

LATIN AMERICA | IDENTITY VERIFICATION

# Enterprise Guide to Docless Identity Verification in Latin America

How to reduce onboarding friction, verify customers against authoritative sources, and adapt one identity flow across LATAM region including Brazil, Mexico, Argentina, Colombia, Chile, and Peru.



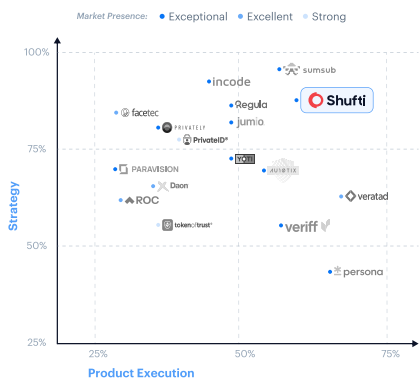


# Industry Recognition 2025–2026

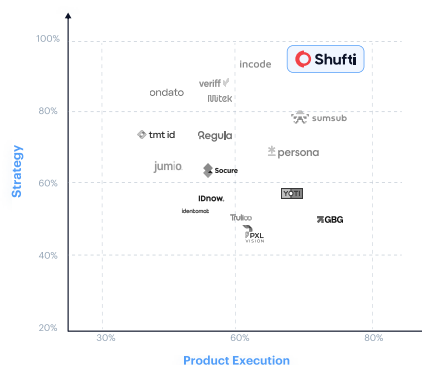
Recognised by leading analyst firms, government bodies and independent research organisations



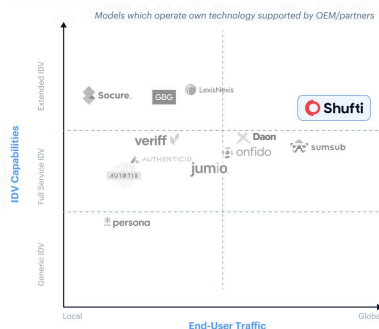
**Ranked Exceptional in Liminal's 2026 Age Estimation Index**



**Ranked Exceptional in Liminal's 2026 Age Verification Index**



**Broadest global reach in the 2025 KuppingerCole Extended IDV report**



**Recognised as a Leader across four G2 Summer 2026 reports**



**Differentiated by Gartner on document diversity and country coverage**



**240+**  
Countries  
& Territories

**10k+**  
Document  
Types



**First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER**

**iBeta Level 3  
Conformance**  
0% APCER



**Ranked Top 5 in the DHS RIVR 2025 for identity validation**

**0%**  
Extraction  
Failure

**0.67%**  
Worst-Case  
FNMR





|           |                                                                                            |           |
|-----------|--------------------------------------------------------------------------------------------|-----------|
| <b>ES</b> | <b>Executive summary and introduction</b>                                                  | <b>03</b> |
|           | The argument, and the three docless methods in one line each                               |           |
| <b>01</b> | <b>What Six Major Markets Reveal About Scaling Onboarding Across Latin America</b>         | <b>07</b> |
|           | Brazil, Mexico, Argentina, Colombia, Chile, and Peru, a priority set inside a wider region |           |
| <b>02</b> | <b>The Identity Infrastructure Shaping Docless Verification Across Latin America</b>       | <b>09</b> |
|           | Account ownership, registry coverage, and the national digital-identity layer              |           |
| <b>03</b> | <b>Six Market Models for Docless Verification Across Latin America</b>                     | <b>13</b> |
|           | One comparable card per market — Brazil, Mexico, Argentina, Colombia, Chile, Peru          |           |
| <b>04</b> | <b>The Regulatory and Data Patterns Businesses Will Encounter Across Latin America</b>     | <b>25</b> |
|           | Six regulators converging, and the honest nuance on data residency                         |           |
| <b>05</b> | <b>The sectors under most onboarding pressure</b>                                          | <b>29</b> |
|           | Fintech and crypto lead, four more verticals follow                                        |           |
| <b>06</b> | <b>Why Regional Coverage Claims Often Break Down at the Local-Market Level</b>             | <b>32</b> |
|           | The deployment gap, the reach gap, and the seven-question checklist                        |           |
| <b>07</b> | <b>Docless onboarding via government registries and national eID</b>                       | <b>34</b> |
|           | Three methods, risk routing, and why a live bind beats a big registry                      |           |
| <b>08</b> | <b>The Identity Foundation Needed to Expand Across Diverse Latin American Markets</b>      | <b>39</b> |
|           | One integration, routing per user, deployable where the data must live                     |           |
| <b>09</b> | <b>The Assurance Evidence Your Compliance and Security Teams Will Ask For</b>              | <b>41</b> |
|           | Coverage proof points and the certifications a reviewer looks for                          |           |
| <b>FQ</b> | <b>The Questions Your Compliance, Product, and Risk Teams Will Ask</b>                     | <b>42</b> |
|           | Legality, methods, fallback, and change management                                         |           |
| <b>RF</b> | <b>References</b>                                                                          | <b>44</b> |
|           | Numbered sources behind every figure                                                       |           |

# Verify More Genuine Customers on the First Attempt

Remote onboarding has become the default way to open a financial account across Latin America, and the region is adding first-time account holders faster than anywhere else. Every one of those accounts needs an identity check, yet most onboarding flows still lead with a document upload. That is the step where genuine users abandon most often, and it is now the step that generative-AI fraud is built to beat.

What sets the region apart is the source a business checks a person against. It is usually not a private data broker but the government's own biometric civil registry, and in several markets that registry already runs as a verification service a regulated business can call. Regulators are now writing biometric verification against those registries into their onboarding rules.

The opportunity is real, and so is the complexity, because the six priority markets in this guide each bring their own registry, financial regulator, AML statute, and data-protection regime. Five of the six changed or are changing that data law between 2024 and 2026. The practical conclusion is that verifying against authoritative government data, with document checks kept as an automatic fallback, converts better and defends better than a document-first flow, as long as the approach can reach each market on its own terms.



## Three Ways to Remove Document Friction—Without Removing Identity Assurance

### METHOD 01

#### Passive verification

A match of the applicant's details against authoritative government, credit, telecom, or utility data.

### METHOD 02

#### Active verification

The applicant authenticates with a national digital-identity credential they already hold.

### METHOD 03

#### Biometrically Enriched

A live selfie is bound to the photo held by the source record.

### DOCUMENT FALLBACK

Document verification stays in the flow as the automatic fallback, so no genuine user is lost.

# Every Failed First Attempt Costs Conversion, Time, and Compliance Resources

The first attempt to verify a customer is the one that decides the economics. When an identity confirms on the first pass, the customer moves straight into the product and the compliance record is complete from the outset. When it fails, a share of genuine applicants walk away, a manual review queue forms, and the same regulatory duty gets discharged twice at higher cost.

Latin America adds a twist that document-first markets like the US and UK lack. Across the six markets in this guide, the source a business verifies a person against is, more often than not, the state's own biometric civil registry. RENIEC in Peru, RENAPER in Argentina, the CPF base and gov.br in Brazil, INE and RENAPO in Mexico, the Registraduría in Colombia and the Registro Civil in Chile are not credit bureaus assembled into a proxy for identity. They are state civil registries, most of them holding fingerprints and facial images, several of them exposing identity-validation web services to banks, fintechs, and telcos. A no-upload check against the government record is not a workaround the regulator grudgingly tolerates here. It is the grain of how the region built its identity infrastructure, and regulators are now actively pushing onboarding toward it.

That is the opportunity. The complication is that these six do not behave as a single market. Latin America built strong government identity registries and instant-payment rails that rank among the world's most used, both in the same decade, and it is now onboarding the previously unbanked in numbers no other region matches. Every new account needs an identity check, and the source it would check against sits behind six different doors. Six national registries, six financial regulators and AML statutes, and six data-protection regimes, five of which either rewrote or are rewriting their law between 2024 and 2026. A flow tuned for one market does not clear the next.

The document upload, the habit most onboarding flows still default to, now carries two problems at once. It is the highest-friction step, where genuine users quit. And it is the weakest security control, because generative AI produces convincing fake identity documents and injected faces cheaply, at the exact moment onboarding volume and regulation are peaking. This guide is about closing that gap. It means verifying low-risk users against the authoritative data the region already runs, binding a live face to the government record where synthetic identity and deepfakes are the threat, and keeping the document flow for the cases that genuinely need it.

