



MINISTÉRIO DA FAZENDA

OFÍCIO SEI Nº 64095/2025/MF

Brasília, 12 de novembro de 2025.

A Sua Excelência o Senhor
Deputado Carlos Veras
Primeiro-Secretário da Câmara dos Deputados

Assunto: Requerimento de Informação.

Senhor Primeiro-Secretário,

Refiro-me ao Ofício 1ª Sec/RI/E/nº 359, de 08.10.2025, dessa Primeira-Secretaria, por intermédio do qual foi remetida cópia do Requerimento de Informação nº 5219/2025, de autoria do Deputado Marcel Van Hattem, que solicita “informações ao Ministro da Fazenda, Sr. Fernando Haddad, sobre a aplicação da Lei Magnitsky (Global Magnitsky Human Rights Accountability Act) pelo Banco do Brasil e pela Caixa Econômica Federal”.

A propósito, encaminho a Vossa Excelência, em resposta à solicitação dos Deputados, o Ofício USI e UNI 2025/2130, do Banco do Brasil e o Ofício nº 0009/2025/VICOR, Anexo _I_PLD_FTD_INGLES e Anexo _I_PLD_FTD, da Caixa Econômica Federal.

Atenciosamente,

Documento assinado eletronicamente

FERNANDO HADDAD

Ministro de Estado da Fazenda



Documento assinado eletronicamente por **Fernando Haddad, Ministro(a) de Estado**, em 12/11/2025, às 22:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://colaboragov.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **55171455** e o código CRC **CCA5C761**.

Esplanada dos Ministérios, Bloco P, 5º andar - Bairro Zona Cívico-Administrativa
CEP 70048-900 - Brasília/DF
(61) 3412-2539 - e-mail aap.df.gmf@economia.gov.br - gov.br/fazenda

Processo nº 19995.008609/2025-66.

SEI nº 55171455

1. PURPOSE

1.1 Preventing CAIXA from being used for money laundering, terrorism financing and financing of the proliferation of mass destruction weapons, in order to mitigate image, legal and reputational risks.

2. LEGAL MOTIVATION

2.1 Compliance with Federal Law nr. 9.613/1998 (Mar 3rd, 1998), BCB¹ Circular nr. 3.978/2020 (Feb 23rd, 2020), CVM² Resolution nr. 50/2021 (Aug 31st, 2021), regarding the establishment and implementation of the Policy for Anti-Money Laundering, Counter-Terrorist Financing, and Countering the Financing of the Proliferation of Weapons of Mass Destruction.

2.2 Accordance with the strategic objectives outlined in CAIXA Institutional Strategic Plan.

3. TERM AND TERMINATION

3.1 This Policy remains in force for five (5) years from its publication date and its content may be updated in case of CAIXA management board identifies any need for improvements, always taking into account the regulatory environment, macroeconomic context, strategic requirements and/or specific requests from the board responsible for approving the matter, as well as any determination made by regulatory and inspection bodies.

4. GUIDELINES

4.1 AML/CTF Strategy

4.1.1 CAIXA adopts the Risk-Based Approach (RBA) to enable reinforced management and mitigation controls for higher risk situations and basic procedures for lower risk situations.

4.1.1.1 The enforcement of Risk-Based Approach is based on CAIXA Internal Risk Assessment, which considers the risk profile of customers, company, operations, transactions, products, and services, covering all distribution channels and the adoption of new technologies, in addition to the activities carried out by employees, partners and outsourced service providers.

4.1.1.1.1 The Internal Risk Assessment covers a methodology for measuring the probability of occurrence, as well as the scale of financial, legal, and reputational impacts for the company.

¹ Central Bank of Brazil (Banco Central do Brasil) – Brazilian banking regulator: <https://www.bcb.gov.br/>

² Federal Securities Commission (Comissão de Valores Mobiliários): <https://www.gov.br/cvm/pt-br>

4.1.1.1.2 The Internal Risk Assessment considers the largest possible number of variables, and is ought to be reviewed every two years, or whenever any eventual improvement is identified.

4.1.2 The procedures for assessment and prior analysis of new products, as well as the use of new technologies, consider the potential risks and weaknesses from an AML/CTF perspective and provide for adoption of mitigating measures compatible with mapped risks.

4.1.3 CAIXA promotes the AML/CTF acculturation program for employees, partners, and outsourced service providers, which is developed and applied according to the target audience.

4.1.4 CAIXA promotes and develops AML/CTF training programs according to the target public, which includes CAIXA employees, as well as Lottery Units and CAIXA Banking Correspondents (CAIXA Aqui).

4.1.5 CAIXA adopts procedures for recording transactions, operations, and financial services, in accordance with external regulatory requirements, which include the identification of the origin and destination of funds to enable the monitoring of AML/CTF.

4.1.6 The monitoring and screening of suspicious operations are made through predictive models, based upon artificial intelligence and/or statistical techniques, aiming at accuracy and strict compliance with legal deadlines.

4.1.7 Procedures for assessment and report of suspicious transactions, as well as operations and proposals are guided by, but not limited to, current legislation, in order to provide assertive reporting to Brazilian Financial Intelligence Unit (Coaf³) and strict compliance with legal deadlines.

4.1.8 CAIXA ensures the quality of information provided through reports of suspicious activities, assuring its authenticity before sending it to the regulatory body (Coaf).

4.1.9 Information on the parameters and other data used for monitoring, selecting, assessing, and reporting suspicious ML/FT operations and proposals to Coaf is confidential and only shared in accordance with internal regulations.

4.1.10 CAIXA conducts AML/CTF monitoring, screening, assessing, and reporting of suspicious operations, proposals and situations in a confidential manner, with the aim of identifying and paying special attention to suspicions of ML/FT, without disclosing the parts involved, such as partners, outsourced service providers, clients, users, or areas that do not work directly with AML/CTF management, unless expressly required by internal regulations.

4.1.11 CAIXA protects the identity of whistleblowers of suspicious money laundering and terrorism financing operations, proposals, and situations, as well as the identity of employees/managers who carry out AML/CTF procedures.

