



WHITE PAPER · IDENTIDAD DIGITAL · ECUADOR

La identidad en Ecuador después de las filtraciones

Por qué pedir una foto de la cédula dejó de probar algo en Ecuador, qué sí prueba el chip, y cómo distinguir lo uno de lo otro al comprar.

Tipo
White paper

País
Ecuador

Fecha
Octubre de 2026

Publica
ISM – Integral Social Media

EN ESTE DOCUMENTO

1 Resumen ejecutivo

2 Qué datos de identidad se filtraron en Ecuador

3 Por qué la verificación por fotografía ya no funciona

4 La cadena de confianza del chip ICAO 9303

5 Qué exige la LOPDP y qué sanciona

6 El costo del fraude de identidad

7 Cómo evaluar a un proveedor de verificación

8 Tres decisiones de diseño

9 Fuentes

Conversemos

1 Resumen ejecutivo

Cuatro afirmaciones, cada una con su fuente en la sección 9.

14,8 millones

de registros de identidad de ecuatorianos en foros clandestinos en mayo de 2026, con más de 10 millones de imágenes de cédula en alta resolución

+1.151%

de crecimiento de los ataques de inyección de video contra verificación facial en iOS, segundo semestre de 2025

hasta 1%

de la facturación del ejercicio anterior: la multa de la LOPDP por infracciones graves, vigente desde mayo de 2023

PRIMERO

Los datos de identidad de los ecuatorianos ya son públicos. La filtración de Novaestrat en 2019 expuso cerca de veinte millones de registros, entre ellos diecisiete millones de ecuatorianos y 6,7 millones de menores^[1]. En mayo de 2026 aparecieron en foros clandestinos **14,8 millones de registros de identidad y más de diez millones de imágenes de cédula en alta resolución**, junto con firmas y huellas dactilares^[2].

SEGUNDO

Por lo tanto, pedir esos datos ya no verifica a nadie. Un proceso que pide número de cédula, una foto del documento y una selfie está comprobando tres cosas que un atacante puede obtener o fabricar. El fraude de identidad en Ecuador subió 26% interanual, y el informe atribuye la causa directa a la debilidad de esos procesos^[5].

TERCERO

El atacante mejora más rápido que la defensa que lo mira. Los ataques de inyección de video contra verificación facial en iOS crecieron 1.151% en el segundo semestre de 2025, y los de cámara virtual nativa 2.665%^[6]. Toda defensa que consista en *mirar mejor* una imagen pierde terreno con cada generación de modelos.

CUARTO

Hay una prueba que no se degrada. El chip de una cédula o un pasaporte ICAO lleva una firma criptográfica del Estado emisor. Verificarla no requiere juzgar una imagen: requiere validar una firma. Un modelo generativo mejor no ayuda a falsificarla, porque lo que falta no es realismo sino la clave privada de un Estado.

2 Qué datos de identidad se filtraron en Ecuador

Tres hechos públicos, en orden.

2019 NOVAESTRAT ~20M de registros expuestos — 17M de ecuatorianos, 6,7M de ellos niños. Cédulas, núcleo familiar, datos tributarios y saldos bancarios.	2024–25 REGISTRO CIVIL Más de 3,5 millones de intentos de ataque informático reportados contra el Registro Civil.	Mayo 2026 FOROS CLANDESTINOS 14,8M de registros de identidad y más de 10M de imágenes de cédula en alta resolución — con huellas y firmas.
---	---	--

Una fotografía de un documento no prueba nada cuando el contenido de todos los documentos ya está publicado.

La brecha de 2019 fue descubierta en un servidor sin protección alojado en Miami y atribuido a una consultora ecuatoriana. Además del número de cédula, expuso composición familiar, historial educativo y laboral, información tributaria y saldos de cuentas de clientes de un banco ecuatoriano ^{[1][11]}. El Estado restringió el acceso al servidor y detuvo al responsable de la empresa.