## What You Will Be Able to Decide After Reading This Guide

**01** What Six Major Markets Reveal About Scaling Onboarding Across Latin America

**02** The Identity Infrastructure Shaping Docless Verification Across Latin America

**03** Six Market Models for Docless Verification Across Latin America

**04** The Regulatory and Data Patterns Businesses Will Encounter Across Latin America

**05** The sectors under most onboarding pressure

**06** Why Regional Coverage Claims Often Break Down at the Local-Market Level

**07** Docless onboarding via government registries and national eID

**08** The Identity Foundation Needed to Expand Across Diverse Latin American Markets

**09** The Assurance Evidence Your Compliance and Security Teams Will Ask For



# What Six Major Markets Reveal About Scaling Onboarding Across Latin America

Latin America runs to roughly twenty countries, and this guide goes deep on the six that carry the most onboarding volume, fraud pressure, and registry strength, Brazil, Mexico, Argentina, Colombia, Chile, and Peru. They are the region's largest economies, together roughly 80 percent of its economic output, and its most active digital-onboarding markets. The same docless approach carries to the rest of the region, so going deep on these six sets a pattern rather than a boundary. The reason to treat them as six markets, and not as one Latin American market, is that the seams run exactly where an onboarding flow has to work.

Each market has its own national identifier and civil registry, from Brazil's CPF to Peru's DNI. Each has its own national digital identity too, and they sit at very different stages, from Brazil's gov.br at more than 160 million accounts to Mexico's Llave MX, which authenticates with little more than a CURP, an email, and a phone number. The financial regulator, the AML statute, the posture on remote onboarding, and the data-protection law all change at the border as well. A flow tuned for Brazil's CPF and gov.br will not clear Mexico's new CNBV biometric rule, Argentina's RENAPER agreement and live-human liveness requirement, or Peru's shifting RENIEC access model.



SIX PRIORITY MARKETS WITHIN A WIDER REGION.

The same registry-first pattern already operates well beyond the six. Government identity rails are commercially reachable today in Guatemala, Bolivia, El Salvador, and Panama, and Panama has moved first on wallet credentials, launching a Tribunal Electoral identity wallet in October 2024 and a digital driver's licence in May 2026. El Salvador's civil registry reports 5.8 million currently valid DUIs. The point of naming them is that the six are a priority set inside a wider region running the same play, not the whole of it.

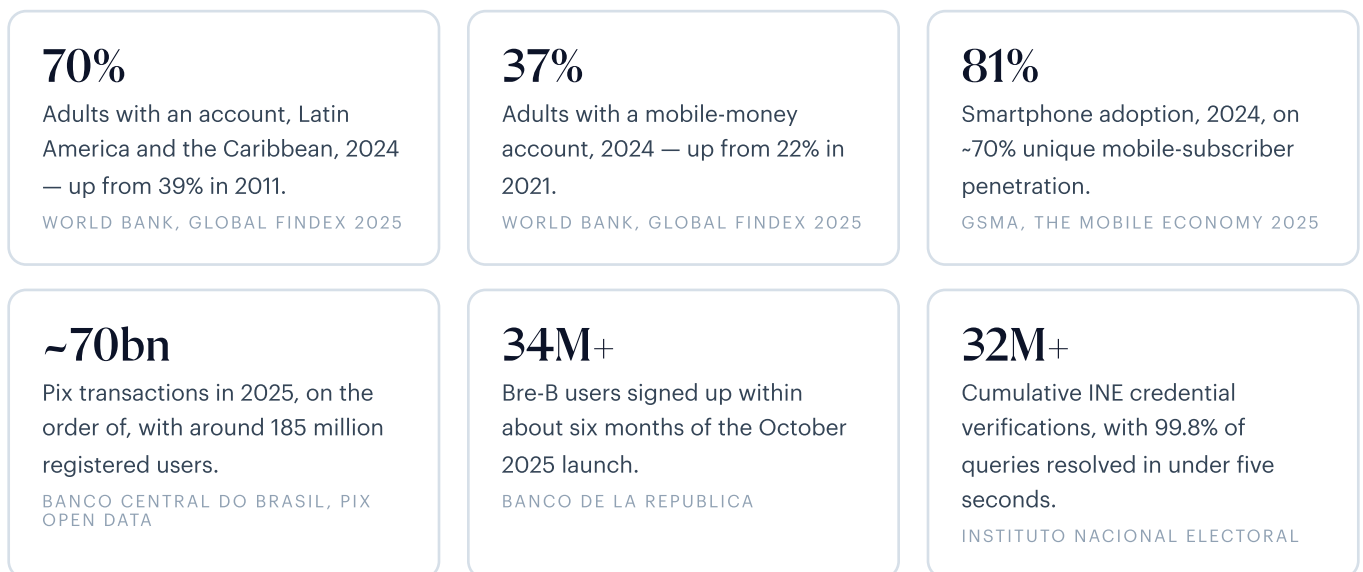
This is also why the guide serves two readers at once. Product, growth, and onboarding leaders feel the drop-off and the inclusion opportunity. Compliance and AML leaders feel the fraud, the AML obligation, and the new biometric mandates. They own the same decision to change the flow, and the same docless approach answers both. The rest of this guide sets out, market by market, what the source is, what the regulator permits, and where the data is allowed to sit.

# The Identity Infrastructure Shaping Docless Verification Across Latin America

The region's distinctive asset is the backbone this section maps. In most of Latin America, the authoritative identity source is a state civil registry that holds the citizen's biometrics, and in several markets that registry runs as a verification service a regulated business can call. Two neutral measures frame the opportunity, and the registry anchors underneath them are the reason docless works here.

Account ownership across Latin America and the Caribbean reached about 70 percent of adults in 2024, up from 67 percent in 2021 and 39 percent in 2011 (World Bank, Global Findex 2025). Mobile-money accounts reached 37 percent of adults in 2024, up from 22 percent in 2021, which is the wallet-led inclusion wave in a single number. The phone-first base underneath it is broad, with Latin America running about 70 percent unique mobile-subscriber penetration and 81 percent smartphone adoption in 2024 (GSMA, The Mobile Economy 2025).

FIG. 01 — THE OPPORTUNITY IN SIX NUMBERS



Per market, account ownership in 2024 ran roughly Brazil 86 percent, Chile 85 percent, Argentina 82 percent, Peru 59 percent, Colombia 57 percent, and Mexico 53 percent (World Bank, Global Findex 2025). Read that alongside the registries and a pattern appears. The still-unbanked share is largest in Mexico, Colombia, and Peru, which is exactly where remote-onboarding volume is growing fastest, and where the government source matters most, because these are first-time accounts with no prior banking footprint to lean on.

**FIG. 02 — ACCOUNT OWNERSHIP ACROSS THE SIX, 2024**  
% OF ADULTS



SOURCE: WORLD BANK, GLOBAL FINDEX 2025.



FIG. 03 — THE IDENTITY BACKBONE, SIX MARKETS

| Market                                                                                                       | Account ownership 2024 | Registry holds biometrics | Government ID-validation service                                        | National eID and maturity                                     |
|--------------------------------------------------------------------------------------------------------------|------------------------|---------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------|
| <a href="#">Brazil</a>      | 86%                    | ● Yes                     | <b>Serpro Datavalid</b><br>Biographic and biometric modes               | <b>gov.br</b><br>Mature — 160M+ accounts, biometric gold tier |
| <a href="#">Mexico</a>      | 53%                    | ● Yes                     | <b>INE verification service</b><br>Data, fingerprint, and facial checks | <b>Llave MX</b><br>Thin — services-access layer               |
| <a href="#">Argentina</a>   | 82%                    | ● Yes                     | <b>RENAPER SID</b><br>Data, fingerprint, and facial validation          | <b>DNI in Mi Argentina</b><br>Narrower                        |
| <a href="#">Colombia</a>  | 57%                    | ● Yes                     | <b>RNEC biometric service</b><br>Authorized public and private entities | <b>Autenticacion Digital Ciudadana</b><br>Present             |
| <a href="#">Chile</a>     | 85%                    | ● Yes                     | <b>Brokered</b><br>No single open government match API yet              | <b>ClaveUnica</b><br>Mature — newly open to private sector    |
| <a href="#">Peru</a>      | 59%                    | ● Yes                     | <b>RENIEC</b><br>2026 transition — see market card                      | <b>ID Peru</b><br>Narrower                                    |

SOURCES: WORLD BANK GLOBAL FINDEX 2025; NATIONAL REGISTRIES AND GOVERNMENT SERIES AS CITED IN SECTIONS 03-04.

The registry coverage underneath is close to total, and it is measurable in each market's own official series. Peru's RENIEC reports 37.15 million identified people, of whom 25.9 million are adults, and issued more than 8 million DNIs in 2025, its highest annual volume in six years (RENIEC). Mexico's INE electoral roll holds roughly 100 million citizens with a current voter credential (INE). Colombia's 2026 electoral census enabled 41.42 million citizens to vote (Registraduria). Brazil's CNH do Brasil digital driver's-licence app passed 40 million users, and the CPF base is effectively universal, a point Section 08 returns to because the registry actually holds more records than the country has living residents.