³ Council of Financial Activities Control (Conselho de Controle de Atividades Financeiras – Coaf): <https://www.gov.br/coaf/pt-br>

4.1.12 CAIXA does not conduct business with Shell Banks.

4.1.13 CAIXA does not allow transfers of funds through anonymous current accounts or accounts linked to fictitious holder(s).

4.1.14 CAIXA complies with the measures imposed by United Nations Security Council (UNSC) sanctions or by the designation of its committees, which determine the unavailability of assets of natural and legal persons or entities.

4.1.15 CAIXA does not conduct business with persons listed on international restrictive ML/FT lists.

4.1.15.1 CAIXA monitors international sanction lists, including those of natural and legal persons and entities with a record of sanctions imposed by the UNSC, as well as other lists defined in internal rules.

4.1.16 CAIXA yearly conducts an Effectiveness Assessment in accordance with mandatory legal requirements, to verify its compliance with AML/CTF policy, procedures, and internal controls.

4.1.16.1 Any deficiencies identified in the Effectiveness Assessment are addressed through action plans, which are monitored by Senior Management.

4.1.17 CAIXA AML/CTF Policy may be extended to companies in the CAIXA Conglomerate, upon formal accession.

4.1.18 Responsible unit: Internal Controls and Integrity Executive Board.

4.2 AML/CTF in Customer Relationship

4.2.1 CAIXA adopts Know Your Customer (KYC) procedures since onboarding and throughout the customer life cycle, in order to mitigate the risk of starting or maintaining connections with people suspected to be involved in money laundering and terrorism financing practices.

4.2.2 The KYC procedures include identifying, qualifying, and classifying customers.

4.2.3 Information related to customer registration data is updated periodically, with intervals based on current legislation analysis and risk criteria established by the Internal Risk Assessment.

4.2.4 CAIXA classifies its customers in risk levels considering AML/CTF aspects, as well as adopts differentiated treatment when conducting business, in accordance with the Internal Risk Assessment.

4.2.5 Registration data is qualified by collecting, verifying, and validating information that is compatible with the customer's risk profile and the nature of the business relationship.

4.2.6 Restrictive measures are adopted for the initiation and maintenance of customers relationships in situations of possible involvement in ML/FT practices.

4.2.7 CAIXA adopts compatible procedures and internal controls for customers qualified as Politically Exposed Person–(PEP), taking this condition into account when classifying risks and evaluating the interest in starting or maintaining a relationship.

4.2.7.1 Such PEP-related procedures and internal controls are also extended to representatives, family members, and close collaborators of these individuals.

4.2.8 CAIXA adopts procedures and internal controls that are compatible with situations in which it is not possible to verify the Ultimate Beneficial Owner.

4.2.9 Responsible unit: Internal Controls and Integrity Executive Board.

4.3 AML/CTF applied to Relationship with Employee / Manager, Partner and Supplier / Outsourced Service Provider

4.3.1 CAIXA adopts procedures to Know Your Employee/Manager (KYE), Know Your Partner (KYP), Know Your Supplier and Outsourced Service Providers (KYS/OSP), including identification, qualification, and risk classification, compatible with its AML/CTF Policy and Internal Risk Assessment.

4.3.2 The procedures aimed at establishing and maintaining relationships with employees/managers, partners, suppliers, and outsourced service providers also consider any updates that may result in a change of risk classification, in order to avoid links with individuals who may be involved in ML/TF suspicious practices.

4.3.3 CAIXA adopts procedures to confirm the information provided by employees/managers, partners, and suppliers/outsourced service providers in financial and non-financial transactions, both domestically and internationally, as well as to verify that these documents have been properly recorded and to evaluate the AML/CTF practices and procedures adopted by partners.

4.3.4 Prior to admission, CAIXA adopts procedures to verify that employees and managers commit themselves to the best practices of integrity for public service and that their names are not associated with any illegal practices.

4.3.5 CAIXA requires its employees and managers to maintain accurate records of their assets and income, including those derived from activities unrelated to their professional responsibilities at the company.

4.3.6 CAIXA requires its employees and managers to inform their immediate superior manager about any other professional activity or employment relationship with another company.

4.3.7 CAIXA adopts appropriate procedures and internal controls to monitor the financial transactions of its staff, employees, and managers, with the aim of identifying ML/TF suspicious transactions and situations, as well as reporting them to the regulatory bodies.

4.3.8 CAIXA relationship with an employee/manager, partner or supplier/outsourced service provider may be interrupted when a possible association to ML/TF practices is identified or non-compliance with regulations or contractual clauses that encourage M/TF by third parties.

4.3.8 In the event that a potential link to LD/FTP practices or non-compliance with regulations or contractual clauses encouraging LD/FTP by third parties is identified, the relationship with the employee/manager, partner, or supplier/outsourced service provider may be terminated.

4.3.9 Responsible unit: Internal Controls and Integrity Executive Board.

5. RESPONSIBILITIES

5.1 CAIXA executives and directors should commit to the effectiveness and continuous improvement of the AML/CTF policy, procedures, and internal controls, as well as to put a governance structure in place to ensure compliance.

5.2 The director responsible for fulfilling the obligations set forth in the AML/CTF rules is in charge with approving the Internal Risk Assessment.

5.3 CAIXA General Secretariat is responsible for formally appointing the director responsible for fulfilling AML/CTF obligations before the Central Bank of Brazil (BCB).

5.3.1 CAIXA Senior Management is responsible for assessing AML/CTF matters.

5.3.1.1 For the purposes of assessing AML/CTF matters, CAIXA Senior Management should be defined as those collegiate bodies appointed by external regulations as the responsible board for the matter to be assessed.

5.3.1.1.1 In the absence of specification by external regulation, the collegiate body responsible for approving the matter will be defined based on the competencies provided for in the CAIXA Bylaws and the Internal Rules of the collegiate bodies.

5.4 All employees, managers and board members should acknowledge CAIXA AML/CTF Policy and should guide their actions in accordance with its guidelines.

