Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Brazil

COUNTRY Brazil

INDUSTRY Banking & Digital Banking

LAST UPDATED 11 November 2026

KEY REGULATORS Central Bank of Brazil · National Monetary Council · Council for Financial Activities Control

Key takeaways

- Taking deposits in Brazil requires prior authorisation from the Central Bank of Brazil (BCB). Digital banks use the same licence types as any other bank, and since December 2025 a firm's legal name, brand and internet domain must not suggest a type of institution it is not licensed as.
- A bank may open a deposit account entirely through an app or website. The rules set no fixed list of documents or biometric methods, but the bank must verify and validate identity before the relationship starts; missing income and other qualification data may follow within 30 days.
- Since 1 December 2025, every new current, savings or prepaid account must first be checked against BC Protege+, the central bank's register where people can block accounts being opened in their name.
- Brands without a banking licence can offer a bank's accounts only as its correspondent (acting in its name) or through a regulated Banking as a Service (BaaS) contract; either way the licensed bank keeps full responsibility for know-your-customer (KYC), fraud and anti-money laundering (AML) checks. Existing partnerships must comply by 31 December 2026.
- Cash reporting now reaches crypto and foreign cash: from 1 October 2026, transfers to or from self-custody crypto wallets and foreign-currency cash operations of US$10,000 or more must be reported to the financial intelligence unit, with the first reports due on the first business day of January 2027.

Brazil is open to digital banks, but entry is through the same licensing gate as any bank: authorisation from the BCB under rules set by the National Monetary Council (CMN). The anti-money laundering rulebook (BCB Circular 3.978/2020) and the account-opening rule (CMN Resolution 4.753/2019) apply in the same way whether a customer walks into a branch or downloads an app.

The principal authorities are the BCB (licensing, prudential and conduct supervision, AML rules for the institutions it authorises), the CMN (system-wide rules) and the Council for Financial Activities Control (COAF), the financial intelligence unit. The single biggest obstacle for a new entrant is no longer remote onboarding itself, but the 2025 to 2026 wave of anti-fraud and anti-impersonation rules: naming rules, BaaS limits, mandatory fraud checks before accounts are opened, and Pix security requirements.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 AML, KYC and customer due diligence
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
Banco Central do Brasil (Central Bank of Brazil, BCB)	Authorises and supervises banks; issues AML/CFT, account-opening, fraud-prevention and Pix rules; imposes sanctions	National	bcb.gov.br
Conselho Monetário Nacional (National Monetary Council, CMN)	Sets system-wide rules, including account opening and cybersecurity; issues joint resolutions with the BCB	National	Published by the BCB
Conselho de Controle de Atividades Financeiras (COAF)	Financial intelligence unit, administratively linked to the BCB with technical and operational autonomy; receives suspicious and cash transaction reports	National	gov.br/coaf
Comissão de Valores Mobiliários (CVM)	Securities regulator; AML rules for brokers and other securities intermediaries	National	gov.br/cvm
Agência Nacional de Proteção de Dados (National Data Protection Agency, ANPD)	Data protection authority under the Brazilian Data Protection Law (LGPD)	National	gov.br/anpd

Financial Action Task Force (FATF) and Financial Action Task Force of Latin America (GAFILAT)	Joint mutual evaluation of December 2023 rated preventive measures (Immediate Outcome 4) and supervision (Immediate Outcome 3) moderately effective; banks were among the most heavily weighted sectors	Supranational	fatf-gafi.org, gafilat.org
Fundo Garantidor de Créditos (FGC)	Deposit guarantee fund whose statute and regulation are approved by the CMN	National	fgc.org.br

2 Licensing and authorisation

Financial institutions need prior BCB authorisation (Law 4.595/1964, Article 18). CMN Resolution 4.970/2021 sets the process for banks, credit cooperatives, direct credit companies and other institution types. Applicants must show controllers' financial capacity, lawful capital, economic viability, adequate IT and governance, and capable managers (Article 2).

Joint Resolution 14/2025 replaced fixed minimum capital with a methodology based on the categories of operational, investment and funding activity an institution carries on; for deposit-takers the activity component is multiplied by 200%, the highest factor (Article 10). Existing institutions phase in any increase until 31 December 2027.