FIG. 04 — REGISTRY-COVERAGE REFERENCE



The rest of the backbone is the national digital identity layer, and the region genuinely has all three docless modes live, which is not true everywhere. Brazil's gov.br and Chile's ClaveUnica are mature national logins. Peru's ID Peru and the DNI electronico, and Argentina's DNI in the Mi Argentina app, are real but narrower. Mexico's Llave MX is still a services-access layer rather than a high-assurance credential. The two methods that do the most work in this region are Passive verification against government registries and biometric binding against government records, because those are the region's distinctive assets and the direct answer to its fraud. Active national-eID login is genuinely strong in Brazil and Chile, and the market deep-dives that follow say plainly where it is and is not ready.

# Six Market Models for Docless Verification Across Latin America

Brazil, Mexico, Argentina, Colombia, Chile, and Peru illustrate the different identity rails, regulatory approaches, and levels of digital-ID readiness businesses may encounter across the wider region. Each market profile covers the core identifier and registry, authoritative data sources, remote-onboarding basis, data-protection requirements, and the payments and crypto context, while clearly flagging developments still evolving in 2026.

## Brazil

---

### IDENTIFIER AND REGISTRY

The CPF is now the single national identification number across all levels of government (Lei 14.534/2023). The new Carteira de Identidade Nacional (CIN) carries the CPF as its number, with a QR code, a machine-readable zone, and an embedded ICP-Brasil digital certificate, issued by state institutes that collect fingerprints and a facial photo. A national biometric database, the Identificacao Civil Nacional (Lei 13.444/2017), sits on the electoral biometric base run by the TSE.

---

### NATIONAL DIGITAL IDENTITY

gov.br is the national login, at more than 160 million registered accounts, with three assurance tiers. Bronze validates self-declared data against government databases, Prata adds document or biometric validation with MFA, and Ouro requires a civil-ID plus a biometric match against government databases, or a digital certificate. More than 100 million accounts were already Prata or Ouro by mid-2025. A separate government app, CNH do Brasil (formerly the Carteira Digital de Transito, renamed in December 2025), carries the digital driver's licence and passed 40 million users, which makes it one of the most widely held digital credentials in the country.

---

### GOVERNMENT EKYC ENABLER

Serpro Datavalid, the government-owned identity-validation API, verifies a person against official federal databases in two modes, biographic and biometric, the second returning a fingerprint and facial-photo comparison against the government base. This is the core docless enabler. A contract requires a corporate digital certificate (e-CNPJ). Open Finance Brasil adds bank-sourced data for passive checks.

---

## **REGULATOR AND REMOTE- ONBOARDING BASIS**

The AML statute is Lei 9.613/1998. The financial intelligence unit, COAF, sits within the Ministério da Fazenda (it was briefly attached to the Banco Central in 2020–22 before MP 1.158/2023 moved it back), while the Banco Central supervises AML compliance at the institutions it licenses. Remote onboarding is expressly permitted, because CMN Resolution 4.753/2019 allows account opening through electronic, non-presential channels. Securities-market AML sits in CVM Resolution 50/2021.

---

## **DATA PROTECTION AND RESIDENCY**

The LGPD (Lei 13.709/2018) makes biometric data sensitive, and the authority is the ANPD. International transfers run under Resolucao CD/ANPD 19/2024 with standard contractual clauses. There is no general localization mandate.

---

## **PAYMENTS AND CRYPTO**

Pix, operated by the Banco Central, is systemic: about 80 billion transactions in 2025, used by 148 million individuals — 86 percent of adults — and 12.8 million businesses in December 2025 alone (Banco Central do Brasil, Relatório de Gestão do Pix 2023–2025). The crypto framework is Lei 14.478/2022, with the Banco Central as regulator. The operative rulebook for virtual-asset providers (BCB Resolutions 519, 520, and 521/2025) imposes full KYC and AML duties from early 2026. Brazil is the region's largest crypto market by on-chain value received (Chainalysis, an analytics firm, industry data).

---

#### DOCLESS READ

Brazil is the region's most complete docless market, a single national number, a mature national login with a biometric gold tier, and a government biometric-match API, all under an explicit remote-onboarding rule.

## Mexico

---

### IDENTIFIER AND REGISTRY

The CURP, an 18-character code issued by RENAPO within SEGOB, is the universal population identifier. The INE voter credential is the most widely held physical ID and the primary object of KYC. A 2025 reform created a biometric CURP (fingerprints plus facial photo) administered through a new Plataforma Unica de Identidad, but that platform is only partially operational and the mandate faces active legal challenge through individual amparo suspensions in 2026. Treat the biometric CURP as a coming rail, not a dependable one yet.

---

### NATIONAL DIGITAL IDENTITY

Llave MX, rolled out during 2025, authenticates with CURP plus email plus phone. It is a government-services access layer, not a high-assurance biometric credential, so a mature national eID login for private-sector KYC does not yet exist in Mexico.

---

### GOVERNMENT EKYC ENABLER

The workhorse is the INE Servicio de Verificacion de Datos de la Credencial para Votar, which supports data, fingerprint, and facial checks, resolves 99.8 percent of queries in under five seconds and handled 32.4 million verifications in May 2026 alone, roughly a million a day, on top of more than 60 million a year since 2022 (Instituto Nacional Electoral, June 2026). till Naciol Electoral

---

### REGULATOR AND REMOTE- ONBOARDING BASIS

The regulators are the CNBV for banks, fintechs, and securities, Banxico for payments, and the UIF for AML. The Ley Fintech (2018) licenses electronic-payment and crowdfunding institutions. The AML law, LFPIORPI, was reformed in July 2025 to add virtual-asset and cross-border activities.



## 2026 DEVELOPMENT

The headline 2026 development is a CNBV resolution published in the Diario Oficial de la Federacion on 1 July 2026. It makes facial-biometric verification, matched at 90 percent or better against government records (the INE voter credential and the SRE passport), mandatory for higher-tier account operations and high-value transactions, with a standing prohibition on selling or transferring the biometric data. This governs biometric authentication of higher-tier operations rather than new-client onboarding as such, a distinction the compliance reader should hold onto.

## DATA PROTECTION AND RESIDENCY

The regime was rebuilt in 2025. The old authority INAI was eliminated by constitutional reform, and a new LFPDPPP took force in March 2025, with the Secretaria Anticorrupcion y Buen Gobierno as the authority. Biometric data is sensitive. Cross-border transfer is permitted with consent or statutory exceptions. There is no general localization mandate, though the CNBV regime bars transfer or sale of financial biometric data.

## PAYMENTS AND CRYPTO

Banxico runs SPEI for real-time interbank transfers, plus CoDi and DiMo. Banxico Circular 4/2019 bars banks and fintechs from offering crypto to the public, so retail crypto runs through independent providers that are AML-obligated under LFPIORPI. Mexico is the region's remittance anchor, at a record near 64.7 billion US dollars in 2024 (Banco de Mexico), a corridor where stablecoin use is growing.

## DOCLESS READ

Mexico's passive rail already exists and is fast, the INE service with more than 32 million checks. The regulator is now pushing government-matched biometrics into banking, while the national biometric-onboarding rail, the biometric CURP, is still maturing.

# Argentina

---

## IDENTIFIER AND REGISTRY

The DNI is issued by RENAPER, a strong biometric civil registry whose fingerprints and facial images also feed SIBIOS, the federal biometric system run by the Ministry of Security. The World Bank's ID4D case study puts DNI coverage at about 98 percent of the population... RENAPER data was stolen in 2021 and re-published at scale in 2024, which is relevant to any data-residency and trust framing.

---

## NATIONAL DIGITAL IDENTITY

The DNI is available in the Mi Argentina app as a credential with the same legal validity as the physical card, except for voting and non-MERCOSUR travel. This is the Active credential a user already holds. As municipal colour, the City of Buenos Aires issued decentralised identifiers to more than 3.6 million miBA platform users in 2024, a city credential rather than a national eID.

---

## GOVERNMENT EKYC ENABLER

RENAPER's SID (Sistema de Identidad Digital) exposes three identity-validation web services, DNI data validation, fingerprint validation, and facial validation, the last a 1:1 biometric match against the RENAPER photo. Access requires a signed Convenio Unico de Confronte de Datos, data-protection compliance, and a legitimate-interest assessment. Telcos, banks, and fintechs are eligible users.