5.5 Each CAIXA management unit is responsible to work along with security units in order to prevent, identify, mitigate, or control the inherent risks of its products, services, information protection, processes and/or channels under its management.

5.5 All employees and managers are required to sign the Term of Acknowledgement of AML/CTF Policy (PO006) and to attend AML/CTF training.

5.6 All employees, managers and board members are responsible to promptly report to the AML/CTF management division all situations of which they become aware of, in the course of their duties, that may indicate suspicions of ML/FT activity, whether carried out by customers, employees, managers and board members, partners, suppliers or service providers.

5.7 As the first line of defense, CAIXA units are responsible for mapping ML/FT risks and weaknesses related to products, services, and distribution channels under their management, as well as to take measures to mitigate those risks before making them available to the relationship network.

5.8 CAIXA branches and Service Points are responsible for keeping customer records updated in CAIXA proper system, as well as to provide the information obtained through the effective exercise of the procedures of Know Your Customer, to enable AML/CTF management division to process suspicious ML/FT proposals, operations, and situations.

5.9 CAIXA Branches and Service Points are responsible for performing as the first line of defense in AML/CTF processes, ensuring the proper handling of proposals, operations, and suspicious ML/FT situations, reporting them to the AML/CTF management division in accordance with current regulations.

5.10 CAIXA AML/CTF management division is responsible for performing Internal Risk Assessment to identify and measure the risk of CAIXA products, services and channels being used for the practice of ML/TF.

5.11 AML/CTF management division is responsible to monitor, screen, assess and report suspicious ML/TF operations and situations to the regulatory bodies.

5.12 AML/CTF management division is responsible for ensuring that all staff have access to communication channels for recording suspicious ML/FT proposals, operations, and situations identified during their activities.

5.13 AML/CTF management division is responsible for promoting AML/CTF organizational culture along with Marketing & Communication unit and Training & Development unit, addressed those activities to CTF, all employees/managers, partners, and suppliers/outsourced service providers.

5.14 AML/CTF management division is responsible for acting as the second line of defense for AML/CTF processes through the monitoring of products, services, and distribution channels, especially those that are more susceptible to being used for ML/TF practices, as well as defining procedures for the evaluation and prior analysis of new products, services, and technologies, in view of the risk of ML/TF.

5.15 As the AML/TF third line of defense, CAIXA Internal Audit division is responsible for reporting any risks or weaknesses identified in the AML/CTF process to the AML/CTF management division. the third line of defense.

5.16 The Ombudsman's Office is responsible for receiving and forwarding any complaints related to ML/TF that are submitted via the designated channels, to be processed by the AML/CTF management division.

5.17 Internal Comptroller division is responsible for promoting internal Disciplinary and Civil Liability Investigation, addressing irregular facts and the identification of responsibilities related to the involvement of employees/leaders in suspicious ML/FT situations, reported by the AML/CTF management division, in accordance with current regulations.

5.18 CAIXA Vice-Presidency of the Operating Agent is responsible for adopting the guidelines set forth in this herein policy, as well as in the current regulations applicable to CAIXA Lotteries, with the aim of preventing the use of its products and processes for the practice of ML/TF.



1. Objetivo

1.1 Prevenir que a CAIXA seja utilizada na prática dos ilícitos de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, e mitigar o risco de imagem, legal e reputacional.

2. Motivação

2.1 Alinhamento à Lei nº 9.613, de 03/03/1998, à Circular do Banco Central nº 3.978, de 23/01/2020, e à Resolução CVM nº 50, de 31 de agosto de 2021, no que tange ao estabelecimento e implementação de Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa.

2.2 Aderência aos objetivos estratégicos que compõem o Plano Estratégico Institucional.

3. Vigência

3.1 A vigência desta Política é de 05 (cinco) anos, podendo ser alterada quando o(s) gestor(es) identificar(em) necessidade de aprimoramento, considerando o ambiente regulatório, o contexto macroeconômico, necessidade estratégica ou solicitações do colegiado o qual aprovou a matéria, além de eventual determinação advinda de órgãos reguladores e de fiscalização.

4. Diretrizes

4.1 Estratégia de PLD/FTP

4.1.1 A CAIXA adota a Abordagem Baseada em Risco de forma a possibilitar a implementação de controles de gerenciamento e de mitigação reforçados para as situações de maior risco e simplificados nas situações de menor risco.

4.1.1.1 A Abordagem Baseada em Risco decorre da Avaliação Interna de Risco da CAIXA, que considera os perfis de risco dos clientes, da instituição, das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias, além das atividades exercidas pelos empregados, parceiros e prestadores de serviços terceirizados.

4.1.1.1.1 A Avaliação Interna de Risco contempla metodologia de aferição da probabilidade de ocorrência e da magnitude dos impactos financeiro, jurídico e reputacional para a instituição.



4.1.1.1.2 A Avaliação Interna de Risco considera o maior número possível de variáveis e é revisada a cada dois anos, ou sempre que identificada a necessidade de aprimoramento.

4.1.2 Os procedimentos voltados à avaliação e à análise prévia de novos produtos, bem como da utilização de novas tecnologias, consideram os riscos e fragilidades, sob a ótica de PLD/FTP, e preveem a adoção de medidas mitigatórias compatíveis com os riscos mapeados.

4.1.3 A CAIXA promove ações de aculturação sobre o tema PLD/FTP para empregados, parceiros e prestadores de serviços terceirizados, desenvolvidas e aplicadas de acordo com o público-alvo.

4.1.4 A CAIXA promove ações de capacitação sobre o tema PLD/FTP para empregados da CAIXA e para as Unidades Lotéricas e Correspondentes CAIXA Aqui, desenvolvidas e aplicadas de acordo com o público-alvo.

4.1.5 A CAIXA adota procedimentos de registro de transações, operações e serviços financeiros, de acordo com as previsões normativas externas, inclusive a identificação da origem e do destino dos recursos, de modo a permitir o monitoramento de PLD/FTP.

4.1.6 Os procedimentos de monitoramento e seleção de operações e situações suspeitas de LD/FTP utilizam modelos preditivos, priorizando inteligência artificial e/ou modelos estatísticos, visando à sua acurácia e ao estrito cumprimento dos prazos legais.

