Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Brazil

COUNTRY Brazil

INDUSTRY Government & Public Services

LAST UPDATED 11 November 2026

KEY REGULATORS Ministry of Management and Innovation in Public Services · Superior Electoral Court · National Institute of Information Technology

Key takeaways

- Brazil runs one national digital identity, the gov.br account, with three assurance levels (bronze, silver and gold) set in a federal ordinance. Each federal service must choose its level after a risk assessment, so the level a user holds decides what they can do online.
- The Individual Taxpayer Registry number (CPF) is the single national identifier: it is the number on the new National Identity Card (CIN) and is enough on its own to identify a person in public-service databases.
- Higher assurance comes from matching a face against government photo databases: the driving-licence database gives silver; the Electoral Court's biometric database, a scan of the CIN's QR code plus a face match, or a qualified digital certificate give gold. Under the ordinance, silver and gold logins require multi-factor authentication.
- The in-person channel is protected: federal bodies cannot refuse an in-person signature because it does not meet an electronic level, and citizens keep a right to face-to-face service.
- A biometric record in a government database is becoming a condition for federal social security benefits: the rule took effect on 21 November 2025, and records made after 31 December 2026 must be in the CIN database. Stricter remote-identification rules for qualified digital certificates, including deepfake and injection-attack defences, have applied since May 2026.

Digital public services in Brazil are widely used: federal bodies must offer their digital services through the gov.br platform and its single sign-on, and states and municipalities can adopt the same rules by their own acts. Identity in this sector is governed by a public-law framework of statutes, decrees and ordinances, not by anti-money laundering (AML) rules.

The principal authorities are the Ministry of Management and Innovation in Public Services (MGI), through its Digital Government Secretariat (SGD), the Superior Electoral Court (TSE), which holds the national civil identification database, the National Institute of Information Technology (ITI), which runs the ICP-Brasil certificate infrastructure, and the Agência Nacional de Proteção de Dados (ANPD).

The biggest obstacle for a private provider is access: the national civil identification database may not be sold, and private parties reach government identity data only through routes the law names, such as the TSE's paid biometric check service, accreditation as a gov.br digital access validator or registration authority work under ICP-Brasil. Private firms cannot integrate the gov.br login into their own services.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
- Sources

1 Who regulates this sector

Authority	Remit	Level	Official site
Ministry of Management and Innovation in Public Services (MGI), Digital Government Secretariat (SGD)	gov.br platform and account levels, National Digital Government Strategy, Civil Identification Digital Public Infrastructure, accreditation of digital access validators	Federal	gov.br/governodigital
Federal Executive Chamber for Citizen Identification (Cefic)	Sets identification and CIN standards by resolution; coordinated by the Presidency's Casa Civil, with the Federal Revenue Service, the SGD and the Justice and Health ministries (Decreto nº 11.797/2023, arts. 9 to 11)	Federal	gov.br/governodigital (Cefic)
State and Federal District identification bodies	Issue the National Identity Card (CIN) to the federal standard	State	gov.br/gestao (CIN)
Superior Electoral Court (TSE)	Stores and manages the National Civil Identification (ICN) database, including electoral biometrics; credentials users; sole provider of biometric checks to private parties	Federal (judiciary)	tse.jus.br

National Institute of Information Technology (ITI)	Root authority of ICP-Brasil (qualified digital certificates); identification rules for certificate applicants	Federal	gov.br/iti
Federal Revenue Service (Receita Federal)	CPF registry, the national key identifier; bronze-level data check	Federal	gov.br/receitafederal
Federal Police	Civil identification of immigrants and the National Migration Registry Card (CRNM)	Federal	gov.br/pf
Agência Nacional de Proteção de Dados (ANPD)	Enforces the General Data Protection Law (LGPD), including against public bodies; an autonomous agency under the Ministry of Justice and Public Security since Lei nº 15.352/2026	Federal	gov.br/anpd

2 Licensing and authorisation

Public bodies need no licence to identify citizens. Lei nº 14.129, de 29 de março de 2021 (Digital Government Law) applies directly to federal bodies, including state-owned companies that provide a public service, and to states and municipalities once they adopt it by their own acts (art. 2). Federal bodies must use the gov.br access mechanism for all of their digital public services (Decreto nº 8.936/2016, art. 4, IV).