---

## REGULATOR AND REMOTE- ONBOARDING BASIS

The regulators are the BCRA and the UIF. The AML law (Ley 25.246) was reformed by Ley 27.739 in 2024, which added virtual-asset service providers as obligated subjects. UIF Resolution 14/2023 permits non-presential onboarding using rigorous, auditable biometric techniques, and requires that the biometric factors be obtained from a genuine live human, which is effectively a regulatory liveness mandate. The BCRA has permitted non-presential savings-account opening validated by RENAPER facial biometrics since 2017.

---

## DATA PROTECTION AND RESIDENCY

Ley 25.326 (2000) remains in force, enforced by the AAIP, and Argentina holds longstanding EU adequacy. One gap stands out. Biometric data is not explicitly listed as sensitive under the 2000 law, a point the pending reform bills are expected to close. There is no general localization, and cross-border transfer is permitted under safeguards.

---

## PAYMENTS AND CRYPTO

Transferencias 3.0 is the BCRA interoperable instant-transfer and QR framework. Argentina is one of the region's most active crypto markets by on-chain value received, with stablecoins driven by inflation and capital controls (Chainalysis, an analytics firm, industry data). Providers must register in the CNV PSAV registry and are UIF-obligated, with a Travel Rule implemented via UIF Resolution 49/2024.

---

### DOCLESS READ

Argentina pairs near-universal registry coverage with a government facial-match web service and an explicit live-human liveness rule, so the biometric bind is effectively required here, a rare posture even within the region.

## IDENTIFIER AND REGISTRY

The Registraduria Nacional del Estado Civil (RNEC) runs the civil registry and the national biometric database. The cedula de ciudadanía digital entered mass rollout from September 2022, activated by a facial-biometric match, with the same legal validity as the physical document (Decreto 1413 of 2017).

---

## NATIONAL DIGITAL IDENTITY

The government login is Autenticacion Digital Ciudadana, run by the Agencia Nacional Digital under MinTIC through GOV.CO, with the cedula digital positioned as the entry point to the citizen digital folder.

---

## GOVERNMENT EKYC ENABLER

The RNEC biometric verification service lets authorized public and private entities verify a person against the biometric database, with the framework in Resolucion 27145 of 2023 and fees in Resolucion 1174 of 2025. SARLAFT accepts "operadores de información" under the habeas-data-financiero law (Ley 1266 of 2008) as independent sources for verification, which in practice means the credit bureaus DataCrédito (Experian) and TransUnion.

---

## REGULATOR AND REMOTE- ONBOARDING BASIS

The supervisor is the SFC and the financial intelligence unit is the UIAF. The AML framework is SARLAFT. SARLAFT 4.0 (Circular Externa 027 of 2020) expressly permits non-presential onboarding through digital and electronic channels using biometrics, strong authentication, and public databases. Decreto 222 of 2020 created low-value deposits opened remotely with simplified due diligence. Two newer laws sharpen the duty. Ley 2502 of 2025 aggravates penalties for AI or deepfake impersonation, and Ley 2573 of 2026 obliges financial entities, telecom operators and merchants that sell on credit to verify identity with sufficient mechanisms, keep the evidence, and carry the burden of proof when a customer alleges impersonation; the duty applies from late 2026.

## DATA PROTECTION AND RESIDENCY

Ley 1581 of 2012 treats biometric data as sensitive, and the authority is the SIC. Cross-border transfer requires adequacy or consent. There is no general localization. A 2025 reform bill circulated but was not enacted as of mid-2026, so Ley 1581 remains in force.

## PAYMENTS AND CRYPTO

Bre-B, the Banco de la Republica interoperable instant-payments rail, entered operation in October 2025 and had signed up more than 34 million users within about six months (Banco de la Republica). Nequi and DaviPlata are the leading wallets. Crypto is not legal tender and has no bespoke statute. The most recent virtual-asset bill (PL 510 of 2025) cleared two Chamber debates and was then archived at the close of the legislature, so the operative duty remains UIAF Resolución 314/2021, which requires suspicious-activity and monthly transaction reporting from providers.

### DOCLESS READ

Colombia has both rails, a government biometric service and named credit bureaus, and a statute (Ley 2573 of 2026) that now obliges banks, telcos, and merchants to verify identity before serving a customer.

**Two newer laws sharpen the duty.** Ley 2502 of 2025 aggravates penalties for AI or deepfake impersonation, and Ley 2573 of 2026 obliges banks, telecom operators, and merchants to verify identity and document authenticity before providing a service.

## IDENTIFIER AND REGISTRY

The Servicio de Registro Civil e Identificación (SRCel) issues the cedula de identidad, which carries the RUN and a fingerprint. A current cedula is obligatory from age 18, so RUN coverage is structurally near-universal. A digital cedula and passport, delivered through the official Identificación Digital app with in-app consent for each data share, began operating in December 2024.

---

## NATIONAL DIGITAL IDENTITY

ClaveÚnica, operated by the Secretaría de Gobierno Digital, passed 15 million activations in 2024 and gives access to more than 1,700 public procedures. The decisive change came in November 2025. New terms published in the Diario Oficial (Resolución Exenta 733/2025) set explicit criteria for private-sector entities to use ClaveÚnica for the first time, and the official strategy proposes a digital-identity broker for per-transaction private-sector authentication. This makes ClaveÚnica the natural Active credential, with the contractual barrier now lowered and the technical broker still maturing.

---

## GOVERNMENT EKYC ENABLER

The SRCel runs an official document-validity check for the cedula and passport, and businesses corroborate standing against commercial and credit bureaus, the Boletín Comercial and Dicom. There is no single open government identity-match API for the private sector yet. Verification is typically brokered, which is exactly the gap the planned ClaveÚnica broker aims to close.



## REGULATOR AND REMOTE- ONBOARDING BASIS

The integrated regulator is the CMF and the financial intelligence unit is the UAF. The AML statute is Ley 19.913. Non-presential account opening is permitted, because the CMF's Recopilacion Actualizada de Normas Chapter 2-2 was amended in 2021 to allow opening current accounts without physical presence, requiring board-approved policies to verify identity reliably and control identity fraud. The Ley Fintec (Ley 21.521) added a licensed framework, and the and CMF NCG 538 (June 2025) mandates reinforced customer authentication, with general provisions in force from August 2025 and mandatory use cases from July 2026.

---

## DATA PROTECTION AND RESIDENCY

The new Ley 21.719 was published in December 2024 and enters into force on 1 December 2026, creating the Agencia de Proteccion de Datos Personales, treating biometric data as sensitive, and setting fines up to 20,000 UTM. Until then Ley 19.628 governs. Cross-border transfer is permitted under safeguards. There is no hard localization.

---

## PAYMENTS AND CRYPTO

Chile has high electronic-payment penetration but, unlike Brazil or Colombia, no Pix-style interoperable instant scheme is live yet. The central bank is building the framework. Crypto has no bespoke statute. Under the Ley Fintec, crypto that qualifies as a financial instrument falls inside the CMF perimeter.

---

### DOCLESS READ

Chile's registry coverage is near-universal and ClaveUnica has just opened to the private sector, but the government identity-match API is still brokered, so partner-agnostic orchestration matters more here than anywhere else.

## IDENTIFIER AND REGISTRY

RENIEC issues the DNI and the electronic DNI (DNle 3.0, the only DNI issued since August 2025), backed by an AFIS biometric database widely regarded as one of the strongest civil registries in the region. RENIEC reports 37.15 million identified people, 25.9 million of them adults, and issued more than 8 million DNIs in 2025, its highest annual figure in six years. RENIEC signed a MOSIP pilot MoU in early 2024.

---

## NATIONAL DIGITAL IDENTITY

ID Peru is RENIEC's digital-identity platform, accessed by validating the DNle, with three assurance levels. The DNI BioFacial app supports remote self-service via a facial match against RENIEC, and the DNle carries authentication and digital-signature certificates.

---

### 2026 DEVELOPMENT

#### GOVERNMENT EKYC ENABLER

RENIEC's biometric verification service has historically sold AFIS-based 1:1 and 1:N verification to banks, fintechs, notaries, and telcos under thousands of convenios. This is the most consequential 2026 development for the market. After detecting irregular bulk querying, RENIEC has said it will wind down the traditional bulk third-party consulta services during 2026 and steer verification toward citizen-consented flows, the DNle chip, ID Peru, and facial biometrics, with dedicated-line queries no longer permitted for non-presential services. Peru's classic passive third-party biometric match is being deliberately curtailed in favour of active and biometric citizen-led verification.

## REGULATOR AND REMOTE- ONBOARDING BASIS

The regulator is the SBS, which houses the UIF-Peru. The AML rulebook is Resolucion SBS 2660-2015. Resolucion SBS 2891-2018 permits simplified, non-presential onboarding of basic accounts, with identity verified through RENIEC, Migraciones, or another modality, even after account opening.

