



WHITE PAPER • DIGITAL IDENTITY • ECUADOR

Identity in Ecuador after the leaks

Why asking for a photo of an ID stopped proving anything in Ecuador, what the chip does prove, and how to tell the two apart when you're buying.

Type
White paper

Country
Ecuador

Date
October 2026

Publisher
ISM – Integral Social Media

IN THIS PAPER

1 Executive summary

2 Which Ecuadorian identity data leaked

3 Why photo-based verification no longer works

4 The ICAO 9303 chip chain of trust

5 What the LOPDP requires, and what it fines

6 The cost of identity fraud

7 How to evaluate an identity-verification vendor

8 Three design decisions

9 Sources

Talk to us

1 Executive summary

Four claims, each with its source in section 9.

14.8 million

Ecuadorian identity records on dark forums in May 2026, with over 10 million high-resolution ID images

+1,151%

growth in video-injection attacks against face verification on iOS, second half of 2025

up to 1%

of the prior year's turnover: the LOPDP fine for serious infringements, live since May 2023

FIRST

Ecuadorians' identity data is already public. The 2019 Novaestrat leak exposed roughly twenty million records, including seventeen million Ecuadorians and 6.7 million children^[1]. In May 2026, **14.8 million identity records and more than ten million high-resolution ID images** appeared on dark forums, together with signatures and fingerprint data^[2].

SECOND

Asking for that data therefore verifies nobody. A process that requests an ID number, a photograph of the document and a selfie is checking three things an attacker can obtain or fabricate. Identity fraud in Ecuador rose 26% year over year, and the report attributes it directly to the weakness of those processes^[5].

THIRD

The attacker improves faster than the defence watching them. Video-injection attacks against face verification on iOS grew 1,151% in the second half of 2025, and native virtual-camera attacks 2,665%^[6]. Any defence that consists of *looking harder* at an image loses ground with every generation of models.

FOURTH

There is one proof that does not degrade. The chip in a national ID or an ICAO passport carries a cryptographic signature from the issuing state. Verifying it does not require judging an image; it requires validating a signature. A better generative model does not help forge one, because what is missing is not realism — it is a state's private key.

2 Which Ecuadorian identity data leaked

Three matters of public record, in order.

2019

NOVAESTRAT

~20M records exposed — 17M Ecuadorians, 6.7M of them children. Cédulas, family records, tax and bank balances.

2024–25

REGISTRO CIVIL

More than 3.5 million attempted cyberattacks reported against the Civil Registry.

May 2026

DARK FORUMS

14.8M identity records and over 10M high-resolution ID images — with fingerprints and signatures.

A photograph of a document proves nothing once the contents of every document are already published.

The 2019 breach was found on an unsecured server hosted in Miami and attributed to an Ecuadorian consultancy. Beyond ID numbers, it exposed family composition, education and employment histories, tax information, and the account balances of customers of an Ecuadorian bank ^{[1][11]}. The state restricted access to the server and detained the company's manager.

The May 2026 event is qualitatively worse. What was published was not only text: it included **more than ten million high-resolution document images, signatures and fingerprint biometrics**. The Civil Registry denied a direct breach of its current systems and pointed to external sources or third-party integrations; the data-protection regulator opened an investigation ^[2].

Between the two, the Civil Registry reported more than **3.5 million attempted cyberattacks** across 2024 and 2025 ^[3]. The operational conclusion does not depend on who is blamed for which episode: anyone designing a verification process must **assume the contents of any Ecuadorian ID are obtainable**.

3 Why photo-based verification no longer works

The problem isn't the quality of the review. It's what is being reviewed.

An image-based document check asks a person for three things: their details, a photograph of their document, and a selfie. It then checks that the photograph looks like a genuine document and that the face resembles the one on it. In Ecuador today, each of those three inputs is obtainable or fabricable.

Details: leaked + Document image: leaked + Selfie: injectable → A verdict that proves none of them

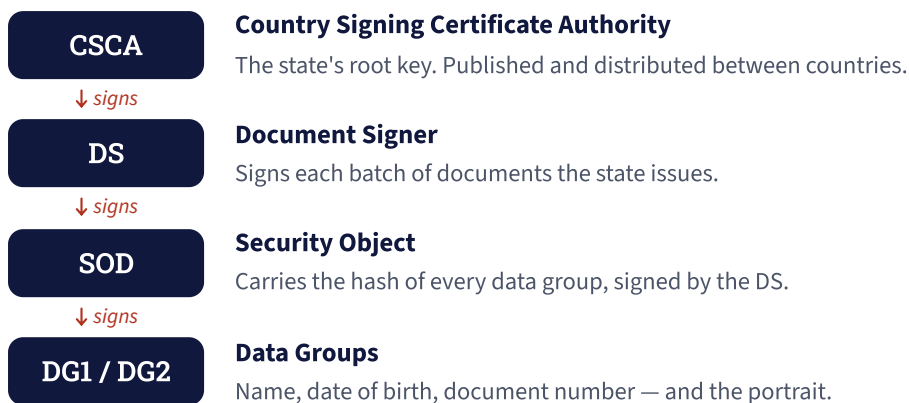
The details are leaked. The high-resolution document images are leaked — ten million of them. And the selfie is precisely where the attacker holds the structural advantage: they do not need to fool a human eye, they need to inject a video into the camera stream, which is a solved and rapidly growing software problem ^{[6][7]}.

The result is a process that feels rigorous — there are steps, a progress bar, a verdict — and that in practice certifies that whoever is on the other end knows how to search a forum. Ecuador's Attorney General recorded **4,784 identity-imper-sonation complaints** between January and October 2025 alone, concentrated in Guayas and Pichincha ^[4].