Private firms take part in public identity flows through three routes set in the rules:

Digital access validator

The SGD accredits validators that confirm identity for gov.br (Decreto nº 10.543/2020, art. 5, § 1; Portaria SGD/MGI nº 11.230/2025). A private firm needs public-facing premises and staff, a head office in Brazil, coverage of at least one state per region and 1% of the economically active population where it operates, and either in-person document validation or biometric validation, in person or remote, against a government database (art. 8, II). The SGD monitors validators and can withdraw accreditation (arts. 12 and 13).

ICP-Brasil certification and registration

Certification and registration authorities operate under ITI rules and answer for damage caused by a faulty identification of an applicant (IN ITI nº 36/2026, art. 1, § 2).

TSE credentialing

Access to the ICN database requires TSE credentialing (Res. TSE nº 23.526/2017, art. 7). Private institutions may use TSE electronic services for identification and authentication only (art. 8, II). Biometric checks for private parties are a paid service: the TSE sets the price and may contract an operator to market it (Res. CGICN nº 7/2021, arts. 4 to 6). Its check services return a match or no match against TSE bases and are offered within access quotas; private access must fit LGPD art. 26, § 1 (Res. TSE nº 23.656/2021, arts. 2, VI, and 4).

The gov.br login, advanced signature and digital proof-of-life products are open only to public bodies, including state-owned companies, offering a public service on a gov.br domain; integration requires a system hosted on an official government domain, and state and municipal bodies must first join the Rede Gov.br (Portaria SGD/MGI nº 7.076/2024, arts. 3 and 8). Private firms and market-facing services such as banking cannot integrate them (SGD integration FAQ). The ICN database may not be sold (Lei nº 13.444/2017, art. 4), and access rights and data obtained from it cannot be passed to third parties (Res. TSE nº 23.526/2017, art. 8, § 2).

3 Identity framework (AML rules do not apply)

Public bodies are not obliged entities under Brazil's AML law: Lei nº 9.613/1998, art. 9, lists finance, insurance, gambling, real estate, high-value goods and similar sectors, not public services. Commercial and public registries are the nearby exception (art. 9, sole paragraph, XIII).

Identity for public services rests instead on four layers:

- **A single identifier.** The CPF is the "single and sufficient" number for identifying citizens in public-service databases, and new public documents use it as their number (Lei nº 14.534/2023, art. 1; Lei nº 14.129/2021, art. 28).
- **A national identity card.** The CIN under Decreto nº 10.977/2022, issued by the states to one federal standard.
- **Civil identification databases.** The ICN database held by the TSE (Lei nº 13.444/2017) and the federal Citizen Identification Service (Decreto nº 11.797/2023), which is mandatory for federal identification outside criminal and state-security systems and keyed to the CPF (arts. 3 and 5). With the gov.br access and signature tools, it forms the Civil Identification Digital Public Infrastructure (Decreto nº 12.069/2024, art. 18).
- **Assurance levels.** The gov.br account levels and the three signature levels of Lei nº 14.063/2020 and Decreto nº 10.543/2020.

Political exposure still matters: ICP-Brasil certificate applicants are checked for politically exposed person (PEP) status, and a PEP application needs a second verification by a different registration agent (IN ITI nº 36/2026, arts. 8 and 9).

4 Identity verification and onboarding

The gov.br account levels

Portaria SGD/MGI nº 11.229/2025, in force since June 2026, defines the levels: bronze rests on biographic data validated in government databases; silver on validation of a civil identity document, in person or remote, by an identity provider, or on biometric validation; gold on document validation plus biometric validation in a deduplicated government database, or on an ICP-Brasil certificate (art. 3). The CPF is the account's unique identifier. Bronze logins may use one factor; silver and gold require multi-factor authentication (art. 5). The SGD's levels page lists the routes:

Level	How it is obtained	Security

Bronze	Online form validated against Federal Revenue or INSS data, or in person at INSS offices and Balcão gov.br points	Basic
Silver	Facial recognition in the gov.br app against the driving-licence (CNH) photo database; validation through one of the accredited banks (17 in March 2026); or SIGEPE credentials for federal civil servants	High
Gold	Facial recognition in the gov.br app against the Electoral Court (TSE) database; reading the CIN QR code in the gov.br app followed by facial recognition; or an ICP-Brasil personal digital certificate	Maximum

Federal bodies must analyse each service's financial and privacy risks, set the account level accordingly and help citizens reach it (art. 7). SGD guidance recommends gold with two-factor authentication for financial transactions and PEP-facing systems, and silver with two-factor for sensitive data and benefit claims. The Federal Revenue Service's e-CAC portal no longer accepts bronze accounts.