## DATA PROTECTION AND RESIDENCY

Ley 29733 treats biometric data as sensitive. A newer regulation (Decreto Supremo 016-2024-JUS, in force from March 2025) adds a 48-hour breach-notification duty and data-protection-officer mandates. The authority is the ANPD within the Ministry of Justice. Cross-border transfer is permitted to jurisdictions with adequate protection or via model contractual clauses. There is no localization.

## PAYMENTS AND CRYPTO

The central bank mandates wallet interoperability. Yape and Plin have been interoperable since 2023, and Yape alone reports around 16.4 million monthly active users. Crypto is unregulated for consumers but AML-obligated. Resolucion SBS 02648-2024 makes virtual-asset service providers register with UIF-Peru and run KYC, with a Travel Rule taking effect from August 2026, the only scheduled provider Travel-Rule mandate among the six.

### DOCLESS READ

Peru has one of the strongest civil registries in the region, but 2026 is a live transition. The passive third-party query is giving way to citizen-led DNle, ID Peru, and facial flows, which raises the value of a provider that can run active and biometric modes, not just passive lookups.

# The Regulatory and Data Patterns Businesses Will Encounter Across Latin America

Pull the six markets together and two things become clear. The regulators are converging on the same answer, and the data rules are close cousins rather than copies. This section sets out both, first the onboarding basis each regulator provides, then the honest nuance on where the resulting data is allowed to sit.

On onboarding, every one of the six now provides a basis for remote, electronic verification, and several go further and name biometrics. Colombia's SARLAFT permits non-presential biometric onboarding. Argentina's UIF requires biometric factors from a genuine live human. Mexico's CNBV now mandates government-matched facial biometrics for higher-tier operations. Chile's CMF permits non-presential account opening and has issued a reinforced-authentication norm aimed at AI fraud. Brazil allows electronic, non-presential account opening. Peru permits simplified non-presential onboarding verified through RENIEC. At the regional level, the FATF Digital Identity guidance holds that reliable, independent digital ID supports customer due diligence and that non-face-to-face onboarding can be standard or even lower risk, and GAFILAT, the FATF-style regional body, carries that position rather than contradicting it.

FIG. 07 — THE REGULATORY TAILWIND, SIX MARKETS

| Market    | Remote onboarding permitted | Biometrics named in the rule | Named instrument                                                             |
|-----------|-----------------------------|------------------------------|------------------------------------------------------------------------------|
| Colombia  | ● Yes                       | ● Yes                        | SARLAFT 4.0 — Circular Externa 027/2020, non-presential biometric onboarding |
| Argentina | ● Yes                       | ● Yes                        | UIF Res. 14/2023 — biometric factors from a genuine live human               |
| Mexico    | ● Yes                       | ● Yes *                      | CNBV resolution, DOF 1 Jul 2026 — 90%+ facial match vs INE / SRE records *   |
| Chile     | ● Yes                       | ● Yes                        | RAN Chapter 2-2 (2021); NCG 538 reinforced authentication vs AI fraud        |
| Brazil    | ● Yes                       | Not explicit                 | CMN Res. 4.753/2019 — electronic, non-presential account opening             |
| Peru      | ● Yes                       | Not explicit                 | Res. SBS 2891-2018 — simplified non-presential onboarding via RENIEC         |

SOURCES: NAMED INSTRUMENTS, AS CITED.

\* Mexico's biometric requirement governs biometric authentication of higher-tier operations and high-value transactions, not new-client onboarding as such.

## Who regulates what — six markets at a glance

| Market                    | Registry and national digital ID                                  | Financial regulator / AML statute                     | Remote or biometric onboarding basis (named)                                                                                            | Data-protection law (status)               |
|---------------------------|-------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <a href="#">Brazil</a>    | CPF and CIN (Receita Federal / TSE base); gov.br (160M+)          | BCB, CVM, COAF / Lei 9.613/1998                       | CMN Res. 4.753/2019 (electronic, non-presential); Serpro Datavalid biometric match                                                      | LGPD (Lei 13.709/2018), ANPD (in force)    |
| <a href="#">Mexico</a>    | CURP and biometric CURP (RENAPO); INE credential; Llave MX (thin) | CNBV, Banxico, UIF / LFPIORPI (reformed Jul 2025)     | INE verification service (non-presential KYC); CNBV facial-biometrics mandate (DOF 1 Jul 2026, 90%+ vs INE/SRE, higher-tier operations) | LFPDPPP (in force Mar 2025, new authority) |
| <a href="#">Argentina</a> | DNI (RENAPER/SIBIOS); DNI in Mi Argentina                         | BCRA, UIF / Ley 25.246 (reformed by Ley 27.739, 2024) | UIF Res. 14/2023 (biometric, genuine-live-human); RENAPER SID web services                                                              | Ley 25.326 (2000, reform pending)          |
| <a href="#">Colombia</a>  | Cedula digital (RNEC base); Autenticacion Digital Ciudadana       | SFC, UIAF / SARLAFT                                   | Circular Externa 027/2020 (non-presential biometric); Decreto 222/2020; Ley 2573/2026                                                   | Ley 1581/2012, SIC (in force)              |
| <a href="#">Chile</a>     | Cedula/RUN and digital cedula (SRCel); ClaveUnica (15M+)          | CMF, UAF / Ley 19.913                                 | RAN Chapter 2-2 (2021, non-presential); ClaveUnica private-sector terms (Nov 2025)                                                      | Ley 21.719 (in force 1 Dec 2026)           |
| <a href="#">Peru</a>      | DNI/DNIE 3.0 (RENIEC AFIS); ID Peru                               | SBS, UIF-Peru / Res. SBS 2660-2015                    | Res. SBS 2891-2018 (non-presential basic accounts via RENIEC); note 2026 RENIEC pivot                                                   | Ley 29733 + DS 016-2024-JUS (in force)     |

SOURCES: NAMED INSTRUMENTS AND NATIONAL AUTHORITIES AS CITED IN SECTIONS 03-04 — CMN RES. 4.753/2019, LFPIORPI, CNBV RESOLUTION (DOF 1 JUL 2026), UIF RES. 14/2023, SARLAFT CE 027/2020, LEY 2573/2026, RAN CHAPTER 2-2, RES. SBS 2891-2018. REGULATORY POSITIONS SUMMARISED AS OF JULY 2026 — CONFIRM CURRENT REQUIREMENTS WITH THE RELEVANT REGULATOR OR COUNSEL.

None of the six imposes hard data localization. Four of the six list biometric data as a sensitive category in statute (Brazil, Colombia, Chile, Peru); Argentina and Mexico reach the same result through regulator guidance rather than the text of the law, so treat it as sensitive everywhere in practice. Five of the six changed or are changing their data-protection law between 2024 and 2026

FIG. 08 — DATA-PROTECTION LAW, 2024 TO 2026

| Market    | Status and instrument                                     |
|-----------|-----------------------------------------------------------|
| Brazil    | ● LGPD — in force since 2018, ANPD transfers rule 2024    |
| Mexico    | ● New LFPDPPP in force Mar 2025, new authority            |
| Peru      | ● DS 016-2024-JUS in force Mar 2025                       |
| Chile     | ○ Ley 21.719 published Dec 2024 — in force 1 Dec 2026     |
| Colombia  | ○ 2025 reform bill not enacted — Ley 1581 (2012) in force |
| Argentina | ○ Ley 25.326 (2000) in force — reform pending             |

SOURCES: NAMED DATA-PROTECTION STATUTES, SECTIONS 03-04.

**Shared facts on data residency.** No hard localization anywhere. Biometric data sensitive everywhere. Five of six laws changed or changing between 2024 and 2026. Sector cloud and outsourcing rules can still push processing in-country. The regimes are close cousins, not copies, and the guide does not rank them on strictness.

## All six regulators permit remote onboarding, and four now name biometrics in the rule. Is your onboarding flow keeping up?

A Shufti specialist can walk your current flow through each market's remote-onboarding and biometric rules and show where a docless route already fits.

[Book a demo](#)



# The sectors under most onboarding pressure

No industry is locked out of docless verification by the technology. Any sector that must verify identity can use electronic identity verification (eIDV), a docless check of an applicant's details against authoritative databases or a national digital ID, instead of a document upload — wherever the authoritative data can be reached..., and in Latin America the regulated sectors are adopting it because they now have both the legal driver and, in several markets, an explicit regulator instruction to use biometrics. The pressure is heaviest where volume, drop-off sensitivity, and fraud incentive meet, which puts fintech and crypto at the front.

