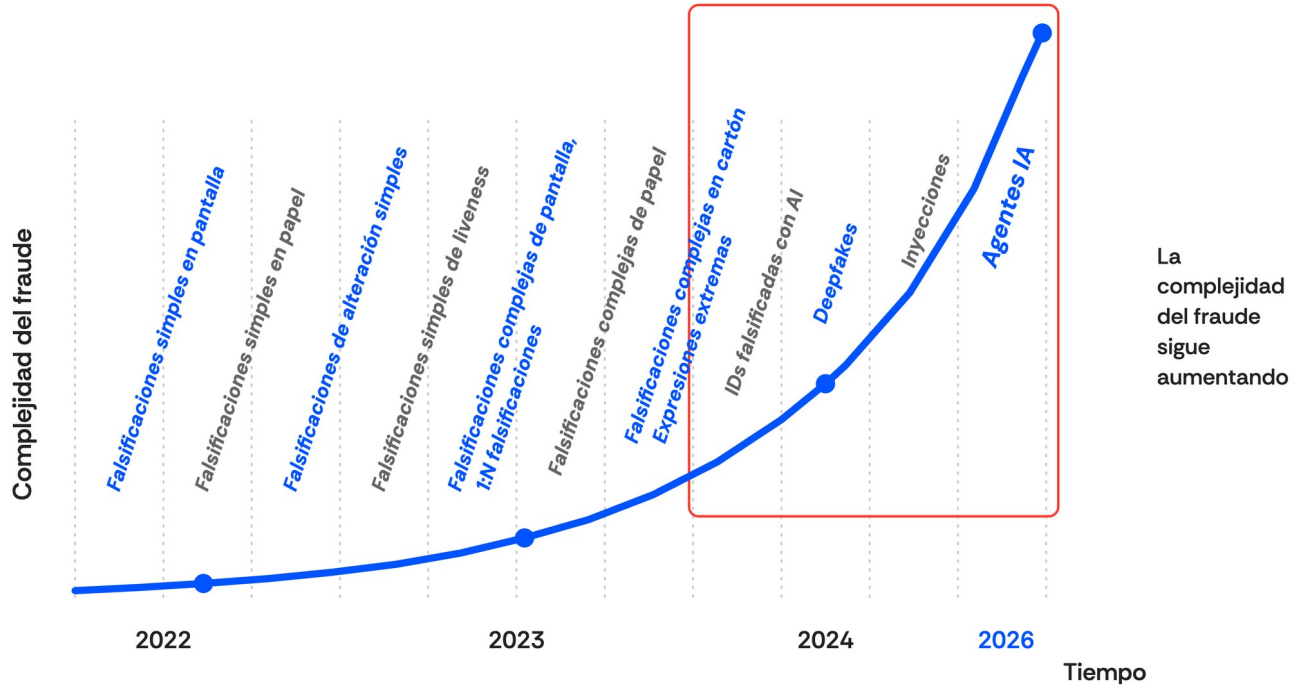
Generado y animado con IA, el rostro no pertenece a una persona real. Los datos del documento sí pueden ser auténticos y provenir de una filtración.

COMPOSICIÓN DEL ATAQUE

Documento sintético +
rostro generado por IA +
prueba de vida sintética =
una sesión de verificación capaz de superar controles.



La IA no inventó el fraude: lo volvió barato, masivo y creíble



Fuente: Incode

Fraude digital

La región se digitalizó más rápido de lo que aprendió a protegerse

- Más servicios y transacciones migran a canales digitales.
- Cada nuevo canal amplía la superficie de ataque.
- La digitalización avanzó más rápido que los mecanismos de protección.
- La identidad se convirtió en un punto crítico de entrada para el fraude.