Naming and presentation

Joint Resolution 17/2025 `In force since 1 Dec 2025` bars an authorised institution from using any name, brand or internet domain that suggests an activity or institution type it is not authorised for, and requires its own domain in all customer e-mails and links. A payment institution or direct credit company may therefore not present itself as a "bank" unless it belongs to a prudential conglomerate that includes one. Non-compliant institutions had 120 days to file an adequacy plan of at most one year.

Deposits are covered by the FGC up to R$250,000 per person per institution or financial conglomerate (CMN Resolution 4.222/2013, Annex II). Operating a financial institution without authorisation is a crime punishable by one to four years' imprisonment and a fine (Law 7.492/1986, Article 16). Foreign ownership, restricted by Article 52 of the Constitution's transitional provisions unless of government interest, is recognised generally by BCB Circular 3.977/2020 under Decree 10.029/2019, subject to normal authorisation.

3 AML, KYC and customer due diligence

Banks are obliged entities under Article 9 of Law 9.613/1998 (the Money Laundering Law), which covers anyone whose activity includes taking, intermediating and investing third parties' funds. Article 10 requires customer identification and up-to-date records, and Article 11 requires reporting to COAF. For BCB-authorised institutions the detailed rules are in BCB Circular 3.978/2020, as last amended by BCB Resolution 591 of 30 September 2026.

Identification

Collect at least full name and CPF (individual taxpayer) number for individuals, and name and CNPJ (company registration) number for companies, and verify and validate them, if necessary against public and private databases (Article 16). Non-resident individuals exempt from a CPF may be identified by travel document.

Qualification

Collect information on place of residence and financial capacity (income or turnover), check politically exposed person (PEP) status for the person and their family and close associates, and verify according to risk (Articles 18 and 19). PEP status lasts five years after leaving office.

Risk classification

Classify each customer into the risk categories of the internal risk assessment and review the class when the profile changes, with enhanced measures for higher-risk customers (Articles 13 and 20).

No relationship before checks

A business relationship may not begin until identification and qualification are complete; if qualification data are insufficient, it may start for up to 30 days, provided monitoring is not impaired (Article 23).

Beneficial ownership

For corporate customers the bank must trace the ownership chain to the natural person who is the beneficial owner, including anyone who exercises de facto control (Article 24). Each bank sets its own ownership threshold on a risk basis, but it may not exceed 25%, counting direct and indirect holdings (Article 25). Listed companies, non-profits, cooperatives, certain regulated funds and certain non-resident investors are exempt, but their representatives, controllers and directors must still be identified.

Monitoring and reporting

- **Suspicious activity:** transactions selected by monitoring must be analysed within 45 days; if the bank decides to report, the report goes to COAF by the next business day

after the decision (Articles 43 and 48). The analysis may not be outsourced or carried out abroad (Article 44).

- **Cash records:** cash operations above R$2,000 must record the name and CPF of the person carrying the cash (Article 33). Cash withdrawals of R$50,000 or more need three business days' advance notice (Article 36).
- **Mandatory reports to COAF** (Article 49), by the next business day: cash deposits and withdrawals of R$50,000 or more; payments and transfers against cash of R$50,000 or more; requests to provision cash withdrawals of R$50,000 or more; foreign-currency cash exchange of US$10,000 or more `From 1 Oct 2026`; and transfers of virtual assets to or from self-custody wallets of US$10,000 or more `From 1 Oct 2026`. Reports for the last two categories for October to December 2026 are due on the first business day of January 2027.
- **Nil return:** an institution that made no reports in a calendar year must declare this within ten business days after year end (Article 54).

KYC data, transaction records and analysis files must be kept for at least ten years (Article 67). Business with customers, correspondent banks and partners in FATF-listed high-risk jurisdictions requires enhanced measures, including operational limits (BCB Normative Instruction 761/2026). Assets of persons designated under United Nations Security Council sanctions must be frozen under Law 13.810/2019, following the procedures in BCB Resolution 44/2020.

4 Identity verification and onboarding

CMN Resolution 4.753/2019 requires procedures and controls that verify and validate the identity and qualification of account holders and the authenticity of the information they provide, including by comparison with public or private databases (Article 2). Neither this resolution nor Circular 3.978 prescribes documents, a biometric or liveness method, or an assurance level; the CPF is the mandatory identifier, and the bank chooses how to prove the applicant holds it.