4.1.7 Os procedimentos de análise e comunicação de propostas, operações e situações suspeitas são direcionados pelos enquadramentos disponíveis na legislação vigente, não se limitando a eles, e visam à assertividade da comunicação ao COAF e ao estrito cumprimento dos prazos legais.

4.1.8 A CAIXA zela pela qualidade das informações veiculadas nas comunicações com suspeitas de LD/FTP, certificando-se de sua autenticidade antes do envio ao órgão regulador.

4.1.9 Informações sobre os parâmetros e demais dados utilizados para o monitoramento, a seleção, a análise e a comunicação de propostas, operações e situações suspeitas de LD/FTP ao COAF são confidenciais e compartilhadas somente em hipóteses devidamente disciplinadas nos normativos internos.

4.1.10 A CAIXA conduz de forma sigilosa os processos de monitoramento, seleção, análise e comunicação de propostas, operações e situações, com o objetivo de identificar e dispensar especial atenção às suspeitas de LD/FTP, sem dar ciência aos envolvidos, a parceiros, prestadores de serviços terceirizados, clientes e usuários, tampouco às áreas que não atuem diretamente com a gestão de PLD/FTP, salvo se houver previsão expressa nos normativos internos.



4.1.11 A identidade das pessoas físicas que reportam propostas, operações e situações suspeitas de LD/FTP, bem como dos empregados/dirigentes que realizam os procedimentos de PLD/FTP, é mantida em sigilo.

4.1.12 A CAIXA não realiza negócios com *Shell Banks*.

4.1.13 A CAIXA não admite a movimentação de recursos por meio de conta corrente anônima ou vinculada a titular(es) fictício(s).

4.1.14 A CAIXA cumpre as medidas impostas pelas sanções do Conselho de Segurança das Nações Unidas – CSNU ou pelas designações de seus comitês que determinem a indisponibilidade de ativos de pessoas naturais e jurídicas ou de entidades.

4.1.15 A CAIXA não realiza negócios com pessoas relacionadas em listas restritivas internacionais de LD/FTP.

4.1.15.1 As listas internacionais monitoradas pela CAIXA contemplam, necessariamente, a lista de pessoas naturais e jurídicas e entidades com registro de sanções impostas pelo CSNU, bem como demais listas definidas em normas internas.

4.1.16 A CAIXA realiza, anualmente, verificação do cumprimento da política, procedimentos e controles internos de PLD/FTP, por meio da avaliação de efetividade, a qual observa os requisitos legais obrigatórios.

4.1.16.1 As deficiências identificadas na Avaliação de Efetividade são endereçadas por meio de planos de ação que são acompanhados pela Alta Administração.

4.1.17 A Política de PLD/FTP da CAIXA poderá ser estendida para as empresas do Conglomerado CAIXA, mediante adesão formal.

4.1.18 Unidade responsável: Diretoria Executiva Controles Internos e Integridade.

4.2 PLD/FTP no Relacionamento com o Cliente

4.2.1 A CAIXA adota procedimentos destinados a conhecer seus clientes desde a solicitação de início de relacionamento e durante todo o seu ciclo, para mitigar o risco de constituição ou manutenção de vínculos com pessoas com possível envolvimento em práticas de LD/FTP.

4.2.2 Os procedimentos destinados a conhecer os clientes alcançam a identificação, a qualificação e a classificação dos clientes.

4.2.3 As informações relativas aos dados cadastrais de clientes são atualizadas com periodicidade definida a partir da análise da legislação vigente e de critérios de riscos estabelecidos pela Avaliação Interna de Risco.



4.2.4 A CAIXA classifica seus clientes em níveis de risco, considerando aspectos de PLD/FTP, em consonância com a Avaliação Interna de Risco.

4.2.5 A qualificação dos dados cadastrais é realizada por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio.

4.2.6 São adotadas medidas de caráter restritivo para o início e para a manutenção de relacionamento com clientes em situações de possível envolvimento em práticas de LD/FTP.

4.2.7 A CAIXA adota procedimentos e controles internos compatíveis com clientes qualificados como PEP, considera essa condição para fins de classificação de risco e avalia o interesse no início ou na manutenção do relacionamento.

4.2.7.1 Os procedimentos e controles internos se estendem a representantes, familiares e estreitos colaboradores dessas pessoas.

4.2.8 A CAIXA adota procedimentos e controles internos compatíveis com as situações de impossibilidade de verificação do Beneficiário Final.

4.2.9 Unidade responsável: Diretoria Executiva Controles Internos e Integridade.

4.3 PLD/FTP no Relacionamento com Empregado/ Dirigente, Parceiro e Fornecedor/ Prestador de Serviço Terceirizado

4.3.1 A CAIXA adota procedimentos destinados a conhecer seus empregados/dirigentes, parceiros, fornecedores e prestadores de serviços terceirizados, incluindo procedimentos de identificação, qualificação e classificação de risco, compatíveis com esta Política de PLD/FTP e com a Avaliação Interna de Risco.

4.3.2 Os procedimentos destinados a conhecer seus empregados/dirigentes, parceiros, fornecedores e prestadores de serviços terceirizados, na constituição e manutenção do relacionamento, consideram, inclusive, eventuais alterações que impliquem mudança de classificação nas categorias de risco, para evitar vínculos com pessoas com possível envolvimento em práticas de LD/FTP.

4.3.3 A CAIXA adota procedimentos para confirmar as informações apresentadas pelos empregados/dirigentes, parceiros e fornecedores/prestadores de serviços em transações financeiras e não financeiras, no país e no exterior, bem como para verificar se esses documentos foram registrados de maneira adequada e para avaliar as práticas e procedimentos adotados pelos parceiros para PLD/FTP.

4.3.4 São adotados, previamente à contratação, procedimentos que permitam verificar a aderência da conduta dos empregados e dos dirigentes às boas práticas de integridade da administração pública e a vinculação de seu nome à prática de ilícitos.