The National Identity Card

The CIN has nationwide validity, uses the CPF as its number and carries an ICAO-standard photograph, the right thumbprint, a QR code and an ICAO machine readable zone; the QR code exposes civil registration data and the thumbprint for verification (Decreto nº 10.977/2022, arts. 2, 3 and 11). The decree's card specifications include no chip (Annexes I and II). Issuing bodies run a biometric check in the Citizen Identification Service (art. 12). Validity is five years to age 11, ten years from 12 to 59 and indefinite from 60 (art. 15). Old-model cards stay valid until 1 March 2032 (indefinitely for holders aged 60 or over in March 2022), when paper issuance also ends (arts. 25 and 26). The digital CIN follows delivery of the physical card and is activated on a phone through facial comparison with liveness detection (art. 5; Annex III, art. 2).

Immigrants are identified by the Federal Police, which registers them biographically and biometrically and issues the CRNM (Decreto nº 9.199/2017, arts. 58, 62 and 63).

Qualified certificates (ICP-Brasil)

IN ITI nº 36/2026 admits in-person, videoconference, existing-certificate and two electronic registration-authority methods, each remote method giving security equivalent to in-person identification (art. 2). Identification includes document verification, biometric capture with liveness detection, a negative-list check and a holder's agreement (art. 3); in person, fingerprint and face are captured, remotely at least the face (art. 8, IV). Matching runs against the CIN, ICN, CNH and Civil Identification Digital Public Infrastructure bases

(art. 5), and document QR codes, machine readable zones and NFC chips must validate or issuance is refused (art. 8, § 6).

Videoconference tools must detect liveness and presentation attacks against deepfakes, detect injection of pre-recorded or synthetic video, block virtual cameras and compromised devices, and use random question scripts in real time (art. 37). Since IN ITI nº 38/2026, applicants may show a digital identity document, and data must be checked against the CNH base through Datavalid for in-person, videoconference and electronic registration-authority issuance (arts. 27 and 38).