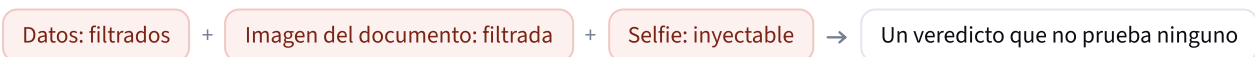
La de mayo de 2026 es cualitativamente peor. Lo publicado no fue solo texto: incluyó **más de diez millones de imágenes de documento en alta resolución, firmas y datos biométricos de huella**. El Registro Civil negó una vulneración directa de sus sistemas actuales y apuntó a fuentes externas o integraciones de terceros; la Superintendencia de Protección de Datos abrió una investigación ^[2].

Entre una y otra, el Registro Civil reportó más de **3,5 millones de intentos de ataque informático** entre 2024 y 2025 ^[3]. La conclusión operativa no depende de a quién se atribuya cada episodio: para quien diseña un proceso de verificación, **hay que asumir que el contenido de cualquier cédula ecuatoriana es obtenible**.

3 Por qué la verificación por fotografía ya no funciona

El problema no es la calidad de la revisión. Es qué se está revisando.

Un proceso de verificación documental por imagen le pide a la persona tres cosas: sus datos, una foto del documento y una selfie. Después revisa que la foto parezca un documento auténtico y que la cara se parezca a la del documento. Cada uno de esos tres insumos es, hoy en Ecuador, obtenible o fabricable.



Los datos están filtrados. Las imágenes de documento en alta resolución están filtradas — diez millones de ellas. Y la selfie es precisamente donde el atacante tiene la ventaja estructural: no necesita engañar a un ojo humano, necesita inyectar un video en el flujo de la cámara, que es un problema de software resuelto y en rápido crecimiento ^{[6][7]}.

El resultado es un proceso que se siente riguroso — hay pasos, hay una barra de progreso, hay un veredicto — y que en realidad certifica que quien está al otro lado sabe buscar en un foro. La Fiscalía registró **4.784 denuncias por suplantación de identidad** solo entre enero y octubre de 2025, concentradas en Guayas y Pichincha ^[4].

Conviene decir con precisión qué falla. No falla el modelo de detección: muchos son buenos. Falla la *premisa*. Un sistema que decide mirando una imagen compite contra un adversario cuyo único trabajo es producir mejores imágenes — y ese adversario mejora cada seis meses sin costo marginal.

4 La cadena de confianza del chip ICAO 9303

La diferencia entre juzgar una imagen y validar una firma.

CSCA	Autoridad Certificadora del País La clave raíz del Estado. Se publica y se intercambia entre países.
↓ firma	
DS	Firmante de Documentos Firma cada lote de documentos que el Estado emite.
↓ firma	
SOD	Objeto de Seguridad Lleva el hash de cada grupo de datos, firmado por el DS.
↓ firma	
DG1 / DG2	Grupos de Datos Nombre, fecha de nacimiento, número — y el retrato.

Cambia un solo byte de cualquier grupo de datos y su hash deja de coincidir con el objeto de seguridad firmado. Para falsificar eso hace falta la clave privada del Estado emisor — no un modelo generativo mejor.

La cédula ecuatoriana con chip y los pasaportes electrónicos ICAO llevan un chip sin contacto que sigue el estándar **ICAO 9303** — el mismo de las puertas automáticas de migración. Dentro hay grupos de datos: nombre y fecha de nacimiento en el DG1, el retrato en el DG2. Y hay un objeto de seguridad que contiene el hash de cada uno de esos grupos, firmado por el Estado emisor.

Validar eso se llama **Passive Authentication**, y no es una opinión: o la firma verifica contra el ancla de confianza del país emisor, o no verifica. Si alguien altera un solo byte de un grupo de datos, su hash deja de coincidir y la comprobación falla. Para producir un chip falso que pase, hace falta la clave privada del Estado.

El segundo cambio importante es *contra qué se compara la cara*. Comparar una selfie contra otra selfie enrolada al registrarse no ayuda si el atacante controla la cuenta desde el principio: enroló su propia cara. Comparar contra **el retrato que el Estado guardó dentro del chip firmado** es una afirmación distinta — dice que esta persona es el titular del documento, no que se parece a quien se registró.