4.3.5 A CAIXA determina que os seus empregados/dirigentes mantenham o cadastro atualizado, informando patrimônio e renda, inclusive as oriundas de atividades não relacionadas ao exercício profissional na empresa.

4.3.6 CAIXA determina que os seus empregados/dirigentes comuniquem ao seu superior hierárquico o exercício de outra atividade profissional ou relação de emprego estabelecida com outra empresa.

4.3.7 A CAIXA adota procedimentos e controles internos adequados para monitoramento da movimentação financeira do seu corpo funcional, empregados e dirigentes, com o objetivo de identificar operações e situações suspeitas de LD/FTP e comunicá-las aos órgãos reguladores.

4.3.8 O relacionamento com o empregado/dirigente, parceiro ou fornecedor/prestador de serviço terceirizado pode ser interrompido quando for identificada possível vinculação a práticas de LD/FTP ou descumprimentos normativos ou de cláusulas contratuais que propiciem a LD/FTP por terceiros.

4.3.9 Unidade responsável: Diretoria Executiva Controles Internos e Integridade.

5. Responsabilidades

5.1 É de responsabilidade de dirigentes e conselheiros assumir compromisso com a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados à PLD/FTP e dispor de estrutura de governança que assegure seu cumprimento.

5.2 É de responsabilidade do diretor responsável pelo cumprimento das obrigações previstas nas normas de PLD/FTP aprovar a Avaliação Interna de Risco.

5.3 É de responsabilidade da Secretaria Geral indicar formalmente ao Banco Central do Brasil o diretor responsável pelo cumprimento das obrigações de PLD/FTP.

5.3.1 É de responsabilidade da Alta administração apreciar as matérias de PLD/FTP.

5.3.1.1 Para fins de apreciação das matérias de PLD/FTP, entende-se como Alta Administração aqueles colegiados determinados pelas normas externas regulamentadoras das matérias a serem apreciadas.

5.3.1.1.1 Na ausência de especificação pelas normas externas, o colegiado responsável pela aprovação das matérias será definido com base nas competências previstas no Estatuto da CAIXA e no Regimento Interno dos colegiados.

5.4 É responsabilidade de todos os empregados, dirigentes e conselheiros conhecer a Política de PLD/FTP da CAIXA e pautar sua atuação conforme suas diretrizes.



5.7 É responsabilidade da unidade gestora atuar, em conjunto com as áreas de segurança, na prevenção, identificação, mitigação ou controle dos riscos inerentes aos seus produtos, serviços, à proteção das informações, dos processos e/ou dos canais sob sua gestão.

5.5 É responsabilidade de todos os empregados e dirigentes assinar o Termo de Ciência da PO006 e realizar os treinamentos de PLD/FTP.

5.6 É responsabilidade de todos os empregados, dirigentes e conselheiros comunicar prontamente à unidade gestora de PLD/FTP todas as situações de que tenham conhecimento, no desempenho de suas atribuições, que apresentem suspeitas de LD/FTP, quer sejam realizadas por clientes, empregados, dirigentes e conselheiros, parceiros, fornecedores ou prestadores de serviços.

5.7 É de responsabilidade de todas as unidades mapear os riscos e fragilidades de LD/FTP existentes nos produtos, serviços e canais de distribuição, sob sua gestão, e adotar medidas mitigatórias desses riscos, antes de disponibilizá-los para a rede de relacionamento, atuando como primeira linha de defesa.

5.8 É de responsabilidade das Agências e Postos de Atendimento manter atualizados os cadastros dos clientes no sistema de cadastro da CAIXA, bem como fornecer as informações obtidas por meio do efetivo exercício dos procedimentos destinados a conhecer os clientes, de modo a permitir o tratamento das propostas, operações e situações suspeitas de LD/FTP pela unidade gestora de PLD/FTP.

5.9 É de responsabilidade das Agências e Postos de Atendimento atuar como primeira linha de defesa nos processos de PLD/FTP, garantindo o tratamento adequado das propostas, operações e situações suspeitas de LD/FTP, reportando-as à unidade gestora de PLD/FTP, conforme normas vigentes.

5.10 É de responsabilidade da unidade gestora de PLD/FTP realizar Avaliação Interna de Risco com o objetivo de identificar e mensurar o risco de utilização dos produtos, serviços e canais da CAIXA na prática da LD/FTP.

5.11 É de responsabilidade da unidade gestora de PLD/FTP monitorar, selecionar, analisar e comunicar aos órgãos reguladores operações e situações suspeitas de LD/FTP.

5.12 É de responsabilidade da unidade gestora de PLD/FTP assegurar canais de comunicação para todo o corpo funcional registrar propostas, operações e as situações suspeitas de LD/FTP identificadas durante a execução de suas atividades.

5.13 É de responsabilidade da unidade gestora de PLD/FTP, em conjunto com as áreas de *Marketing* e Comunicação e de Desenvolvimento e Aprendizagem, promover a cultura organizacional de PLD/FTP, contemplando os empregados/dirigentes, os parceiros e os fornecedores/prestadores de serviços terceirizados.



5.14 É de responsabilidade da unidade gestora de PLD/FTP atuar como segunda linha de defesa nos processos de PLD/FTP, realizando o monitoramento de produtos, serviços e canais de distribuição, sobretudo aqueles que apresentem maior suscetibilidade para utilização em práticas de LD/FTP, bem como definir procedimentos voltados à avaliação e à análise prévia de novos produtos, serviços e tecnologias, tendo em vista o risco de LD/FTP.

5.15 É de responsabilidade da Auditoria Interna reportar para a unidade gestora de PLD/FTP eventuais riscos e fragilidades identificadas no processo de PLD/FTP durante a atuação da terceira linha de defesa.

5.16 É de responsabilidade da Ouvidoria receber e encaminhar as denúncias relacionadas à LD/FTP, recebidas via canal de denúncias, para tratamento pela unidade gestora de PLD/FTP.

5.17 É de responsabilidade da Corregedoria promover a Apuração de Responsabilidade Disciplinar e Civil, com a investigação de fato irregular e a identificação de responsabilidades relacionadas ao envolvimento de empregados/dirigentes em situações suspeitas de LD/FTP, reportadas pela área gestora da PLD/FTP, conforme normas vigentes.