- **Simplified accounts:** an account may be opened on simplified qualification if appropriate balance and inflow limits are set (Article 2, paragraph 2). The bank sets the limits in the account contract.
- **BC Protege+:** before opening a current, savings or prepaid payment account, or adding a holder or representative, the bank must query the BCB's restriction register (Article 2-A, in force since 1 December 2025). For a company, the CNPJ and the CPF of every holder and representative must be checked. If a restriction is registered, opening anyway is

permitted only in documented exceptional cases, and the query result is kept for ten years (Article 2-A; Normative Instruction 661/2025).

- **Fraud data sharing:** banks must share and consult indications of fraud through a shared system, on the basis of contractual consent (Joint Resolution 6/2023).
- **Security:** account-opening technology must protect the integrity, authenticity and confidentiality of electronic documents (Article 7).

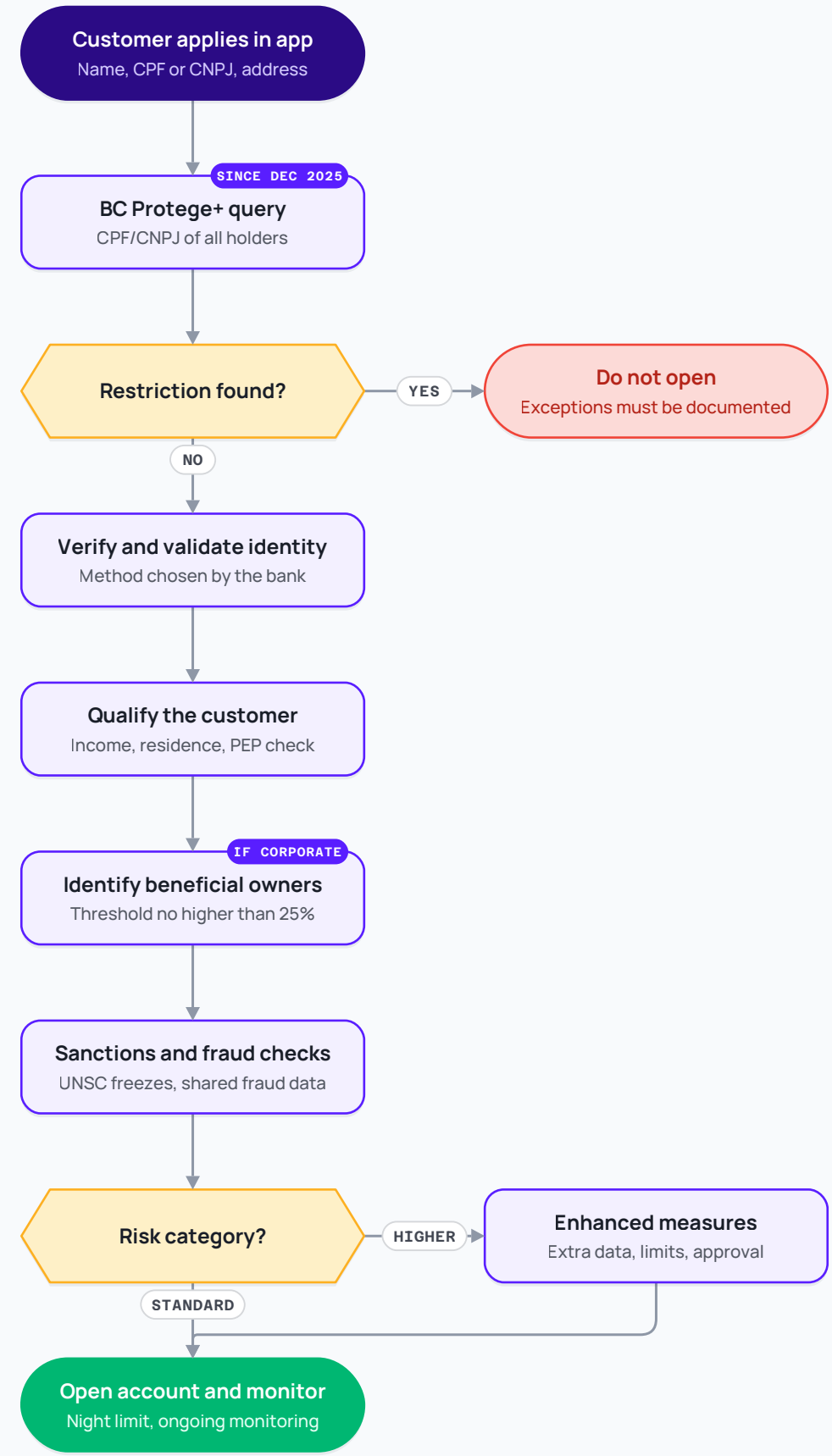


Figure 1. Remote deposit account opening at a BCB-authorised bank.

