ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

VERSÃO PARA DIVULGAÇÃO PÚBLICA

POLÍTICA CORPORATIVA DE PREVENÇÃO A ATOS ILÍCITOS

POLÍTICA CORPORATIVA DE PREVENÇÃO A ATOS ILÍCITOS

1. OBJETIVO

Consolidar os princípios e diretrizes do Conglomerado Itaú Unibanco para promover uma cultura de integridade, ética e prevenção de atos ilícitos, incluindo o combate à lavagem de dinheiro, ao financiamento ao terrorismo, à proliferação de armas de destruição em massa, à corrupção, a fraudes e sinistros. Este documento busca garantir a conformidade com as legislações e regulamentações vigentes, além de se alinhar às melhores práticas nacionais e internacionais.

2. PÚBLICO-ALVO

Esta política aplica-se ao Conglomerado Itaú Unibanco e suas empresas no Brasil e no exterior.
Os requerimentos das políticas e legislações locais, onde se encontram as representações do exterior, deverão ser avaliadas individualmente e seguirão as diretrizes determinadas pela Regra de Governança de PLD/CFT – Unidades Internacionais.

3. INTRODUÇÃO

As instituições financeiras têm papel central na prevenção a atos ilícitos, como lavagem de dinheiro, financiamento do terrorismo, corrupção, fraudes e sinistros. Esses atos envolvem a ocultação de recursos ilegais, o apoio a atividades criminosas ou o uso indevido de estruturas financeiras para fins ilícitos.

A lavagem de dinheiro busca ocultar ou disfarçar a origem criminosa de bens ou valores.

O financiamento do terrorismo e da proliferação de armas de destruição em massa ocorre quando recursos são destinados, direta ou indiretamente, a essas finalidades.

A corrupção envolve o oferecimento ou recebimento de vantagens indevidas para influenciar decisões ou ações.

A fraude se refere a práticas enganosas com objetivo de obter ganhos indevidos.

Sinistros são eventos inesperados que causam prejuízos, como assaltos, furtos ou sequestros.

Embargos e restrições comerciais são medidas impostas por autoridades contra países, empresas ou indivíduos envolvidos em atividades ilícitas.

O desafio está em identificar e impedir operações cada vez mais sofisticadas que tentam mascarar a origem e o destino de recursos ilegais.

O Itaú Unibanco, atento a esse cenário, mantém uma estrutura dedicada à prevenção de atos ilícitos, com foco em governança, transparência, conformidade regulatória e cooperação com autoridades.

4. PAPÉIS E RESPONSABILIDADES

Conselho de Administração
Aprovar diretrizes de supervisão e prevenção de atos ilícitos e acompanhar relatórios de avaliação e planos de ação.

Comitê de Auditoria
Supervisionar o programa corporativo de prevenção a atos ilícitos e receber para ciência os relatórios da área.

Adicionalmente, o Conselho de Administração e Comitê de Auditoria recebem para ciência a Avaliação Interna de Risco, Relatório de Avaliação de Efetividade, bem como os planos de ação elaborados para solucionar deficiências, e seu respectivo Relatório de Acompanhamento

Comissão Superior de Compliance e OpRisk
Definir a orientação estratégica da instituição na prevenção a atos ilícitos. Entre suas principais funções, destacam-se: estabelecer e propor ao Conselho de Administração as diretrizes de prevenção a ilícitos; avaliar os resultados do programa de prevenção; e deliberar sobre situações excepcionais não previstas na política vigente.

Comitê de Gestão de Riscos e Capital
Apoiar o Conselho de Administração na supervisão da gestão de riscos e capital do Itaú Unibanco. Também recebe, para ciência, a Avaliação Interna de Risco elaborada pela DPLD.