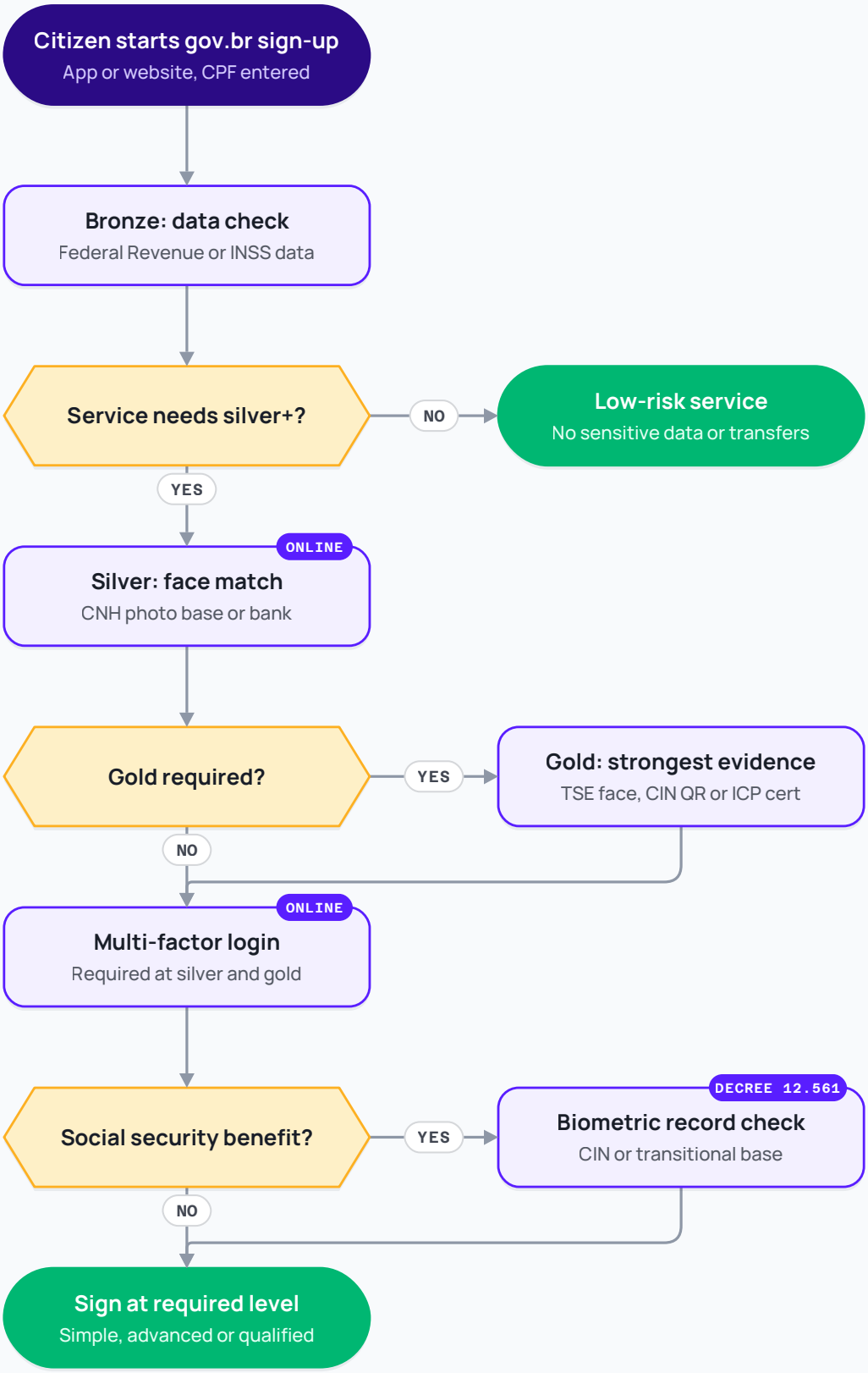


Figure 1. Remote identity proofing and step-up for a federal digital public service in Brazil.

5 Digital channels: what's different

Bottom line: digital is the default channel for federal services, but the law protects the in-person route: online assurance comes from biometric matching against government databases, while in-person identification stays acceptable at every level.

Requirement	In person	Online / remote	Difference
Right to the channel	Guaranteed on request	Default, preferably self-service	Differs
Basic (bronze) account	INSS office or Balcão gov.br	Form checked against Revenue or INSS data	Same
Higher assurance	Identity checked by a public agent	Face match against CNH or TSE base, CIN QR or certificate	Differs
Private validators	Document or biometric validation	Biometric validation against a government base only	Differs
Acceptance of signatures	Cannot be refused for not meeting an electronic level	Minimum level set per interaction	Differs
Qualified certificate biometrics	Fingerprint and face	At least face, with liveness and injection-attack detection	Differs
Evidence kept for certificates	Documents, biometrics, audit trail	Same, plus video recording	Differs
Biometric record for benefits	Required	Required	Same

The in-person route cannot be closed

Digital delivery must not prejudice the citizen's right to face-to-face service (Lei nº 14.129/2021, art. 14), and a digital channel does not replace other channels a service's public needs (Decreto nº 8.936/2016, art. 5). Minimum electronic signature levels cannot be used to reject signatures made in person or derived from in-person identification

(Decreto nº 10.543/2020, art. 4, § 2). A design with no in-person route conflicts with that right.

Remote assurance means database matching

Advanced signatures require registration with identity assurance from a validator: document validation by a public agent, biometric validation against a government database, or an authorised validator with a high degree of security (Decreto nº 10.543/2020, art. 5, II). In practice, any gov.br account can sign at simple level, silver and gold accounts can give advanced signatures, and qualified signatures need an ICP-Brasil certificate (Portaria SGD/MGI nº 11.230/2025, arts. 3 to 5). A private validator may work remotely only through biometric matching against a government database (art. 8, II).

Account security online

Account holders must protect their credentials, use two-step verification where possible and report incidents; the platform must re-check evidence whenever an account changes level (Portaria SGD/MGI nº 11.229/2025, arts. 4 and 6). The gov.br account page lists multi-factor authentication for silver and gold; app-based two-step verification is still a user setting, and each integrating body decides whether to require it (SGD access-requirements page). A user who loses access drops back to bronze until re-verified (MGI, March 2026), and compromised signature credentials can be suspended individually or collectively (Decreto nº 10.543/2020, art. 8).