LATAM

25%

incremento anual en incidentes cibernéticos entre 2014 y 2023

+2,800

ciberataques por semana

41%

más ciberataques que el promedio global

$3.81M USD

costo promedio de respuesta, recuperación e impacto

277 días

tiempo promedio para identificar y contener una brecha en LATAM



- 207 días para detección
- 70 días para contención

Fuente: Reporte Ciberseguridad, habilitador de confianza y competitividad. Incode y Endeavor, 2025.

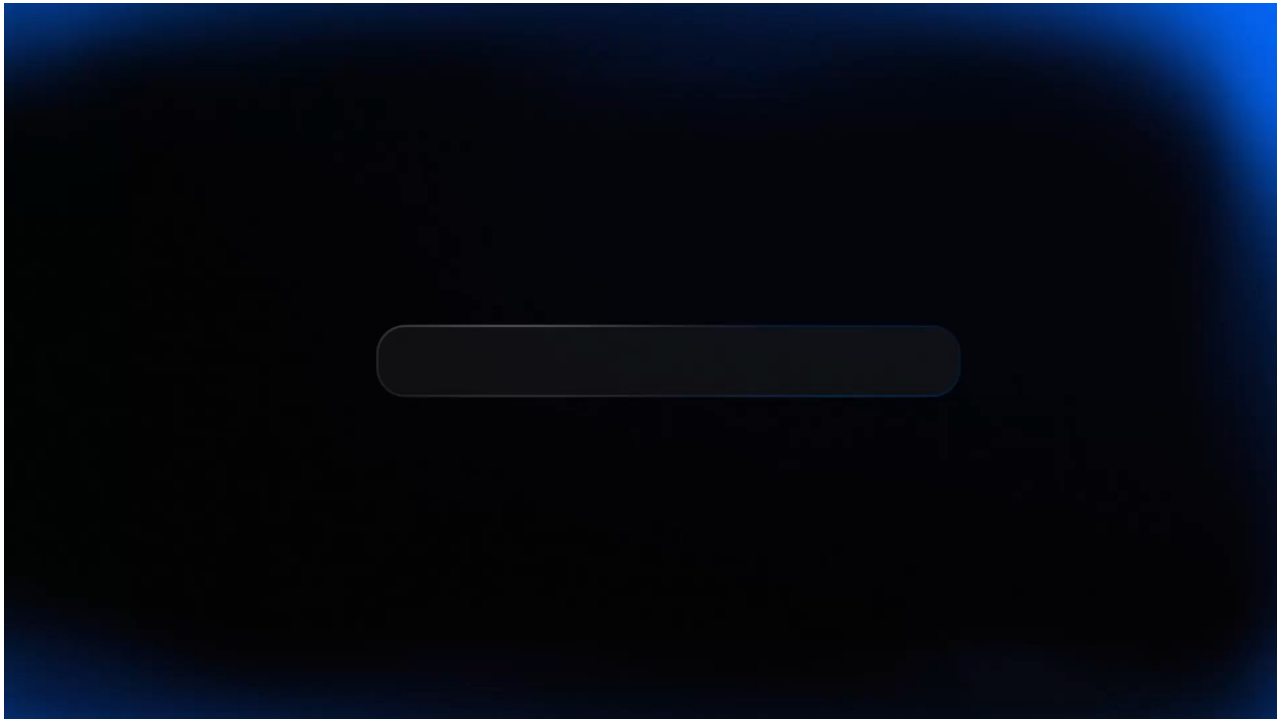


Ya no es fraude individual. Es crimen organizado en olas coordinadas

El **fraude agéntico** ocurre cuando un **agente de IA autónomo** ejecuta un ataque de identidad de principio a fin. Analiza las respuestas del sistema, adapta su estrategia y realiza nuevos intentos a escala, sin intervención humana en cada iteración.

Este ciclo adaptativo le permite atacar tanto el contenido presentado durante la verificación como el propio proceso de captura.

Miles de intentos automatizados hasta encontrar la grieta



El registro civil es el primer eslabón: su fuerza defiende todo el sistema

El documento con el que alguien abre una cuenta, contrata una línea o cobra un apoyo nació en un registro civil. Todo el ecosistema hereda la confianza (o el fraude) de ese primer trámite.