FIG. 09 — SECTORS UNDER ONBOARDING PRESSURE

|                                     |                                                                                                                                                        |                         |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Fintech and payments</b>         | Instant-payment rails and the inclusion wave — every Pix registration, Bre-B alias, or Yape wallet ties an account to an identity.                     | <b>HIGHEST PRESSURE</b> |
| <b>Crypto and virtual assets</b>    | Provider rulebooks tightened 2024–2026 — BCB Res. 519/520/521 of 2025, CNV PSAV registry, SBS Travel Rule from Aug 2026, LFPIORPI vulnerable activity. | <b>HIGHEST PRESSURE</b> |
| <b>Remittances and cross-border</b> | Some of the world's largest flows, Mexico near USD 64.7bn in 2024 (Banco de Mexico), often settled through digital wallets.                            |                         |

**iGaming and online betting**

Regulated and expanding, including Brazil's newly licensed betting regime, with age and identity checks expected at signup.

**Lending and BNPL**

Speed at application is the whole game — thin-file and repeat users, millions of first-time borrowers.

**Telecommunications**

SIM registration becoming an identity-binding event — Chile's Subtel rules, Argentina's ENACOM and RENAPER agreement.

## Lead worked example — fintech and payments

This is the region's highest-volume, most drop-off-sensitive sector, and the one being reshaped by instant payments and financial inclusion. A digital bank or payments app can verify a low-risk applicant in the background against government or bureau data, Serpro Datavalid in Brazil, RENAPER SID in Argentina, the INE service in Mexico, the Registraduria in Colombia, RENIEC-linked flows in Peru, so the account opens with no upload. For higher-risk cases, an active national-eID check (gov.br, ClaveUnica) or a biometric bind raises assurance without forcing a document scan, and the biometric bind is the direct counter to the synthetic-identity and deepfake fraud growing across the region. The instant-payment rails make this urgent. Every Pix registration, Bre-B alias, or Yape wallet ties an account to an identity, and the onboarding wave behind them is enormous. Colombia's Bre-B alone signed up more than 34 million users within about six months of launch (Banco de la Republica).

## Co-lead — crypto and virtual assets

Latin America is one of the world's most active crypto and stablecoin regions, and the compliance perimeter has tightened sharply between 2024 and 2026. Brazil's provider rulebook (BCB Resolutions 519, 520, and 521/2025) hard-wires KYC and AML into crypto onboarding from early 2026. Argentina's CNV PSAV registry and UIF Travel Rule, Peru's SBS registration with a Travel Rule from August 2026, Mexico's treatment of virtual-asset activity as a vulnerable activity, and Colombia's and Chile's evolving regimes all push exchanges toward bank-grade docless verification. Because stablecoins in this region work as a retail dollar proxy, exchange onboarding volume is high and the fraud incentive is acute, which makes crypto a natural fit for biometric binding against the government record. Crypto-adoption and stablecoin volumes here come from Chainalysis, an analytics firm, and are industry data.

## The same principle carries to the other regulated verticals



### Remittances and cross-border payments

The region receives some of the world's largest remittance flows, with Mexico alone near 64.7 billion US dollars in 2024 (Banco de Mexico), often settled through digital wallets. Fast, docless verification of sender and recipient against national registries is the enabler.



### iGaming and online betting

Regulated and expanding in several markets, including Brazil's newly licensed betting regime, with age and identity checks expected at signup. High volume, fast onboarding, a strong docless case.



### Lending and BNPL

Speed at application is the whole game. Background attribute and registry checks remove the upload step for thin-file and repeat users, and the inclusion wave is bringing millions of first-time borrowers.



### Telecommunications

SIM registration is becoming an identity-binding event in its own right, from Chile's Subtel rules to Argentina's ENACOM and RENAPER agreement, which raises the fraud stakes and validates the same government-registry verification the financial sector uses.

**The throughline is identical across all of them.** The same compliance outcome as documents, fewer drop-offs, a biometric bind where synthetic identity and deepfakes are the threat, and a document fallback when a case needs it.

# Why Regional Coverage Claims Often Break Down at the Local-Market Level

Two structural gaps separate a vendor that works in Latin America from one that merely claims coverage. Both follow directly from the market cards, and both are easy to test in a procurement conversation before a contract is signed.

## GAP 01

### The deployment gap

A SaaS-only vendor that can process data only in its own cloud, in its own region, runs into the region's data reality. No market imposes hard localization, but every market treats biometric data as sensitive, five of the six rewrote or are rewriting their data-protection law between 2024 and 2026, and financial-sector cloud and outsourcing rules can still push processing in-country. A provider that can deploy in-region or on-premises, and route each market's data to where that market's regulator needs it to sit, is a different proposition from one that offers a single multi-tenant endpoint and hopes the rules hold.

## GAP 02

### The reach gap

A vendor built for Western documents, and unable to reach or bind to the region's government biometric registries, is a step behind before it starts. The source here is frequently the state's own civil registry, exposed as a verification service with its own credential, contract, and access model, from Argentina's RENAPER convenio to Brazil's e-CNPJ requirement to Peru's shifting RENIEC model. The whole game is reaching those sources and binding a live face to them, and that is exactly what a document-first vendor does not do.

## Before selecting an IDV provider for this region, ask

- 01 Can you run Passive verification against government or bureau sources in each of my target markets, not just document capture?
- 02 Can you bind a live selfie to a government biometric record where the market and the risk call for it?
- 03 Can you deploy in-region or on-premises where a regulator or a sector cloud rule requires it?
- 04 Do you support the national eID credentials that are live (gov.br, ClaveUnica) as an Active option, and where is Active not yet ready?
- 05 Do you keep document verification in the same flow as an automatic fallback, so no genuine user is lost?
- 06 Is AML screening part of the same integration, or a separate vendor and a separate seam?
- 07 Can you adapt as the rules move, for example Peru's 2026 RENIEC change or Chile's data law entering force in December 2026, without a re-integration?

**A provider that answers yes across that list is orchestrating identity for the region.** A provider that answers yes only to document capture is selling one step of it.

# Docless onboarding via government registries and national eID

This is where the three methods run on Latin America's authoritative sources, with assurance rising in step with risk. The model is straightforward to describe, and it maps onto this region cleanly because the sources it draws on are, unusually, the government's own. The section closes with the one caveat that matters most here, why registry size alone never proves an identity.

## METHOD 01

### Passive verification

The user provides their details, name, date of birth, national identifier, and the match runs silently in the background against authoritative sources. That may be a government civil registry where one is exposed as a service, a regulated credit bureau where that is the named route, or telecom and utility data as added coverage. From the user's side there is nothing beyond the form they were already filling in. In Latin America this is the primary method, because the source is frequently the state registry itself.

## METHOD 02

### Active verification

The user authenticates with a national digital-identity credential they already hold, and the issuer confirms the identity in real time. This is genuinely strong in Brazil (gov.br, with a biometric gold tier) and Chile (ClaveUnica, now open to the private sector), real but narrower in Peru and Argentina, and still immature in Mexico, where Llave MX is a services-access layer rather than a high-assurance credential. The guide presents Active as market-dependent by design, because pretending to a uniform national-eID grid the region does not yet have would not survive the first question a buyer asks.

## Biometrically Enriched verification

A live selfie is matched against the photo held by the authoritative source, layered on top of the Passive or Active data match. This is the strongest assurance level in the docless flow and the direct counter to synthetic identity and deepfakes, because a fabricated or stolen identity may carry plausible data, yet cannot present the live face the government record belongs to. This is Shufti's biometric face verification layer, and it is the answer to the fraud beat that runs through the whole region.

**Automatic fallback built in.** Not every check returns a confident match. Recent migrants, young applicants, and anyone with a thin footprint will not always clear a passive lookup, and a market like Peru is actively changing its access model mid-year. The flow escalates automatically, from Passive to Active where a rail exists, or to document verification with biometric matching, so no genuine user is lost to a failed database check. The escalation logic sits in configuration, not in code.

## One platform routes each applicant to the right method

EVERY APPLICANT

Risk assessment

Scores each applicant on fraud signals, data availability and market, then picks the method below



### **Passive — background match, no upload**

A silent match against the government or bureau source. The low-risk majority skips the upload entirely.

LOW RISK

Peru, 2026 — the passive branch is moving toward citizen-consented DNle, ID Peru, and facial flows.

### **Active — national-eID presentation**

The applicant authenticates with a credential they already hold, and the issuer confirms in real time.

WHERE THE APPLICANT  
HOLDS ONE

Live and mature in Brazil and Chile. Narrower elsewhere — Active is not uniform across the six.

### **Biometrically Enriched — live face, government record**

A live selfie is bound to the photo held by the source record. The region's direct answer to synthetic identity and deepfakes.