6 Data protection and biometrics

Biometric data are sensitive data under Lei nº 13.709/2018 (LGPD). Public bodies process personal data to fulfil their legal competences, must publish the legal basis, purpose and practices of each processing activity and must appoint a data protection officer (art. 23). Sensitive data may be processed without consent where shared processing is needed for public policies set in law or regulation, and public bodies must publicise when they rely on that exemption (art. 11, II, b, and § 2).

Public bodies may transfer personal data to private entities only in listed cases, including legal authorisation or contracts and transfers made solely to prevent fraud or protect the data subject (art. 26, § 1). Executives may copy ICN data except biometrics into their own databases (Lei nº 13.444/2017, art. 3, § 1), and the TSE releases biometric data only to courts, prosecutors, police and identification bodies (Res. TSE nº 23.526/2017, art. 8, § 1; Res. TSE nº 23.656/2021, art. 2, § 3).

7 Sector-specific obligations

Biometric record for social security benefits

Lei nº 15.077/2024 makes a document with a biometric record taken by the State a condition for granting, maintaining and renewing social security benefits, with exceptions for hard-to-reach places and people who cannot travel (art. 1). Decreto nº 12.561/2025, in force since 21 November 2025, makes the CIN biometric database the reference base and accepts the CNH, Federal Police and TSE databases transitionally (art. 2). Under Portaria SGD/MGI nº 2.907/2026, in force since 30 April 2026, those transitional records count until 31 December 2027 if made by 31 December 2026; after that only the CIN database may be used (art. 2). The biometric verification service must reach benefit-managing bodies by 31 December 2026 (art. 3).

Electronic signature levels per interaction

Federal bodies apply minimum levels by interaction: simple for scheduling, logging in, sending documents and claiming benefits; advanced for classified information, contracts, system self-registration, benefit decisions and appeals; qualified for real-estate transfers, acts of the President and ministers and other cases set by law (Decreto nº 10.543/2020, art. 4). They may require more and must publish their advanced-signature requirements (arts. 4, § 1, and 5, § 2). Public and private providers of advanced signatures used with the federal administration must follow the cryptographic standards set by ITI and the SGD (Portaria Conjunta ITI/SGD nº 1/2021, Annex, item 1.2). Digitally signed submissions are presumed authentic (Lei nº 14.129/2021, art. 26).

8 Risk indicators and red flags

IDENTITY-ABUSE INDICATORS IN PUBLIC DIGITAL SERVICES

- **Exposed benefit data**: leaked CPFs, bank details and dates of birth enable fraud and identity theft (ANPD, INSS decision).
- **Untrusted devices**: with device management on, a login from a new device needs approval in the gov.br app.
- **Synthetic or replayed video**: deepfakes, injected video streams and virtual cameras in remote identification.
- **Document features that fail validation**: QR code, MRZ or chip data that do not validate bar certificate issuance.
- **Unusable photographs**: documents that prevent facial matching cannot be used for certificates.
- **Changed appearance**: physical changes raising founded doubt can lead to a CIN being refused as valid.
- **Inactive taxpayer status**: CPFs marked cancelled, null or deceased.

9 Enforcement and penalties

The LGPD applies to public bodies with a reduced sanction set: warnings, publication of the infringement, blocking or deletion of data, partial suspension of the database or of the processing for up to six months (extendable once) and prohibition of processing (art. 52, § 3). Fines of up to 2% of Brazilian turnover, capped at R$ 50 million per infringement, apply to private-law entities such as contractors and identity providers (art. 52, II).

In February 2024 the ANPD ordered the INSS to publish, for 60 days, its failure to notify people of a 2022 benefits-system breach exposing CPFs and bank details.

Sector rules add sanctions: the TSE may suspend a body's ICN access where harm is imminent, contractors misusing ICN data face contract termination and administrative, civil and criminal sanctions (Res. TSE nº 23.526/2017, arts. 12 and 13), and the SGD can withdraw a validator's accreditation (Portaria SGD/MGI nº 11.230/2025, art. 13). Under the Penal Code, electronic fraud using data obtained through social networks, calls, fake emails or device cloning carries four to eight years' imprisonment since Lei nº 15.397/2026, increased by a third against a public entity (art. 171, §§ 2-A and 3).