5.18 É de responsabilidade da Vice-Presidência Agente Operador - VIMAR adotar as diretrizes constantes nesta Política, bem como na regulamentação vigente, aplicável às Loterias CAIXA, de modo a prevenir a utilização dos produtos e processos, sob sua gestão, para a prática de LD/FTP.

Ao
Sr. Fernando Haddad
Ministro de Estado
Ministério de Estado da Fazenda

Ref.: Processo SEI nº 19995.008609/2025-66 – Ofício SEI nº 60473/2025/MF, de 13/10/2025 – Requerimento de Informações da Câmara nº 5.219/2025 – esclarecimentos do Banco do Brasil S.A.

Prezado Sr. Ministro de Estado da Fazenda,

1. Banco do Brasil S.A. (“**BB**” ou “**Banco**”), neste ato representado pelas Unidades Segurança Institucional (“**USI**”) e Negócios Internacionais (“**UNI**”), em atenção ao quanto requisitado no referido ofício, relativamente ao Requerimento de Informações da Câmara (“**RIC**”) nº 5.219/2025, vem, pela presente, prestar os seguintes esclarecimentos em resposta aos questionamentos formulados.

1. Os bancos possuem políticas internas formais destinadas ao cumprimento da Lei Magnitsky? Em caso afirmativo, especificar objetivamente quais são tais políticas, enviando os documentos pertinentes.

Resposta: O Banco atua em plena conformidade com a legislação brasileira, as normas dos mais de 20 países onde está presente e os padrões internacionais que regem o sistema financeiro estando suas normas internas e suas políticas de acordo com a legislação aplicável a cada País.

2. Os bancos realizam monitoramento da lista de pessoas sancionadas (Specially Designated Nationals and Blocked Persons List - SDN List) publicada pelo Office of Foreign Assets Control – OFAC? Em caso positivo, detalhar os procedimentos adotados para o monitoramento, bem como indicar o normativo interno que o fundamenta, com o encaminhamento da documentação pertinente.

3. Existem manuais, circulares, normativos ou comunicados internos que orientem os empregados sobre os procedimentos a serem observados em relação a clientes ou usuários de serviços que constem da SDN List?



Resposta: Em resposta aos questionamentos 2 e 3, o Banco do Brasil atua ainda em mais de 20 países cumprindo as legislações e regulamentações aplicáveis locais, assim como cumpre a legislação brasileira.

Os normativos internos, por sua vez, são protegidos pelo sigilo empresarial, pois contém informações de segurança e estratégicas motivo pelo qual o Banco do Brasil está impossibilitado de divulgá-los nos termos do disposto no artigo 23, §3º, da Lei nº 13.303/2016¹.

4. Os bancos já receberam notificações ou comunicações oficiais de autoridades estrangeiras, em especial do OFAC, relacionadas à aplicação da Lei Magnitsky? Em caso afirmativo, quais medidas foram adotadas pelas instituições para o cumprimento dessas determinações?

5. Os bancos já procederam ao bloqueio, suspensão ou encerramento de contas de clientes em razão da aplicação da Lei Magnitsky?

6. Além das contas, os bancos já determinaram o bloqueio, suspensão ou encerramento de outros serviços financeiros em decorrência da Lei Magnitsky? Em caso positivo, especificar quais.

Em resposta aos questionamentos 4, 5 e 6, as informações solicitadas são consideradas sigilosas sob o enfoque comercial e bancário e, portanto, protegidas na forma do artigo 23, §3º, da Lei nº 13.303/2016.

Ademais, cumpre-nos registrar que eventual resposta sobre o assunto poderia expor situações pertinentes a operações bancárias de clientes identificados ou identificáveis, resultando em violação do sigilo bancário protegido pela Lei Complementar nº 105/2001².

Com base nessas normas o Banco do Brasil está impedido de confirmar ou negar o recebimento de notificação ou comunicação sobre o assunto, bem como confirmar ou negar qualquer informação relativa à existência de prestação de serviços ou de contas.

¹ **Lei 13.303/2016:** Art. 23. [...]

§ 3º Excluem-se da obrigação de publicação a que se refere o § 2º as informações de natureza estratégica cuja divulgação possa ser comprovadamente prejudicial ao interesse da empresa pública ou da sociedade de economia mista.

² “Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.”



7. Qual é o número atual e histórico de clientes e usuários dos serviços financeiros dos bancos que constam ou já constaram da SDN List?

Resposta: Cumpre-nos esclarecer que as informações pertinentes a clientes específicos do Banco do Brasil são protegidas pelo sigilo bancário previsto pela Lei Complementar nº 105/2001, motivo pelo qual a instituição financeira está obrigada, por lei, a manter o sigilo de tal informação.

No entanto, no intuito de colaboração, esclarecemos que a lista de todas as pessoas atualmente sancionadas pela OFAC – SDN List pode ser consultada através do site <https://sanctionssearch.ofac.treas.gov/>.

8. Nos últimos cinco anos, foram realizadas análises jurídicas, auditorias internas ou revisões de compliance com o objetivo de avaliar os riscos de descumprimento da Lei Magnitsky? Em caso positivo, indicar se foram identificados riscos relevantes para os bancos.

9. Quais são os potenciais riscos jurídicos, financeiros e operacionais para os bancos em caso de descumprimento das obrigações decorrentes da referida norma?

Resposta: Em resposta aos questionamentos 8 e 9, o Banco do Brasil esclarece que realiza, continuamente, análise de riscos financeiros e operacionais relativos ao cumprimento de normas legais nos mais de 20 países nos quais atua e conta com assessoramento jurídico especializado para garantir atuação alinhada às melhores práticas de governança, integridade e financeira.

10. Existe avaliação formal sobre os impactos que a aplicação da Lei Magnitsky poderia produzir na estabilidade do sistema financeiro nacional?