5 Qué exige la LOPDP y qué sanciona

En Ecuador la exposición regulatoria ya no es teórica.

La Ley Orgánica de Protección de Datos Personales entró en vigencia en mayo de 2021 y dio dos años de adecuación. Desde **mayo de 2023 las sanciones administrativas están vigentes**: las infracciones leves se multan entre 0,1% y 0,7% de la facturación del ejercicio anterior, y las graves entre 0,7% y 1%^[8].

INFRACCIÓN	MULTA, COMO PORCENTAJE DE LA FACTURACIÓN DEL EJERCICIO ANTERIOR
Leve	0,1% – 0,7%
Grave	0,7% – 1%

Esto cambia la aritmética de una decisión que suele tomarse por inercia: **guardar la imagen del documento**. Un repositorio de cédulas escaneadas es un pasivo permanente, valorado como porcentaje de la facturación, mantenido para un trámite que ya terminó. Los datos biométricos son además categoría especial, con un estándar de consentimiento más alto.

La consecuencia de diseño es directa: **el mejor tratamiento de un dato sensible es no tenerlo**. Si el negocio necesita saber que alguien es mayor de edad, lo correcto es recibir un sí o un no — no una fecha de nacimiento, y desde luego no una fotografía del documento que la contiene.

6 El costo del fraude de identidad

Ecuador es un caso particular de un problema global.

ESTADOS UNIDOS · COMISIÓN FEDERAL DE COMERCIO · 2024^[9]

USD 12.500 millones

en pérdidas por fraude declaradas, +25%

1,1 millones+

reportes de robo de identidad

27% → 38%

víctimas que perdieron dinero

En Estados Unidos, la Comisión Federal de Comercio reportó **12.500 millones de dólares** en pérdidas por fraude declaradas en 2024, un 25% más que el año anterior, con más de 1,1 millones de reportes de robo de identidad^[9]. El dato interesante no es el total sino su composición: el número de reportes se mantuvo estable y lo que subió fue la proporción de víctimas que efectivamente perdió dinero, del 27% al 38%.

Es decir: no hay más intentos. Hay intentos que funcionan mejor. Esa es exactamente la firma de un adversario que mejoró sus herramientas, y coincide con el crecimiento medido de los ataques de inyección y de intercambio de rostro^[6].

En el plano local, el efecto se ve en cosas concretas y cotidianas: una sola banda engañó a alrededor de ochenta personas con ventas falsas de vehículos de alta gama antes de que once de sus integrantes fueran capturados en Guayaquil y Quito^[10].

7 Cómo evaluar a un proveedor de verificación de identidad

Ocho preguntas. Las respuestas separan una prueba criptográfica de una fotografía con pasos adicionales.

PREGÚNTALE AL PROVEEDOR	QUÉ TE DICE LA RESPUESTA
1. ¿Lee el chip, o fotografía el documento?	Si la respuesta es una fotografía — por bueno que sea el modelo que la revisa — el proveedor está inspeccionando datos que ya son públicos.
2. ¿Se verifica de verdad la firma del Estado emisor?	Leer un chip no es lo mismo que validarlo. Pregunta explícitamente por <i>Passive Authentication</i> y de dónde salen las anclas de confianza.
3. ¿Qué pasa cuando la verificación falla?	Debe fallar cerrado. Si igual entrega el dato con una confianza más baja, el «sí» no significa nada.
4. ¿Dónde se calcula la comparación biométrica?	¿En el dispositivo, o en sus servidores? La segunda respuesta crea una base de datos de rostros de la que ahora respondes tú.
5. ¿Contra qué se compara el rostro?	Una selfie enrolada al registrarse puede ser sustituida por quien controle la cuenta. El retrato dentro del chip, no.
6. ¿Puede devolver un solo dato en vez de un expediente?	Si la única salida es la identidad completa, la minimización es imposible y toda integración recoge de más por construcción.
7. ¿El consentimiento de datos y el de biometría son separados?	El consentimiento empaquetado para datos de categoría especial es el defecto de cumplimiento más común de este mercado.
8. ¿Qué se guarda, y por cuánto tiempo?	Pregunta qué queda almacenado después del veredicto. La respuesta correcta es corta, y no incluye la imagen del documento.