SYNTHETIC-RISK OR  
DEEPFAKE SIGNALS

### **Fallback — document verification plus biometrics**

The automatic escalation path in the same flow. Thin-file, new-to-country, and migrating applicants stay onboardable.

STANDARD / HIGH RISK, OR  
NO MATCH

## **The fastest way to see the fit is to watch it run.**

A demo maps your products, risk tiers, and target markets to a live verification configuration, showing which rail applies in each country.

[\*\*Book a demo\*\*](#)

# Why a live bind beats a big registry

Latin American registries are large, and in several markets they are larger than the working-age population. Brazil is the clean illustration. A Tribunal de Contas da Uniao audit found 216.84 million regular CPF records against a 2022 census population of 203.08 million, an excess of roughly 13.8 million records the audit ordered Receita Federal to work down. Registries count all ages, emigrants, and records not yet purged, so registry size divided by adult population routinely overshoots.

The lesson for onboarding is direct. Registry reach is what makes docless possible, and registry excess is exactly why a live biometric bind against the record matters more than the raw count. A data match confirms that a record exists. A live face bound to that record confirms that the person in front of you owns it.

FIG. 12 — BRAZIL, REGISTRY EXCESS  
MILLIONS OF RECORDS / PEOPLE



EXCESS OF ROUGHLY 13.8 MILLION RECORDS. SOURCE: TCU AUDIT, REPORTED BY INFOMONEY.

**Two caveats.** Active is not uniform, so the national-eID step applies where the credential is live and mature, in Brazil and Chile, and as a lighter option elsewhere. And Peru's 2026 RENIEC shift is live rather than settled, so the passive branch for that market should be read as moving toward citizen-consented DNle, ID Peru, and facial flows rather than an open third-party lookup. A provider that runs all three modes, rather than passive lookups alone, is what keeps a market like Peru onboardable through the change.

FIG. 13 — ACTIVE-MODE READINESS ACROSS THE SIX

| Market    | Readiness | National eID           |
|-----------|-----------|------------------------|
| Brazil    | Mature    | gov.br                 |
| Chile     | Mature    | ClaveUnica             |
| Peru      | Narrower  | ID Peru / DNle         |
| Argentina | Narrower  | Mi Argentina           |
| Colombia  | Present   | Aut. Digital Ciudadana |
| Mexico    | Immature  | Llave MX               |

### Registry size proves coverage, not identity

Brazil's CPF base held about 216.8 million records against a census population of 203.1 million in 2026, a surplus of roughly 13.7 million that the Tribunal de Contas da União attributes to duplicates, deceased holders and dormant records. A match against a registry that large confirms that a record exists; only a live face bound to that record confirms the applicant is the person it describes.

# The Identity Foundation Needed to Expand Across Diverse Latin American Markets

The architectural answer to a six-market region is a single integration rather than six. Most teams assemble the alternative from parts, one provider for a government or bureau check in each market, another for document capture, a third for watchlist screening, and internal engineering holding the seams together. That approach is costly. It also breaks every time a market changes, and in this region markets change often. The design principles that matter here follow directly from the market cards.

## **Owned end to end, one API**

Passive, Active, biometric, document, and AML capabilities delivered as one platform, so a change in one market is a configuration change, not a new vendor.

## **Routing per applicant, inside each market**

Each applicant is routed to the right method by risk, data availability, and the market they are in, so the low-risk majority skips the upload while high-risk and no-match cases get the step-up they need.

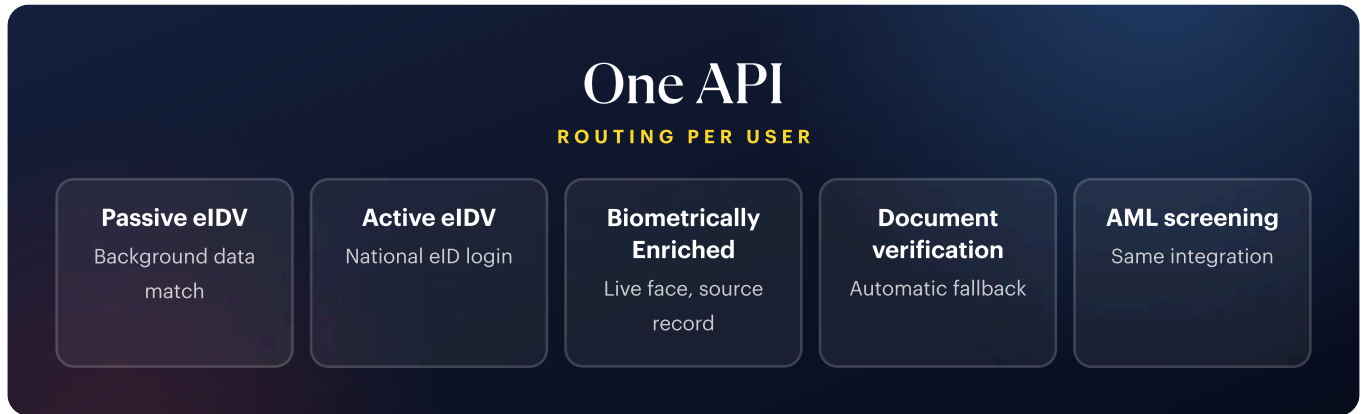
## **Deployable where each regulator needs the data to live**

In-region or on-premises where a data-protection regime or a sector cloud rule calls for it, which is the deployment gap that sidelines SaaS-only vendors here.

## **Built to absorb change**

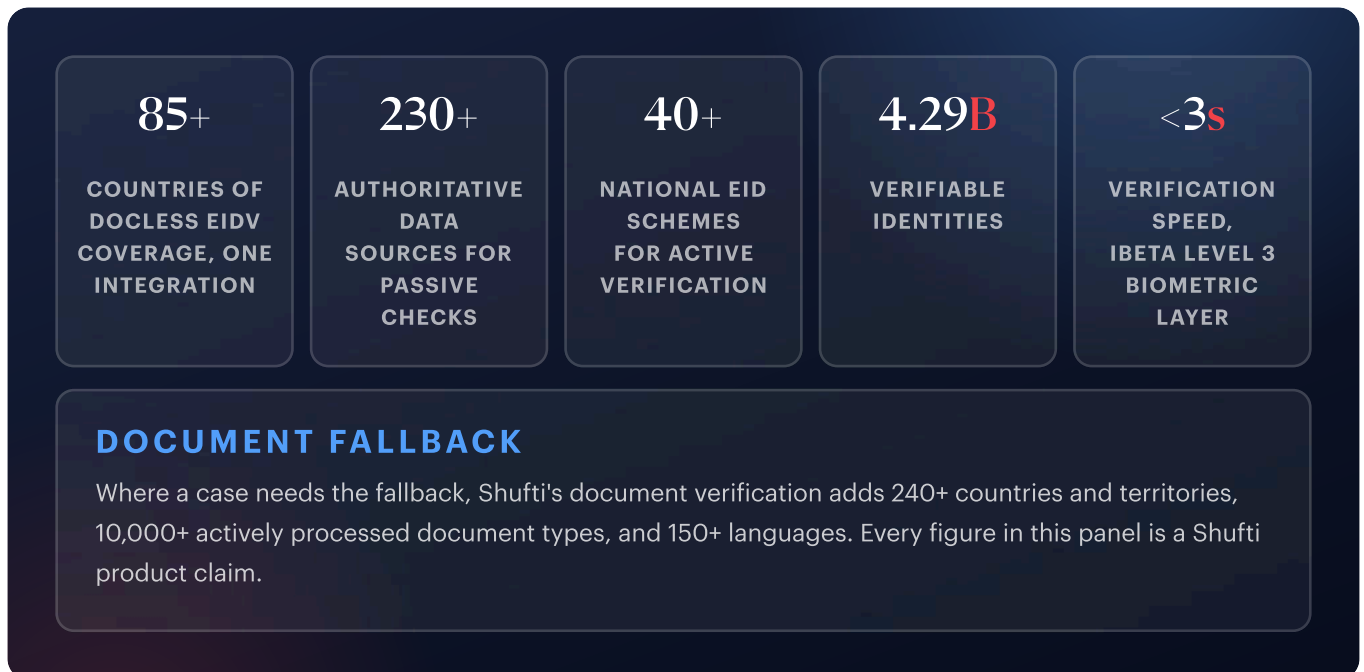
When Peru's RENIEC access model shifts in 2026, or Chile's data law takes force in December 2026, or Mexico's biometric CURP stabilizes, the flow adapts through configuration rather than re-integration.