5 Digital channels: what's different

Bottom line: the identification, qualification and reporting rules are channel-neutral; what changes online is the anti-fraud layer around the account (transfer limits, a 24-hour wait to raise them, and strict rules for brands that distribute a bank's accounts through their own apps).

Requirement	In person / branch	Online / remote	Difference
Opening a deposit account	Permitted	Permitted by electronic means; not by voice telephone	Same
Identity verification standard	Verify and validate, including database checks	Same obligation; method chosen by the bank	Same
Risk rating	Risk-based	Risk-based; remote opening is not an automatic enhanced due diligence trigger	Same
BC Protege+ query before opening	Required	Required	Same
Cash thresholds (R$2,000 record, R$50,000 report)	Apply at the counter	Not triggered by electronic transfers, which are covered by monitoring	Differs
Raising transfer limits	Per bank policy	Increase requested in electronic channels takes effect after at least 24 hours	Differs
Distribution by a non-bank brand	Banking correspondent acting for the bank, which bears full responsibility	Correspondent via its own website or app, or a BaaS contract (electronic channel only)	Differs

Pix from a new device	Not applicable	A device never used for Pix must be registered first, with identity confirmation and two-factor authentication; unregistered devices capped at R$200 per transaction and R$1,000 per day	`Differs`
Closing the account	At the branch	Must be possible through the channel used to open it	`Same`

Remote opening is permitted, not privileged

CMN Resolution 4.753, Article 3, allows accounts to be opened and closed through any service channel the bank offers, including electronic means (defined as remote channels without in-person contact), but not voice telephony. Circular 3.978 does not treat remote onboarding as higher risk in itself, but the internal risk assessment must cover all distribution channels and new technologies (Article 10).

Transfer limits and fraud rejection

Under BCB Resolution 142/2021, banks must cap transfers between different individuals from 8 p.m. to 6 a.m. at R$1,000 per account per payment scheme (Pix, TED, internal transfers, boletos), and a customer's request to raise limits in electronic channels may take effect only after at least 24 hours (Article 2). Since 13 October 2025, institutions must reject payments to current, savings or prepaid accounts where there is well-founded suspicion of involvement in fraud, and the institution holding the account must inform its holder (Article 2-A). Under the Pix Regulation (BCB Resolution 1/2020, Article 89), account opening needs robust security, and individuals may initiate Pix from a device never before used for Pix only after registering it. Registration requires confirming the holder's identity (by personal data, tokens, one-time passwords or biometrics) and two-factor authentication; unregistered devices are capped at R$200 per transaction and R$1,000 per day (BCB Normative Instruction 491/2024, Articles 4 and 9).

Banking as a Service

Joint Resolution 16/2025 limits BaaS to account opening and maintenance, payments through those accounts, merchant acquiring and credit, delivered only through an electronic channel. The customer holds the account at the licensed bank, which remains responsible for KYC, fraud prevention and AML; the brand may perform only ancillary tasks with the bank's tools. A brand may not use a bank-like name, must tell customers it is not authorised by the BCB, and may hold a deposit-account BaaS contract with only one provider. Existing contracts must comply by 31 December 2026

`Transition ends 31 Dec 2026`. Providers must list their partner brands on their websites and, since 1 October 2026, register them in the BCB's Unicad system.

6 Data protection and biometrics

The Brazilian Data Protection Law (LGPD, Law 13.709/2018) classifies biometric data linked to a natural person as sensitive (Article 5, II). Article 11, II, (g) allows sensitive data to be processed without consent where indispensable for fraud prevention and the data subject's security in identification and authentication processes in electronic systems, unless the data subject's fundamental rights prevail. Onboarding biometrics can thus rest on a basis other than consent if indispensable. A specific ANPD regulation on biometric data is on its 2025 to 2026 regulatory agenda; no draft had been published by November 2026.