10 Recent changes and what to watch

- **20 October 2026**: IN ITI nº 38/2026 `In force` tightens injection-attack defences and accepts digital identity documents in videoconference certificate issuance.
- **June 2026**: Portaria SGD/MGI nº 11.229/2025 `In force` formally defines the gov.br levels and requires multi-factor login at silver and gold; Portaria nº 11.230/2025 (in force since 16 December 2025) sets validator accreditation rules.
- **5 May 2026**: IN ITI nº 36/2026 `In force` consolidates certificate-applicant identification, including liveness and national biometric bases.
- **30 April 2026**: Portaria SGD/MGI nº 2.907/2026 `In force` sets the benefits biometric timetable, with the verification service due by 31 December 2026.
- **25 February 2026**: Lei nº 15.352/2026 `In force` makes the data protection authority an autonomous agency.
- **2025 to 2026**: ANPD regulations on public-sector data sharing and on biometric data `Proposed, not adopted`. The sharing draft was consulted on until 12 December 2025; the biometric project is still being scoped.
- **1 March 2032**: end of paper CIN issuance and of old-model card validity `Adopted, effective 1 Mar 2032`.

11 What this means for identity verification

- **Documents**: accept the CIN in all formats and old-model state cards until March 2032, read the QR code and machine readable zone, handle the CRNM for immigrants and treat the CPF as the primary key.
- **Assurance mapping**: design to each service's gov.br and signature level, with step-up.
- **Biometrics**: remote assurance depends on face matching against government bases, with liveness and injection-attack detection where ICP-Brasil rules apply.
- **Fallback**: keep an in-person or assisted route.
- **Evidence**: for certificates keep biometrics, documents, validation results, recordings and audit trails.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- ID document capture and verification for the National Identity Card and older state ID cards, including QR code and machine readable zone checks.
- Biometric liveness and face match for remote identity proofing at the assurance level each service requires.
- Video KYC sessions with recordings and audit trails where remote identification must be equivalent to in-person checks.
- No-code workflow builder to set step-up rules per service and keep an assisted or in-person fallback route.
- Cloud, on-premises or hybrid deployment to fit public-sector data protection and hosting requirements.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Lei nº 14.129, de 29 de março de 2021 [Digital Government Law]**, arts. 2, 14, 25, 26, 28, Câmara dos Deputados consolidated text, camara.leg.br
- **Lei nº 14.063, de 23 de setembro de 2020 [electronic signatures in interactions with public bodies]**, arts. 4 and 5, Câmara dos Deputados consolidated text, camara.leg.br
- **Decreto nº 10.543, de 13 de novembro de 2020 [electronic signatures in the federal administration]**, arts. 3 to 8, Planalto, planalto.gov.br
- **Decreto nº 8.936, de 19 de dezembro de 2016 [gov.br Platform]**, arts. 1, 3, 4, 5, as amended, Planalto, planalto.gov.br