Diretoria de Prevenção à Lavagem de Dinheiro
Garantir a efetiva implementação do Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/CFTP) no Conglomerado Itaú Unibanco, no Brasil e no exterior. Suas principais atribuições incluem:

- **Gestão de Riscos**: Elabora e aprova a Avaliação Interna de Risco, define critérios de classificação e acompanha a evolução das tipologias de lavagem de dinheiro e financiamento do terrorismo.
- **Governança e Conformidade:** Assegura o cumprimento da política de PLD/CFTP, valida os procedimentos das áreas de negócio e reporta fatos relevantes ao Comitê de Auditoria.
- **Prevenção e Monitoramento:** Avalia riscos em novos produtos, serviços e tecnologias, e implementa uma abordagem baseada em risco com indicadores de efetividade.
- **Relacionamentos e Parcerias:** Analisa contratos com instituições financeiras estrangeiras e terceiros em arranjos de pagamento, conforme regulamentação vigente.
- **Atribuições do Diretor de PLD/CFTP:** Gerencia riscos estratégicos, aprova a Avaliação Interna de Risco, delega alçadas operacionais e acompanha decisões críticas relacionadas ao programa.

Diretoria de Prevenção a Fraudes
Gerenciar o programa de prevenção a fraudes e sinistros, garantindo a integridade das informações e segurança física.

Unidades de Negócios e Suporte
Implementar controles e procedimentos aderentes às diretrizes corporativas, e garantir a adesão dos colaboradores ao treinamento de integridade.

Jurídico
Auxiliar na análise de requisitos legais e regulatórios, na elaboração de planos de ação de controles de PLD/CFTP, e na avaliação de risco em ocorrências de transações ou operações suspeitas de lavagem de dinheiro, fraudes e sinistros.

Diretoria Compliance e OpRisk
Assegurar, de forma independente, a eficácia dos controles internos por meio de monitoramentos e testes de efetividade. Reporta o risco residual, acompanha deficiências identificadas e elabora relatórios periódicos, conforme os prazos e critérios definidos na política interna e na regulamentação vigente.

Auditoria Interna
Avaliar periodicamente a eficácia da governança, gerenciamento de riscos e controles internos.

Colaboradores e Administradores
Conhecer e seguir as diretrizes, treinamentos e comunicar suspeitas de realização de atos ilícitos.

5. PROGRAMA CORPORATIVO DE PREVENÇÃO A ATOS ILÍCITOS

Com o objetivo de viabilizar o cumprimento das diretrizes desta política e evitar que seus produtos e serviços sejam usados em atividades ilícitas, o Itaú Unibanco estabeleceu Programa de Prevenção a Atos Ilícitos. O programa deverá ser aplicado, no Brasil e nas Unidades Internacionais. Deverá conter minimamente:

5.1. Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo

Políticas e Procedimentos

O Itaú Unibanco adota políticas e procedimentos estruturados que orientam a prevenção a atos ilícitos, em conformidade com normas legais e regulatórias. Essas diretrizes consideram o perfil de risco de clientes, colaboradores, parceiros e operações, promovendo uma atuação proporcional e eficaz.

Avaliação Interna De Risco e Avaliação de Efetividade

Trata-se da avaliação interna com o objetivo de identificar e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo. E devem avaliar a efetividade da política, dos procedimentos e dos controles internos.

A avaliação fundamenta a abordagem baseada em risco, que orienta a aplicação de medidas proporcionais à criticidade dos riscos identificados — reforçadas para riscos elevados e simplificadas para riscos reduzidos — conforme diretrizes internas. E o Relatório de Efetividade inclui a metodologia utilizada, os testes aplicados, a qualificação dos avaliadores e as deficiências identificadas. As ações corretivas decorrentes são acompanhadas por meio de um Relatório de Acompanhamento, assegurando a melhoria contínua do programa.

Identificação de Clientes

Trata-se de um conjunto de ações voltadas à identificação e qualificação de clientes, seus administradores e representantes, por meio da coleta, verificação e validação de informações essenciais para confirmar sua identidade. Esses dados devem ser atualizados e armazenados conforme os prazos regulatórios.

A qualificação completa inclui a verificação da condição de Pessoa Exposta Politicamente (PEP) e a análise da cadeia societária até a identificação do beneficiário final. As diretrizes que orientam esse processo estão descritas na Política Corporativa de Cadastro de Clientes.