Banking secrecy under Complementary Law 105/2001 also applies; in a BaaS arrangement the bank may not give the partner brand access to the BCB's Credit Information System (Joint Resolution 16/2025, Article 10). The ANPD can fine up to 2% of Brazilian turnover, capped at R$50 million per infringement (LGPD, Article 52).

7 Sector-specific obligations

Cybersecurity and outsourcing

CMN Resolution 4.893/2021, as amended by CMN Resolution 5.274/2025, requires a cybersecurity policy covering authentication, encryption, end-to-end audit trails, vulnerability management, multi-factor remote access and dark web monitoring. Pix and reserve transfer (STR) environments must be isolated, with multi-factor administrative access, and annual independent penetration tests are mandatory (adaptation deadline 1 March 2026).

Account closure for unlicensed financial services

Since 1 December 2025, banks must close accounts used to provide financial or payment services without authorisation, such as paying on behalf of hidden third parties (CMN Resolution 4.753, Article 6, as amended by CMN Resolution 5.261/2025). Criteria must be documented and approved by the executive board (diretoria).

Payments to betting operators

Banks must block unlicensed betting operators' accounts within 24 hours of a Ministry of Finance notice and report them to COAF (Law 14.790/2023, Article 21-A, as amended in 2026; CMN Resolution 5.320/2026). Provisional Measure 1.394/2026 then banned fixed-odds betting; banks may process betting payments only for wind-down and refunds (Article 14; BCB Resolution 597/2026).

Securities side

Securities brokers follow CVM Resolution 50/2021, which since CVM Resolution 245/2026 requires enhanced due diligence for investors linked to FATF-listed jurisdictions.

8 Risk indicators and red flags

Selected situations from BCB Circular Letter 4.001/2020 most relevant to digital banking:

ACCOUNT OPENING AND MOVEMENT RED FLAGS (CIRCULAR LETTER 4.001/2020)

- **Batch openings**: several accounts registered on the same date or in a short period with common elements such as address, telephone or representatives.
- **Shared IP or e-mail**: the same e-mail address or Internet Protocol (IP) address used by different legal entities.
- **Hidden owner**: transactions where the beneficial owner cannot be identified.
- **Funnel accounts**: deposits from many sources with no economic rationale, especially from regions far from the customer.
- **Pass-through**: cash withdrawals from an account that receives many electronic transfers from various origins in a short time.
- **Threshold avoidance**: amounts just below reporting limits.
- **Public funds**: attempts to withdraw in cash funds from parliamentary amendments (added May 2026).

9 Enforcement and penalties

For breaches of the identification, record-keeping and reporting duties, Law 9.613/1998, Article 12, allows a warning, a fine not exceeding twice the transaction value, twice the

profit obtained or R$20 million, disqualification of managers for up to ten years, and suspension or revocation of authorisation. For other BCB and CMN rule breaches, Law 13.506/2017, Article 7, caps fines at the higher of 0.5% of the previous year's revenue from financial services and products or R$2 billion, and the BCB may agree settlement commitments (termos de compromisso) under Article 11.

In August 2026 the BCB's sanctions committee fined Banco Genial R$21,560,000 for inadequate AML controls, failing to verify the qualification of foreign-exchange customers and late or deficient reporting of suspicious transactions to COAF; a director was barred for six years. In May 2026 Banco Topázio was fined R$16,280,000 on similar grounds and banned for two years from certain foreign-exchange operations. The fines were under appeal as of November 2026; the ban was in effect.

10 Recent changes and what to watch

- **1 Oct 2026, BCB Resolution 591** `In force`: COAF reports for foreign-currency cash and self-custody crypto transfers of US$10,000 or more; first reports due January 2027.
- **25 Sep 2026, Provisional Measure 1.394** `In force, pending conversion`: fixed-odds betting banned; banks must refuse betting payments. It lapses unless Congress converts it into law.
- **9 Jul 2026, BCB Normative Instruction 761** `In force`: enhanced measures, including operational limits, for business linked to FATF high-risk jurisdictions.
- **24 Mar 2026, Law 15.358** `In force`: courts may order blocks on accounts and Pix in organised crime cases; banks must block unlicensed betting operators.
- **1 Dec 2025, BC Protege+ and account closure** `In force`: register check before opening accounts; closure of accounts used for unlicensed financial services.
- **28 Nov 2025, Joint Resolutions 16 and 17** `BaaS transition ends 31 Dec 2026`: BaaS framework and naming rules.
- **Bill 3.019/2026** `Bill, not enacted`: would let prosecutors and police order five-day emergency freezes that banks must execute immediately; awaiting the Senate plenary.