Resposta: A avaliação dos impactos que a Lei Magnitsky poderia produzir caberia aos órgãos e entidades responsáveis pela supervisão e acompanhamento da higidez do Sistema Financeiro Nacional, nos termos da Lei nº 4.595/1964³ e regulação aplicável.

³ “Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências.”



11. As instituições já reportaram ao Banco Central do Brasil ou à Comissão de Valores Mobiliários (CVM) eventuais riscos relacionados à não aplicação da Lei Magnitsky?

Resposta: O Banco do Brasil realiza, continuamente, a gestão de riscos e os reportes cabíveis à autoridade de fiscalização competente, nos termos da Lei nº 4.594/1964 e da Resolução CMN nº 4.557/2017⁴.

12. Os bancos participaram, participam ou têm previsão de participar de grupos de trabalho da Federação Brasileira de Bancos (Febraban) ou de outros fóruns institucionais voltados à discussão sobre o cumprimento de sanções decorrentes da Lei Magnitsky? Em caso positivo, quais foram os resultados?

Resposta: As discussões havidas no âmbito dos grupos de trabalho e fóruns da Febraban estão sujeitas ao sigilo empresarial dos partícipes, inclusive demais instituições financeiras privadas, de modo que o Banco do Brasil esclarece que está impedido legalmente de confirmar ou negar a existência de discussões da espécie no âmbito daquela entidade.

13. As instituições mantêm diálogo formal com autoridades norte-americanas acerca da aplicabilidade e do alcance da Lei Magnitsky em relação a clientes no Brasil? Em caso afirmativo, relatar o teor das informações eventualmente fornecidas por tais autoridades.

Resposta: Destacamos que o Banco do Brasil mantém interlocução com autoridades em todos os países em que atua, tratando de diversos temas regulatórios, sendo que as informações prestadas a tais autoridades estão protegidas pelo sigilo empresarial.

2. Sendo o que se tem a informar, reitera-se os protestos de elevada estima e consideração.

Atenciosamente,

⁴ “Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.”



VP Riscos
SBS Quadra 4, Lotes 3/4
Edifício Matriz I, 21º andar
70.070-140 - Brasília - DF

Ofício nº 0009/2025/VICOR #PUBLICO

Brasília/DF, 12 de novembro de 2025.

Ao
Senhor
Wagner Primo Figueiredo Neto
Chefe da Assessoria Especial para Assuntos Parlamentares e Federativos
Ministério da Fazenda
Esplanada dos Ministérios, Bloco P
70.048-900 – Brasília/DF

Assunto: **Requerimento de Informação nº 5219/2025.**

Senhor Chefe da Assessoria Especial,

1. Reportamo-nos ao Despacho constante no Ofício SEI nº 60470/2025/MF, recepcionado em 14/10/2025, por meio do qual esse Ministério encaminhou o Requerimento de Informação (RIC) nº 5219/2025, de autoria do Deputado Federal Marcel Van Hattem (Novo/RS), por meio do qual requer *“informações ao Ministro da Fazenda, Sr. Fernando Haddad, sobre a aplicação da Lei Magnitsky (Global Magnitsky Human Rights Accountability Act) pelo Banco do Brasil e pela Caixa Econômica Federal.”*

2. O referido Requerimento de Informação apresenta os seguintes questionamentos, para os quais tecemos as considerações a seguir:

2.1 *“1. Os bancos possuem políticas internas formais destinadas ao cumprimento da Lei Magnitsky? Em caso afirmativo, especificar objetivamente quais são tais políticas, enviando os documentos pertinentes.”.*

2.1.1 A CAIXA em atendimento à legislação Brasileira na qual está sujeita, segue os preceitos das Leis nº 9.613/1998, nº 13.260/2016 e nº 13.810/2019, além das recomendações do GAFI/FATF, incorporadas à regulamentação nacional, Circular BCB nº 3.978/2020, que fundamentam a política interna formal específica e definem procedimentos para o relacionamento com cliente, monitoramento contínuo e comunicação de operações suspeitas de lavagem de dinheiro e financiamento do terrorismo ao COAF, observando os princípios da Abordagem

Baseada em Risco (ABR), que orienta a aplicação proporcional de controles reforçados para situações de maior risco e simplificados para cenários de menor exposição.

2.1.2 A CAIXA ainda faz uso de listas específicas internacionais a exemplo da lista OFAC com objetivo de identificar eventuais riscos envolvendo clientes, prezando pelas melhores práticas.

2.1.3 Trata-se da Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLD/FTP), encaminhada juntamente com a presente resposta (anexo I), bem como disponível no link a seguir: <https://www.caixa.gov.br/Downloads/caixa-governanca/Politica-PLD-FTP-PRT-ENG.zip>.

2.2 “2. Os bancos realizam monitoramento da lista de pessoas sancionadas (*Specially Designated Nationals and Blocked Persons List - SDN List*) publicada pelo *Office of Foreign Assets Control – OFAC*? Em caso positivo, detalhar os procedimentos adotados para o monitoramento, bem como indicar o normativo interno que o fundamenta, com o encaminhamento da documentação pertinente.”.

2.2.1 Consoante nossa política interna, as listas internacionais monitoradas pela CAIXA contemplam, necessariamente, a lista de pessoas naturais e jurídicas e entidades com registro de sanções impostas pelo CSNU, em atendimento à Lei nº 13.810/2019, bem como demais listas de PLD/FTP definidas em normas internas.

2.2.2 A lista publicada pelo OFAC é consultada diretamente do seu site oficial (<https://sanctionssearch.ofac.treas.gov/>). Por meio de processo automatizado, é realizada a comparação dos dados dos clientes com os registros constantes na referida lista. Esse processo utiliza algoritmos de *matching* textual, baseados em técnicas de similaridade fonética e semântica, para calcular o índice de correspondência entre nomes e atributos correlatos, garantindo maior precisão na identificação de potenciais alertas.

2.2.3 O normativo interno é identificado como Manual Normativo CR432 (Modelos de Monitoramento e Seleção de Operações e Situações Suspeitas de LD/FTP).