Identidad raíz

El acta de nacimiento es el único documento que no se puede verificar contra otro anterior. Ahí empieza la cadena.

Unicidad

Solo el padrón biométrico responde la pregunta clave: ¿esta persona ya está registrada con otro nombre?

Confianza en línea

La consulta contra el registro convierte esa unicidad en valor para bancos, telcos y servicios digitales.

Todo el ecosistema hereda lo que pasa en ese primer trámite.

El papel del estado

Podemos mitigar el fraude validando contra fuentes de verdad oficiales

SOLO VALIDACIÓN DE DATOS

El Estado valida los datos, pero no a la persona

El nombre, número de población y fecha de nacimiento coinciden con el padrón, pero un atacante puede combinarlos con un rostro y documento generados con IA.

VALIDACIÓN BIOMÉTRICA CONTRA EL REGISTRO ESTATAL

El Estado confirma al titular de la identidad

El rostro presentado se compara con el registro oficial para confirmar que corresponde a la persona identificada.

+99%

de reducción de fraude con documentos manipulados mediante IA entre clientes de Incode

Caso de éxito

Caso de éxito en EE.UU: Validación biométrica contra registros oficiales

GovFaceMatch compara el rostro directamente con registros estatales de EE. UU. para reforzar la detección de fraude sin afectar la experiencia del usuario.

1,000x

mayor detección de fraude que la verificación basada solo en datos

150x

más precisión que la verificación basada solo en documentos

20%

de conversión frente a flujos tradicionales, sin fricción adicional

La protección debe abarcar todo el ecosistema

Defensa en ecosistema

El fraude se muda al eslabón más débil: la defensa tiene que ser compartida

El mismo rostro sintético se prueba en un banco, en una telco y en una ventanilla de gobierno la misma semana. Cada institución lo ve como un caso aislado; el atacante lo ve como un intento con tres oportunidades.

Ninguna institución puede defenderse sola.

Registro civil

Es la fuente de verdad: define quién existe y garantiza que exista una sola vez.

Gobierno digital

Consume esa verdad para dar acceso a trámites, apoyos y servicios sin fricción ni suplantación.

Sector privado

Bancos, fintechs y telcos verifican contra el registro en lugar de confiar en el documento.

La protección debe abarcar todo el ecosistema



Gobierno
Fuente de verdad: confirma quién es cada ciudadano

Servicios digitales
Bancos, telcos y trámites que verifican contra el registro

Proveedor tecnológico
Aporta la tecnología; opera bajo contrato y auditoría

Ciudadano
Titular de la identidad: consiente y debe ser protegido

Organismo regulador
Fija estándares y sanciona el uso indebido de datos

Auditor externo
Verifica que los controles técnicos y legales se cumplan

La confianza se defiende en el primer trámite

01

El enrolamiento es irreversible

Las defensas se construyen desde el primer trámite, no se reparan después.

02

El Gobierno como fuente de verdad

Registro civil, identificaciones oficiales gubernamentales, registros de población, son la diferencia entre detección probabilística y verificación determinista.

03

Detectar redes, no casos

El crimen es organizado. La única defensa que escala es la que detecta olas, no incidentes sueltos.

04

Servicio biométrico confiable

La validación biométrica debe ser confiable y estar altamente disponible, el estándar de confianza nacional cuida a cada usuario.

XXIII ENCUENTRO CLARCIEV
HONDURAS 2026

Muchas gracias

GOBIERNO DE LA REPÚBLICA DE HONDURAS

RNP
JUNTOS SOMOS PATRIA

CLARCIEV
CONSEJO LATINOAMERICANO Y DEL CARIBE DE REGISTRO CIVIL, IDENTIDAD Y ESTADÍSTICAS VITALES

OEA

UNHCR ACNUR
La Agencia de la ONU para los Refugiados