It is worth being precise about what fails. The detection model does not fail: many are good. The *premise* fails. A system that decides by looking at an image competes against an adversary whose only job is producing better images — and that adversary improves every six months at no marginal cost.

4 The ICAO 9303 chip chain of trust

The difference between judging an image and validating a signature.



Change one byte of any data group and its hash stops matching the signed security object. To forge that, an attacker needs the issuing state's private key — not a better generative model.

Ecuador's chip cédula and ICAO e-passports carry a contactless chip following the **ICAO 9303** standard — the same one used at automated border gates. Inside are data groups: name and date of birth in DG1, the portrait in DG2. And there is a security object holding the hash of each of those groups, signed by the issuing state.

Validating that is called **Passive Authentication**, and it is not an opinion: either the signature verifies against the issuing country's trust anchor, or it does not. Alter a single byte of a data group and its hash stops matching, and the check fails. Producing a forged chip that passes requires the state's private key.

The second important change is *what the face is matched against*. Comparing a selfie to another selfie enrolled at signup does not help if the attacker controlled the account from the start: they enrolled their own face. Comparing against **the portrait the state placed inside the signed chip** is a different claim — it says this person is the document's holder, not that they resemble whoever registered.

5 What the LOPDP requires, and what it fines

In Ecuador the regulatory exposure is no longer theoretical.

The Organic Law on Personal Data Protection came into force in May 2021 and allowed two years to comply. Since **May 2023 administrative sanctions have been live**: minor infringements are fined between 0.1% and 0.7% of the prior year's turnover, and serious ones between 0.7% and 1% ^[8].

INFRINGEMENT	FINE, AS A SHARE OF THE PRIOR YEAR'S TURNOVER
Minor	0.1% – 0.7%
Serious	0.7% – 1%

That changes the arithmetic of a decision usually made out of habit: **keeping the document image**. A repository of scanned IDs is a permanent liability, priced as a percentage of turnover, retained for a process that already finished. Biometric data is additionally special-category, carrying a higher consent standard.

The design consequence is direct: **the best way to handle sensitive data is not to hold it**. If the business needs to know someone is an adult, the right thing to receive is a yes or a no — not a date of birth, and certainly not a photograph of the document containing one.

6 The cost of identity fraud

Ecuador is a particular case of a global problem.

UNITED STATES · FEDERAL TRADE COMMISSION · 2024 ^[9]

\$12.5 billion

reported fraud losses, up 25%

1.1 million+

identity-theft reports

27% → 38%

share of victims who lost money

In the United States, the Federal Trade Commission reported **\$12.5 billion** in fraud losses for 2024, up 25% on the prior year, with more than 1.1 million identity-theft reports ^[9]. The interesting datum is not the total but its composition: the number of reports stayed flat, and what rose was the share of victims who actually lost money — from 27% to 38%.

In other words: there are not more attempts. There are attempts that work better. That is exactly the signature of an adversary whose tooling improved, and it matches the measured growth in injection and face-swap attacks ^[6].

Locally, the effect shows up in concrete, everyday things: a single ring defrauded around eighty people with fake luxury-vehicle sales before eleven of its members were arrested in Guayaquil and Quito ^[10].

7 How to evaluate an identity-verification vendor

Eight questions. The answers separate cryptographic proof from a photograph with extra steps.

ASK THE VENDOR	WHAT THE ANSWER TELLS YOU
1. Does it read the chip, or photograph the document?	If the answer is a photograph — however good the model checking it — the vendor is inspecting data that is already public.
2. Is the issuing state's signature actually verified?	Reading a chip is not the same as validating it. Ask specifically about Passive Authentication and where the trust anchors come from.
3. What happens when verification fails?	It must fail closed. If unverified data is still passed on with a lower confidence score, the “yes” means nothing.
4. Where is the biometric comparison computed?	On the device, or on their servers? The second answer creates a database of faces that you are now responsible for.
5. What is the face matched <i>against</i> ?	A selfie enrolled at signup can be replaced by an attacker who controls the account. The portrait inside the chip cannot.
6. Can it return a single fact instead of a record?	If the only output is a full identity payload, minimization is impossible and every integration over-collects by construction.
7. Are consent for data and consent for biometrics separate?	Bundled consent for special-category data is the most common compliance defect in this market.
8. What is kept, and for how long?	Ask what is stored after the verdict. The right answer is short, and it does not include the document image.

A vendor who answers all eight well may still be the wrong fit. A vendor who cannot answer the first four is selling a photograph.

8 Three design decisions

Three design decisions taken once and lived with for years.

1

Verify against the chip, not the image

If a process can read the chip, the rest of the discussion changes in kind — it stops being forgery detection and becomes signature validation.

2

Process biometrics on the device

This is not only a privacy posture: it is what avoids building the database of faces you then have to defend, and it removes the per-verification server cost.

3

Receive facts, not files

Design the integration to request the minimum claim the business decision needs. What you never receive cannot be stored, cannot leak, and cannot be fined.

9 Sources

- [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 May 2026)
<https://www.infobae.com/america/america-latina/2026/05/06/casi-15-millones-de-datos-de-identidad-de-ecuadorianos-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* (Sumsu 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* (April 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* (LOPD)
<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>

Every figure quoted in this paper is linked to its source. Where a source is a news report of a private-sector study, the study is named. Figures were checked on 30 August 2026; check them again before relying on them.



Talk to us

Let's work through your case. Banking, telco, betting, marketplace or public sector — the analysis shifts a good deal depending on which decision the verification has to carry.

ism.ec/contact · info@ism.ec · ism.ec/id-protect

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