FIG. 15 — ONE INTEGRATION, FIVE CAPABILITIES



Shufti runs Passive, Active, and Biometrically Enriched verification, plus document verification and AML screening, through a single integration, with routing rules set per market and applied per applicant, so a change in one market is a configuration change rather than a new vendor.. The proof points behind the model split into the docless layer and the document fallback.

FIG. 16 — SHUFTI EIDV COVERAGE · A SHUFTI PRODUCT CLAIM  
SOURCE: SHUFTIPRO.COM/EIDV



VERIFICATION SPEED IS STATED AS UNDER THREE SECONDS, WITH THE BIOMETRIC LAYER BUILT TO IBETA LEVEL 3 CONFORMANCE TO ISO/IEC 30107-3.

# The Assurance Evidence Your Compliance and Security Teams Will Ask For

For a compliance reader, the platform's assurances carry as much weight as its features. The standards below are the ones a Latin American AML or data-protection reviewer will look for, and they belong in a guide as verifiable facts, presented plainly rather than dressed up.

|                                                     |                                                                                                                                                                                             |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ISO 27001</b>                                    | For information-security management.                                                                                                                                                        |
| <b>SOC 2 Type 2</b>                                 | For the operating effectiveness of security controls over time.                                                                                                                             |
| <b>iBeta Level 3 Conformance to ISO/IEC 30107-3</b> | For the biometric presentation-attack-detection layer that makes the live-face bind resistant to spoofing, the exact control the region's synthetic-identity and deepfake fraud is testing. |
| <b>PCI DSS</b>                                      | For the handling of payment-card data.                                                                                                                                                      |
| <b>GDPR alignment</b>                               | Alongside alignment with the region's own data-protection laws, Brazil's LGPD, Mexico's LFPDPPP, Argentina's Ley 25.326, Colombia's Ley 1581, Chile's Ley 21.719, and Peru's Ley 29733.     |

# The Questions Your Compliance, Product, and Risk Teams Will Ask

## 01 Is docless identity verification permitted in these markets?

Yes. Every one of the six provides a basis for remote, electronic verification, and several name biometrics, from Colombia's SARLAFT to Argentina's UIF live-human rule to Mexico's CNBV facial-biometrics mandate. The FATF Digital Identity guidance holds that reliable digital ID supports customer due diligence and that non-face-to-face onboarding can be standard or lower risk.

---

## 02 What makes Latin America different from other regions for docless?

The authoritative source is usually the government's own biometric civil registry, exposed as a verification service, rather than a credit bureau assembled into a proxy for identity. That makes a clean, government-grade passive and biometric backbone available in most of the region.

---

## 03 Does docless verification stop synthetic identity and deepfake fraud?

A data match alone does not, because a fabricated or stolen profile can look plausible on paper. Biometrically Enriched verification counters it by requiring a live facial match against the authoritative government record, which a fabricated identity cannot supply. The presentation-attack-detection layer holds iBeta Level 3 Conformance to ISO/IEC 30107-3.

---

## 04 What happens to users who cannot be matched against a registry?

They fall back automatically to document verification with biometric matching in the same flow. Thin-file, new-to-country, and migrating applicants stay onboardable, and nobody is turned away because a registry lookup did not return.

---

## 05 Is one integration enough for all six markets?

Yes. Shufti runs Passive, Active, and Biometrically Enriched verification, document verification across 240+ countries and territories, and AML screening through one API, with routing configured per market and per risk tier, and deployment where each regulator needs the data to live.

---

## 06 How does the platform handle a market whose rules are changing, like Peru in 2026?

Through configuration rather than re-integration. A provider that runs all three modes, not passive lookups alone, keeps a market onboardable when its access model shifts, as Peru's RENIEC model is shifting toward citizen-consented flows during 2026.

---

# Sources

- 01 World Bank, Global Findex 2025 (Little Data Book on Financial Inclusion 2025). [worldbank.org/en/publication/globalfindex](https://worldbank.org/en/publication/globalfindex)
- 02 GSMA, The Mobile Economy 2025. [gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy](https://gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy)
- 03 FATF, Guidance on Digital Identity (2020). [fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf](https://fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf)
- 04 Banco Central do Brasil, Pix open data. [bcb.gov.br/en/financialstability/pix\\_en](https://bcb.gov.br/en/financialstability/pix_en)
- 05 Serpro, CNH do Brasil. [serpro.gov.br/menu/noticias/revista-tema-240/cnh-do-brasil](https://serpro.gov.br/menu/noticias/revista-tema-240/cnh-do-brasil)
- 06 Tribunal de Contas da Uniao CPF audit, reported by InfoMoney. [infomoney.com.br/brasil/cadastro-da-receita-tem-137-mil-hoes-de-cpfs-a-mais-que-o-censo-aponta-tcu](https://infomoney.com.br/brasil/cadastro-da-receita-tem-137-mil-hoes-de-cpfs-a-mais-que-o-censo-aponta-tcu)
- 07 Instituto Nacional Electoral (Mexico), Servicio de Verificacion de Datos de la Credencial para Votar. [ine.mx/servicio-verificacion-datos-credencial-votar](https://ine.mx/servicio-verificacion-datos-credencial-votar)
- 08 Instituto Nacional Electoral (Mexico), lista nominal statistics. [ine.mx/credencial/estadisticas-lista-nominal-padron-electoral](https://ine.mx/credencial/estadisticas-lista-nominal-padron-electoral)
- 09 CNBV facial-biometrics resolution, DOF 1 July 2026, as analysed by BASHAM. [basham.com.mx/en/resolution-amending-the-general-provisions-applicable-to-credit-institutions](https://basham.com.mx/en/resolution-amending-the-general-provisions-applicable-to-credit-institutions)
- 10 Banco de la Republica (Colombia), Bre-B. [banrep.gov.co/en](https://banrep.gov.co/en)
- 11 Registraduria Nacional del Estado Civil (Colombia), censo electoral 2026. [registraduria.gov.co/-Censo-Electoral-al-7-de-abril-de-2026-.html](https://registraduria.gov.co/-Censo-Electoral-al-7-de-abril-de-2026-.html)
- 12 Congreso de Colombia / SISJUR, Ley 2573 de 2026. [funcionpublica.gov.co/eva/gestornormativo/norma.php](https://funcionpublica.gov.co/eva/gestornormativo/norma.php)
- 13 RENIEC (Peru), estadísticas. [identidad.reniec.gob.pe/estadisticas](https://identidad.reniec.gob.pe/estadisticas)
- 14 RENIEC 2025 DNI issuance, reported by Infobae. [infobae.com/peru/2026/01/09/reniec-supera-los-ocho-millones-de-dni-emitidos-en-peru-y-el-extranjero-en-2025-la-cifra-mas-alta-en-seis-anos](https://infobae.com/peru/2026/01/09/reniec-supera-los-ocho-millones-de-dni-emitidos-en-peru-y-el-extranjero-en-2025-la-cifra-mas-alta-en-seis-anos)
- 15 Banco de Mexico, remittance statistics (2024). [banxico.org.mx](https://banxico.org.mx)
- 16 Banco Central de Reserva del Peru, wallet interoperability. [bcrp.gob.pe](https://bcrp.gob.pe)
- 17 Shufti, eIDV coverage. [shuftipro.com/eidv](https://shuftipro.com/eidv)

**Disclaimer.** This guide is practitioner guidance, not legal advice. Regulatory positions are summarised as of the dates shown and may change. Confirm current requirements with the relevant regulator or counsel before acting.





## Talk to Shufti's Latin America team

If you are adding docless verification to an existing document flow, entering one or more of these six markets, or extending across the wider region, the fastest way to see the fit is to watch it run. A demo maps your products, risk tiers, and target markets to a live verification configuration, showing which rail applies in each country, where Active national-eID is ready, and how document verification and AML screening run in the same flow.

The same platform reaches beyond these six markets across 240+ countries and territories, so the model holds as you expand. No commitment, and no engineering work required to see it configured for your markets.

[Book a demo](#)

**Shufti is based in the United Kingdom and operates offices worldwide.**



### United States

16200 SW Pacific  
Hwy, Suite H PMB  
1053,  
Tigard, OR



### Cyprus

Arch. Makarios III  
Avenue 229,  
Limassol



### Dubai

Unit 507, Level 5,  
Gate District  
Precinct  
Building 03, DIFC,  
Dubai



### Hong Kong

8 Queen's Road  
East, Wan Chai,  
Hong Kong



### Pakistan

322-G3 Main Blvd,  
Johar Town, Lahore,  
Pakistan



### Singapore

68 Circular Road  
#02-01, Singapore



### United Kingdom

Office 408,  
Coppergate  
House, 10 Whites  
Row, London E1  
7NF

[shuftipro.com](https://shuftipro.com)

[sales@shuftipro.com](mailto:sales@shuftipro.com)