Conheça Seu Cliente - KYC

Trata-se de um conjunto de ações destinadas a assegurar a identidade, a atividade econômica e a origem dos recursos dos clientes, permitindo avaliar sua capacidade financeira e prevenir o uso indevido dos produtos e serviços. Quanto mais precisas forem as informações coletadas no início do relacionamento, maior será a eficácia na identificação de riscos e atos ilícitos.

Com base em uma abordagem baseada em risco, clientes com maior exposição são submetidos a análises mais rigorosas.

As diretrizes completas estão descritas nas regras internas, bem como a alçada para iniciar e manter relacionamento com PEPs.

Conheça Seu Parceiro - KYP

Trata-se de um conjunto de práticas destinadas à identificação e qualificação de parceiros comerciais — pessoas jurídicas que mantêm relações contratuais com empresas do Conglomerado, conforme critérios definidos na Política de Governança de Parcerias Comerciais.

Esses parceiros, incluindo correspondentes no país e no exterior, devem ser classificados por categorias de risco, considerando suas atividades. O objetivo é prevenir relações com contrapartes inidôneas ou envolvidas em atividades ilícitas, assegurando que adotem controles adequados de PLD/CFTP. As diretrizes completas estão descritas na regra internas.

Conheça Seu Fornecedor - KYS

Trata-se de um conjunto de práticas voltadas à identificação e qualificação de fornecedores e prestadores de serviços terceirizados, com base na natureza das atividades exercidas e no risco associado ao relacionamento.

Esses agentes devem ser classificados em categorias de risco, e, quando identificada maior exposição a atos ilícitos, são aplicados critérios de diligência mais rigorosos. O objetivo é assegurar relações com contrapartes íntegras e alinhadas às diretrizes de PLD/CFTP. As orientações completas estão descritas nas regras internas.

Conheça Seu Funcionário - KYE

Trata-se de um conjunto de medidas destinadas à identificação e qualificação de colaboradores e candidatos, com foco na prevenção a riscos relacionados à lavagem de dinheiro, financiamento ao terrorismo e outros atos ilícitos.

A classificação por categoria de risco considera as funções desempenhadas, permitindo ações preventivas desde o processo seletivo até o acompanhamento contínuo da conduta. O objetivo é garantir integridade e segurança nas relações de trabalho. As orientações completas estão descritas nas regras internas.

Avaliação de Novos Produtos e Serviços

Trata-se da avaliação previa, sob a ótica de PLD/CFTP, dos riscos dos novos produtos e serviços, incluindo a utilização de novas tecnologias, quando aplicável, devem ser avaliados de forma prévia, conforme as diretrizes internas.

Cumprimento às Sanções
Trata-se de um conjunto de controles voltados ao cumprimento de sanções econômicas, políticas e comerciais impostas por autoridades nacionais e internacionais. Inclui o monitoramento de listas restritivas e a vedação de relações com pessoas, entidades ou países envolvidos em atividades ilícitas. As orientações completas estão descritas nas regras internas.

Monitoramento, Seleção e Análise de Operações Suspeitas
Trata-se de um processo contínuo de monitoramento de transações, com base no perfil e comportamento dos clientes, para identificar indícios de lavagem de dinheiro ou financiamento ao terrorismo. Clientes com maior risco estão sujeitos a regras mais rigorosas e acompanhamento mais frequente.

Esse processo deve ser conduzido de forma independente pela área de PLD/CFTP, segregada das áreas comerciais.

Comunicação de Transações Suspeitas
As operações, situações ou propostas que contêm indícios de lavagem de dinheiro ou de financiamento ao terrorismo devem ser comunicadas aos órgãos reguladores competentes, quando aplicável, em cumprimento às determinações legais e regulamentares. As comunicações de boa-fé não acarretam responsabilidade civil ou administrativa ao Itaú Unibanco, nem a seus administradores e colaboradores.
Informações sobre essas comunicações são restritas, não devendo ser divulgadas a clientes e/ou terceiros.