2.2.4 O normativo em questão reúne informações técnicas, operacionais e de inteligência classificadas como segredo empresarial, que fundamentam os modelos de monitoramento aplicados à Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa, em conformidade com as Leis nº 9.613/1998, 13.260/2016 e 13.810/2019.

2.3 “*Existem manuais, circulares, normativos ou comunicados internos que orientem os empregados sobre os procedimentos a serem observados em relação a clientes ou usuários de serviços que constem da SDN List?*”

2.3.1 O Manual Normativo relacionado à Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa que estabelece as responsabilidades, procedimentos e gerenciamento de risco para prevenir que a CAIXA seja utilizada para práticas de LD/FTP.

2.4 “4. Os bancos já receberam notificações ou comunicações oficiais de autoridades estrangeiras, em especial do OFAC, relacionadas à aplicação da Lei Magnitsky? Em caso afirmativo, quais medidas foram adotadas pelas instituições para o cumprimento dessas determinações??”.

2.4.1 Informamos que a CAIXA não recebeu notificação ou comunicação oficial de autoridades estrangeiras, em especial do OFAC, relacionadas à aplicação da Lei Magnitsky.

2.4.2 Considerando o item anterior, entendemos que não se aplica.

2.5 “5. Os bancos já procederam ao bloqueio, suspensão ou encerramento de contas de clientes em razão da aplicação da Lei Magnitsky?”.

2.5.1 Primeiramente, em virtude da necessidade de estabelecimento de um horizonte temporal para análise, permita-nos utilizar o período de 5 anos, adotando-se como referência o período solicitado na questão 8.

2.5.2 Nos últimos cinco anos, a CAIXA já procedeu o encerramento de contas de clientes/usuários em decorrência da inclusão de seus titulares na *SDN List*.

2.6 “6. Além das contas, os bancos já determinaram o bloqueio, suspensão ou encerramento de outros serviços financeiros em decorrência da Lei Magnitsky? Em caso positivo, especificar quais.”.

2.6.1 Tendo em vista que os referidos titulares citados na questão anterior não possuíam outros produtos além de contas de depósitos, não houve determinação de bloqueio, suspensão ou encerramento de outros serviços financeiros.

2.6.2 Considerando o item anterior, entendemos que não se aplica.

2.7 “7. Qual é o número atual e histórico de clientes e usuários dos serviços financeiros dos bancos que constam ou já constaram da *SDN List*?”.

2.7.1 As informações sobre clientes e usuários de serviços financeiros são resguardadas pelo sigilo bancário, imposto pela LC nº 105/2001.

2.8 “8. Nos últimos cinco anos, foram realizadas análises jurídicas, auditorias internas ou revisões de compliance com o objetivo de avaliar os riscos de descumprimento da Lei Magnitsky? Em caso positivo, indicar se foram identificados riscos relevantes para os bancos.”.

2.8.1 Considerando a consistência do processo realizado pela CAIXA e em atendimento à legislação nacional, informamos que não foram realizadas análises jurídicas, auditorias internas ou revisões de compliance específica e exclusivamente com o objetivo de avaliar os riscos de descumprimentos da Lei Magnitsky.

2.8.2 Considerando o item anterior, entendemos que não se aplica.

2.9 “9. *Quais são os potenciais riscos jurídicos, financeiros e operacionais para os bancos em caso de descumprimento das obrigações decorrentes da referida norma?*”.

2.9.1 A CAIXA esclarece que possui processos e políticas adequadas a legislação nacional e dessa forma não vislumbra potenciais riscos jurídicos, financeiros e operacionais decorrentes das atuais questões relacionadas à norma em questão.

2.10 “10. *Existe avaliação formal sobre os impactos que a aplicação da Lei Magnitsky poderia produzir na estabilidade do sistema financeiro nacional?*”.

2.10.1 Uma avaliação formal de tais impactos sobre a estabilidade de todo o sistema financeiro nacional necessita de informações dos potenciais impactos de cada integrante do SFN, informações estas que a CAIXA não detém.

2.10.2 Entretanto, considerando o contexto da IF e a natureza de nossas operações, não vislumbramos até o momento impactos que possam contaminar o sistema financeiro nacional.

2.11 “11. *As instituições já reportaram ao Banco Central do Brasil ou à Comissão de Valores Mobiliários (CVM) eventuais riscos relacionados à não aplicação da Lei Magnitsky?*”.

2.11.1 Tendo em vista que a CAIXA não identificou, até o momento, em seu contexto atual impactos relativos à não aplicação da referida Lei, entendemos não caber por parte dessa instituição necessidade de reporte aos reguladores.

2.12 “12. *Os bancos participaram, participam ou têm previsão de participar de grupos de trabalho da Federação Brasileira de Bancos (Febraban) ou de outros fóruns institucionais voltados à discussão sobre o cumprimento de sanções decorrentes da Lei Magnitsky? Em caso positivo, quais foram os resultados?*”.

2.12.1 Informamos que não houve participação, nem tampouco previsão de participação da CAIXA em grupos de trabalho ou em outros fóruns institucionais voltados à discussão sobre o cumprimento de sanções decorrentes da Lei Magnitsky.

2.12.2 Considerando o item anterior, entendemos que não se aplica.

2.13 “13. *As instituições mantêm diálogo formal com autoridades norte-americanas acerca da aplicabilidade e do alcance da Lei Magnitsky em relação a clientes no Brasil? Em caso afirmativo, relatar o teor das informações eventualmente fornecidas por tais autoridades?*”.

2.13.1 A CAIXA não mantém ou manteve diálogo formal com autoridades norte-americanas acerca da aplicabilidade e do alcance da Lei Magnitsky em relação a clientes no Brasil.

2.13.2 Considerando o item anterior, entendemos que não se aplica.

3. Colocamo-nos à disposição para eventuais esclarecimentos necessários.

Respeitosamente,

HENRIETE ALEXANDRA SARTORI Assinado de forma digital por
BERNABE:07867756884 HENRIETE ALEXANDRA SARTORI
BERNABE:07867756884

HENRIETE ALEXANDRA SARTORI BERNABÉ
Vice-Presidente
VP Riscos