Un proveedor que responda bien las ocho puede aún no ser el adecuado. Un proveedor que no pueda responder las primeras cuatro te está vendiendo una fotografía.

8 Tres decisiones de diseño

Tres decisiones de diseño que se toman una vez y se viven durante años.

1

Verifica contra el chip, no contra la imagen

Si un proceso puede leer el chip, el resto de la discusión cambia de naturaleza — deja de ser detección de falsificaciones y pasa a ser validación de firmas.

2

Procesa la biometría en el dispositivo

No es solo una postura de privacidad: es lo que evita construir la base de datos de rostros que después hay que defender, y elimina el costo de servidor por verificación.

3

Recibe hechos, no expedientes

Diseña la integración para pedir la afirmación mínima que la decisión de negocio necesita. Lo que no se recibe no se almacena, no se filtra y no se sanciona.

9 Fuentes

- [1] Infosecurity Magazine — *Data of Virtually All Ecuadoreans Leaked Online* (2019)
<https://www.infosecurity-magazine.com/news/data-of-virtually-all-ecuadoreans/>
- [2] Infobae — *Casi 15 millones de datos de identidad de ecuatorianos aparecieron en redes y foros clandestinos* (6 de mayo de 2026)
<https://www.infobae.com/america/america-latina/2026/05/06/casi-15-millones-de-datos-de-identidad-de-ecuatorianos-aparecieron-en-redes-y-foros-clandestinos-autoridades-investigan-una-nueva-filtracion-masiva/>
- [3] Primicias — *Fraudes digitales en Ecuador se sofistican: aumentan estafas con IA y suplantación de identidad*
<https://www.primicias.ec/seguridad/fraudes-digitales-ecuador-118595/>
- [4] Radio Pichincha — *La suplantación de identidad golpea a Ecuador: más de 4.700 víctimas en 2025*
<https://www.radiopichincha.com/suplantacion-identidad-ecuador-victimas/>
- [5] La Nota en Línea — *Los fraudes con identidades falsas crecieron en un 26% en Ecuador* (Sumsub Identity Fraud Report 2025–2026)
<https://lanotaenlinea.com/los-fraudes-con-identidades-falsas-crecieron-en-un-26-en-ecuador/>
- [6] Biometric Update — *Biometric injection attack surge spreads to iOS: iProov report* (abril de 2026)
<https://www.biometricupdate.com/202604/biometric-injection-attack-surge-spreads-to-ios-iproov-report>
- [7] iProov — *Threat Intelligence Report 2025: Remote Identity Under Attack*
<https://www.iproov.com/reports/threat-intelligence-report-2025-remote-identity-attack>
- [8] Primicias — *Multas por la Ley de Protección de Datos comenzarán en mayo* (LOPDP)
<https://www.primicias.ec/noticias/economia/ley-proteccion-datos-personales-sanciones/>
- [9] Federal Trade Commission — *New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024*
<https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
- [10] Expreso — *Estafa en venta de vehículos: capturan a presunta banda que engañó a 80 personas*
<https://www.expreso.ec/guayaquil/estafa-venta-vehiculos-capturan-presunta-banda-engano-80-personas-236796.html>
- [11] Fast Company — *The personal data of almost everyone in Ecuador has been leaked*
<https://www.fastcompany.com/90404473/the-personal-data-of-almost-everyone-in-ecuador-has-been-leaked>

Cada cifra citada en este documento está enlazada a su fuente. Cuando la fuente es una nota de prensa sobre un estudio privado, se nombra el estudio. Las cifras se comprobaron el 30 de agosto de 2026; compruébalas otra vez antes de apoyarte en ellas.



Conversemos

Analicemos tu caso. Banca, telco, apuestas, marketplace o sector público — el análisis cambia bastante según qué decisión tenga que soportar la verificación.

ism.ec/es/contact · info@ism.ec · ism.ec/es/id-protekt

ISM – Integral Social Media · VISITEC VISION Y TECNOLOGIA S.A. · Quito, Ecuador