Treinamento e Conscientização
O programa de treinamento de PLD/CFTP promove a capacitação contínua e dissemina a cultura do tema, alcançando, assim, a aprendizagem e conscientização da sua importância, bem como o aprofundamento e reciclagem do conhecimento. O treinamento deve ser aplicado aos administradores, a todos os colaboradores e parceiros comerciais elegíveis.

As ações de treinamento podem ocorrer por meio de cursos presenciais ou online, palestras, campanhas e outras iniciativas, conforme diretrizes internas.

5.2. Prevenção e Combate a Fraudes
A prevenção e o combate a fraudes são compromissos institucionais que envolvem todos os colaboradores, com base em princípios de ética, integridade e conformidade. As fraudes podem ocorrer por:

- Infrações ao Código de Ética e às normas internas, como adoção de práticas não autorizadas pela empresa, desvios de comportamento e quebra de sigilo e conflito de interesse.
- Descumprimento de obrigações legais e regulatórias, que coloquem em risco a imagem, o patrimônio ou a continuidade da Organização.
- Atos ilícitos como falsificação, estelionato, apropriação indébita, furto, roubo e extorsão.

A atuação preventiva busca identificar comportamentos inadequados, mitigar riscos e proteger a organização, seus clientes e parceiros contra prejuízos financeiros, operacionais e reputacionais.

Avaliação de Riscos no Início do Relacionamento

Os processos de contratação de serviços e produtos devem contemplar procedimentos para prevenir e mitigar o risco de fraude no início do relacionamento com proponentes.

Prevenção e Combate à Fraude Interna

O Itaú Unibanco adota medidas específicas para evitar a ocorrência de fraudes envolvendo seus colaboradores, por meio de diretrizes e procedimentos de controle para prevenção e detecção de atividades irregulares.

Prevenção e Combate à Fraude Contábil

O Itaú Unibanco adota medidas específicas para evitar a ocorrência de fraudes envolvendo seus colaboradores, por meio de diretrizes e procedimentos de controle para prevenção e detecção de atividades irregulares.

Avaliação de Riscos em Novos Produtos e Serviços

Os novos produtos e serviços devem ser avaliados de forma prévia, sob a ótica de prevenção a fraudes, conforme as diretrizes internas.

Monitoramento de Transações

Os produtos e serviços contratados pelos clientes devem ser monitorados para detecção e apuração de situações atípicas ou suspeitas de ocorrência de fraude ou outros atos ilícitos.

Tratamento de Ocorrências

As situações sob suspeita ou confirmadas devem ser tratadas para apuração de responsabilidades e providências necessárias.

Os procedimentos e decisões tomados durante o tratamento das ocorrências devem ser formalizados visando à geração de subsídios a processos judiciais.

Treinamento e Conscientização

O programa de treinamento é contínuo e voltado ao fortalecimento da cultura de integridade e prevenção a fraudes e sinistros. Tem como objetivos aprofundar o conhecimento normativo dos colaboradores e capacitá-los a identificar, prevenir, tratar e comunicar situações suspeitas. As ações de capacitação são promovidas institucionalmente e nas unidades de negócio, por meio de cursos presenciais e online, palestras, campanhas e outras formas de disseminação do conhecimento.

6. MANUTENÇÃO E GUARDA DE INFORMAÇÕES E REGISTROS

Todas as informações e registros relacionados a atos ilícitos devem ser mantidos conforme prazos estabelecidos pela legislação.

7. TRANSPARÊNCIA NO RELACIONAMENTO COM OS CLIENTES

Os clientes têm acesso facilitado às suas informações financeiras por diversos canais, o que os torna aliados importantes na prevenção a atos ilícitos. Além disso, são continuamente orientados sobre riscos e cuidados por meio dos canais de relacionamento.