11 What this means for identity verification

- **The CPF is the anchor.** Validate it against databases and check BC Protege+ for every holder and representative.

- **Method is the bank's choice.** Write the criteria into the KYC manual approved by the executive board.
- **Document the biometric legal basis** under LGPD Article 11.
- **Collect more than identity:** residence, income, PEP status and beneficial owners at onboarding.
- **Keep evidence for ten years:** KYC data from the end of the relationship, and BC Protege+ query results.
- **Device registration is an identity check:** confirm the holder and use two factors before enabling Pix on a new device.

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:

- Remote KYC onboarding with ID document capture and verification, face match and biometric liveness, configurable to each bank's documented verification criteria.
- KYB and beneficial owner verification to trace corporate ownership chains down to the natural persons behind them.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring as customer risk changes.
- No-code workflow builder to add steps such as registry checks, proof of address and KYC questionnaires, with an audit trail for each decision.
- Cloud, on-premises or hybrid deployment to fit data residency and outsourcing 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 9.613, de 3 de março de 1998 [Money Laundering Law]**, arts. 9 to 12, compiled text, Presidência da República, planalto.gov.br
- **Lei nº 4.595, de 31 de dezembro de 1964 [Banking Reform Law]**, art. 18, Presidência da República, planalto.gov.br
- **Lei nº 7.492, de 16 de junho de 1986 [Financial System Crimes Law]**, art. 16, Presidência da República, planalto.gov.br
- **Lei nº 13.506, de 13 de novembro de 2017 [Administrative Sanctioning Proceedings Law]**, arts. 7 and 11, Presidência da República, planalto.gov.br
- **Lei nº 13.709, de 14 de agosto de 2018 [Brazilian Data Protection Law (LGPD)]**, arts. 5, 11 and 52, compiled text, Presidência da República, planalto.gov.br
- **Lei nº 13.810, de 8 de março de 2019 [implementation of UN Security Council sanctions]**, art. 9, Presidência da República, planalto.gov.br
- **Lei Complementar nº 105, de 10 de janeiro de 2001 [banking secrecy]**, art. 1, Presidência da República, planalto.gov.br
- **Circular nº 3.978, de 23 de janeiro de 2020 [AML/CFT policy, procedures and controls]**, consolidated text including Resolução BCB nº 591/2026, BCB, bcb.gov.br
- **Resolução BCB nº 591, de 30 de setembro de 2026** [amends Circular 3.978, art. 49], BCB, bcb.gov.br
- **Carta Circular nº 4.001, de 29 de janeiro de 2020 [list of suspicious operations and situations]**, consolidated text including Instrução Normativa BCB nº 732/2026, BCB, bcb.gov.br
- **Instrução Normativa BCB nº 761, de 9 de julho de 2026 [enhanced measures, FATF high-risk jurisdictions]**, BCB, bcb.gov.br
- **Resolução nº 4.753, de 26 de setembro de 2019 [opening, maintenance and closure of deposit accounts]**, consolidated text including CMN Resolutions 5.218/2025 and 5.261/2025, BCB, bcb.gov.br
- **Resolução BCB nº 475, de 26 de maio de 2025 [contracting restriction system]**, BCB, bcb.gov.br
- **Instrução Normativa BCB nº 661, de 11 de setembro de 2025 [BC Protege+ operating procedures]**, BCB, bcb.gov.br
- **Resolução Conjunta nº 6, de 23 de maio de 2023 [sharing of fraud indications]**, BCB, bcb.gov.br
- **Resolução BCB nº 142, de 23 de setembro de 2021 [fraud prevention in payment services]**, as amended by Resoluções BCB nº 501/2025 and 584/2026, BCB, bcb.gov.br
- **Resolução Conjunta nº 16, de 28 de novembro de 2025 [Banking as a Service]**, BCB, bcb.gov.br
- **Resolução Conjunta nº 17, de 28 de novembro de 2025 [naming and presentation to the public]**, BCB, bcb.gov.br
- **Resolução Conjunta nº 14, de 3 de novembro de 2025 [minimum capital methodology]**, as amended by Resolução Conjunta nº 19/2026, BCB, bcb.gov.br
- **Resolução CMN nº 4.970, de 25 de novembro de 2021 [authorisation processes]**, BCB, bcb.gov.br