- **Decreto nº 10.977, de 23 de fevereiro de 2022 [National Identity Card]**, arts. 2 to 26 and Annexes I to III, as amended, Planalto, planalto.gov.br
- **Decreto nº 11.797, de 27 de novembro de 2023 [Citizen Identification Service and Cefic]**, arts. 2 to 5 and 9 to 11, Câmara dos Deputados, camara.leg.br
- **Decreto nº 12.069, de 21 de junho de 2024 [National Digital Government Strategy]**, arts. 16 to 18, Planalto, planalto.gov.br
- **Lei nº 15.077, de 27 de dezembro de 2024**, art. 1, Planalto, planalto.gov.br
- **Decreto nº 12.561, de 23 de julho de 2025 [biometric record for social security benefits]**, arts. 2 to 5, Planalto, planalto.gov.br
- **Lei nº 13.444, de 11 de maio de 2017 [National Civil Identification]**, arts. 1 to 4, Planalto, planalto.gov.br
- **Lei nº 14.534, de 11 de janeiro de 2023 [CPF as single number]**, arts. 1 and 2, Câmara dos Deputados, camara.leg.br
- **Resolução CGICN nº 7, de 1º de outubro de 2021 [guidelines for the biometric data check service]**, ICN Management Committee, Diário da Justiça Eletrônico do TSE, 3 December 2021, arts. 1 to 6, tse.jus.br
- **Resolução TSE nº 23.656, de 7 de outubro de 2021 [access to personal data held by the Electoral Justice]**, arts. 2 and 4, Tribunal Superior Eleitoral, tse.jus.br
- **Resolução TSE nº 23.526, de 26 de setembro de 2017 [ICN database]**, arts. 7, 8, 12 and 13, Tribunal Superior Eleitoral, tse.jus.br
- **Instrução Normativa ITI nº 36, de 29 de abril de 2026 [identity confirmation of certificate applicants]**, arts. 1 to 9, 27, 37, 38, as amended by IN ITI nº 38/2026, ITI, gov.br/iti
- **Saiba mais sobre os níveis da conta gov.br [gov.br account levels]**, Digital Government Secretariat, gov.br/governodigital
- **Orientações sobre os critérios de segurança adotados na Conta GOV.BR [security criteria guidance for public managers]**, Digital Government Secretariat, gov.br/governodigital
- **Lei nº 13.709, de 14 de agosto de 2018 (LGPD)**, arts. 11, 23, 26, 52, Câmara dos Deputados consolidated text, camara.leg.br
- **Lei nº 9.613, de 3 de março de 1998 [AML law]**, art. 9, Câmara dos Deputados consolidated text, camara.leg.br
- **ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD**, ANPD, 1 February 2024, gov.br/anpd
- **Nota Técnica nº 23/2025/CON1/CGN/ANPD [consolidation of the biometric data call for input]**, ANPD, November 2025, gov.br/anpd
- **Portaria SGD/MGI nº 11.229, de 12 de dezembro de 2025 [gov.br account levels]**, arts. 3 to 7 and 10, Diário Oficial da União, 16 December 2025, in.gov.br
- **Portaria SGD/MGI nº 11.230, de 12 de dezembro de 2025 [signatures and digital access validators]**, arts. 3 to 13, Diário Oficial da União, 16 December 2025, in.gov.br

- **Portaria SGD/MGI nº 2.907, de 2 de abril de 2026 [biometric base and verification service timetable]**, arts. 2, 3 and 5, Diário Oficial da União, 6 April 2026, in.gov.br
- **Governo do Brasil divulga prazos para adoção gradual do cadastro biométrico** [entry into force of Decreto nº 12.561/2025], Secom, 19 November 2025, gov.br/secom
- **Instrução Normativa ITI nº 38, de 19 de outubro de 2026**, arts. 1 to 5, ITI, gov.br/iti
- **Portaria SGD/MGI nº 7.076, de 2 de outubro de 2024 [integration with gov.br authentication and advanced signature]**, arts. 3, 4 and 8, Diário Oficial da União (republished version), in.gov.br
- **Portaria Conjunta ITI/CC/PR SGD/SEDGG/ME nº 1, de 8 de setembro de 2021 [cryptographic standards for advanced signatures]**, Diário Oficial da União, 17 September 2021, in.gov.br
- **Dúvidas Frequentes do Ecossistema da Identidade Digital GOV.BR [integration FAQ]**, Digital Government Secretariat, gov.br/governodigital
- **Imposto de Renda 2026: saiba como ter uma conta Prata ou Ouro no GOV.BR**, MGI, 19 March 2026, gov.br/gestao
- **Conta gov.br [account levels and authentication]** and **Requisitos para acesso aos serviços [service access requirements]**, Digital Government Secretariat, gov.br/governodigital
- **Dúvidas para aumentar o nível com a CIN [gold level with the CIN]** and **Ativar a verificação em duas etapas [two-step verification]**, Digital Government Secretariat, gov.br/governodigital
- **Como acessar com a conta gov.br [e-CAC access]**, Federal Revenue Service, gov.br/receitafederal
- **Lei nº 15.352, de 25 de fevereiro de 2026 [Agência Nacional de Proteção de Dados]**, art. 1, Câmara dos Deputados, camara.leg.br
- **Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [Penal Code]**, art. 171, as amended by Lei nº 15.397/2026, Câmara dos Deputados consolidated text, camara.leg.br
- **Decreto nº 9.199, de 20 de novembro de 2017 [Migration Law regulation]**, arts. 58, 62, 63, Câmara dos Deputados consolidated text, camara.leg.br
- **Balanço da Agenda Regulatória 2025-2026, 1º semestre de 2026 [regulatory agenda review]**, ANPD, gov.br/anpd