- **Resolução CMN nº 4.893, de 26 de fevereiro de 2021 [cybersecurity policy and cloud services]**, and **Resolução CMN nº 5.274, de 18 de dezembro de 2025**, BCB, bcb.gov.br
- **Resolução nº 4.222, de 23 de maio de 2013 [FGC statute and regulation]**, Annex II, consolidated, BCB, bcb.gov.br
- **Resolução BCB nº 44, de 24 de novembro de 2020 [implementation of Law 13.810/2019 sanctions]**, BCB, bcb.gov.br
- **Constituição Federal, Ato das Disposições Constitucionais Transitórias [Constitution, transitional provisions]**, art. 52, Presidência da República, planalto.gov.br
- **Decreto nº 10.029, de 26 de setembro de 2019 [delegation to the BCB on foreign participation]**, Presidência da República, planalto.gov.br
- **Lei nº 15.358, de 24 de março de 2026 [organised crime framework law]**, arts. 9 and 42 (amending Lei 14.790/2023, arts. 21-A, 24-A and 24-C), Presidência da República, planalto.gov.br
- **Medida Provisória nº 1.394, de 25 de setembro de 2026 [ban on fixed-odds betting]**, arts. 1 and 14, Presidência da República, planalto.gov.br; status: senado.leg.br
- **Lei nº 14.790, de 29 de dezembro de 2023 [fixed-odds betting law]**, arts. 21-A, 24-A and 24-C as amended by Lei 15.358/2026 and Medida Provisória 1.394/2026, compiled text, Presidência da República, planalto.gov.br
- **Resolução CMN nº 5.320, de 25 de junho de 2026 [blocking accounts of unlicensed betting operators]**, BCB, bcb.gov.br
- **Resolução BCB nº 597, de 30 de setembro de 2026 [Pix: block on fixed-odds betting payments]**, BCB, bcb.gov.br
- **Instrução Normativa BCB nº 491, de 23 de julho de 2024 [Pix device registration and limits]**, as amended by Instrução Normativa BCB nº 594/2025, arts. 4 and 9, BCB, bcb.gov.br
- **Circular nº 3.977, de 22 de janeiro de 2020 [foreign participation in financial institutions]**, BCB, bcb.gov.br
- **Resolução CMN nº 4.935, de 29 de julho de 2021 [correspondents in the country]**, BCB, bcb.gov.br
- **Resolução BCB nº 1, de 12 de agosto de 2020 [Pix arrangement and Regulation]**, Regulation art. 89, compiled version, BCB, bcb.gov.br
- **Instrução Normativa BCB nº 754, de 1º de julho de 2026 [Unicad registration of BaaS partners]**, as amended by Instrução Normativa BCB nº 776/2026, BCB, bcb.gov.br
- **Resolução BCB nº 427, de 16 de outubro de 2024 [COAF internal rules]**, annex art. 2, BCB, bcb.gov.br
- **Agenda Regulatória 2025-2026, item 4: Dados Pessoais Sensíveis, Dados Biométricos [ANPD regulatory agenda]**, ANPD, gov.br/anpd
- **Resolução CVM nº 50, de 31 de agosto de 2021 [AML for securities market]**, consolidated text including Resolução CVM nº 245/2026, CVM, cvm.gov.br
- **Ata da 47ª Sessão do Copas, 11 de maio de 2026 [BCB sanctions committee minutes, PAS 266470]**, BCB, bcb.gov.br

- **Ata da 48ª Sessão do Copas, 12 de agosto de 2026 [BCB sanctions committee minutes, PAS 280965]**, BCB, bcb.gov.br
- **Quadro geral de penalidades em processo administrativo sancionador [BCB sanctions open data]**, BCB, olinda.bcb.gov.br
- **Mutual Evaluation Report of Brazil**, FATF and GAFILAT, December 2023, Table 1 (effectiveness ratings) and section 5.2, fatf-gafi.org; Spanish edition (Informe de Evaluación Mutua de la Cuarta Ronda), gafilat.org
- **Projeto de Lei nº 3.019, de 2026 [bill amending Law 9.613/1998]**, Senado Federal, senado.leg.br