8. CANAIS DE COMUNICAÇÃO DE ATOS ILÍCITOS

Os administradores, os colaboradores, parceiros e os prestadores de serviços terceirizados do Itaú Unibanco devem, no limite de suas atribuições, comunicar imediatamente as propostas ou ocorrências de situações ou operações com indícios ou evidências de atos ilícitos, identificadas na prospecção, negociação ou durante o relacionamento utilizando-se dos seguintes canais estabelecidos, por meio físico ou eletrônico:

Situações Relacionadas com Lavagem de Dinheiro ou Financiamento do Terrorismo
No Brasil as comunicações devem ser encaminhadas à DPLD - Área de PLD
- Canal Interno: IU Conecta > Utilidades > PLD Online
- Site:https://www.itau.com.br/atendimento-itau/para-voce/denuncia/

Nas unidades internacionais as comunicações devem ser encaminhadas aos canais locais ou "*Compliance Officers*" da Unidade.

Situações Relacionadas com Fraudes e Outros Ilícitos
No Brasil as comunicações devem ser encaminhadas à Superintendência de Inspetoria e Prevenção a Fraudes ou ao Comitê de Auditoria:

Superintendência de Inspetoria e Prevenção de Fraudes:
- CHAT: PF > EA > Relacionamento > Chat > Inspetoria.
-CHAT: PJ > Pelo ícone da Iris no teams ou https://itau.service-now.com/tech.

- Site: www.itau.com.br/atendimento-itau/para-voce/denuncia;
- E-mail externo: inspetoria@itau-unibanco.com.br

Nas unidades internacionais as comunicações devem ser encaminhadas aos canais locais ou *"Compliance Officers* da Unidade*"*

Comitê de Auditoria:
- E-mail externo: comitê.auditoria@itau-unibanco.com.br
- Endereço de correspondência:
A/C Comitê de Auditoria do Itaú Unibanco Holding S.A.
Praça Alfredo Egydio de Souza Aranha, 100
Torre Olavo Setubal – Piso PT
CEP 04344-902 – SP – São Paulo

Nas unidades internacionais as comunicações podem ser enviadas ao canal estabelecido pelo Comitê de Auditoria local, quando existir, ou ao canal do Comitê de Auditoria de Itaú Unibanco detalhado acima.

Estes canais devem ser divulgados e também podem ser utilizados pelos clientes, prestadores de serviços e público em geral.

9. PROTEÇÃO A DENUNCIANTES

A proteção ao denunciante é um princípio essencial para garantir a integridade do ambiente corporativo. É vedada qualquer forma de retaliação contra quem, de boa-fé, reportar suspeitas ou violações às diretrizes da política. As manifestações podem ser anônimas, e a confidencialidade das informações deve ser preservada durante todo o processo de apuração. Sanções disciplinares serão aplicadas tanto a quem praticar retaliação quanto a quem agir de má-fé ao realizar denúncias infundadas. As denúncias anônimas podem ser realizadas através do site: www.itau.com.br/atendimento-itau/para-voce/denuncia

10. SANÇÕES PREVISTAS

O descumprimento das disposições legais e regulamentares sujeita os administradores e os colaboradores a sanções que vão desde penalidades administrativas até criminais, por lavagem de dinheiro, financiamento do terrorismo, fraudes, corrupção e outros atos ilícitos.

A negligência e a Falha Voluntária são consideradas descumprimento desta política, do Código de Ética e da Política Corporativa de Integridade, Ética e Conduta], sendo passível a aplicação de medidas disciplinares previstas nas Regras de Orientação e Aplicação de Medidas Disciplinares.

11. INTERCÂMBIO DE INFORMAÇÃO

Quando aplicável e de acordo com as diretrizes de segurança da informação determinadas na Política Corporativa de Segurança da Informação e Cyber Security poderá ser realizado intercâmbio de informações entre suas áreas de controles para cumprimento das diretrizes aqui estabelecidas.

12. NORMATIVOS RELACIONADOS

Esta política deve ser lida e interpretada em conjunto com os seguintes documentos:

Carta-Circular nº 4.001/2020 do Banco Central do Brasil;
Circular nº 3.691/2013 do Banco Central do Brasil;
Circular nº 3.680/2013 do Banco Central do Brasil;
Circular nº 3.978/2020 do Banco Central do Brasil e respectivas alterações;
Circular nº 612/2020 da Superintendência de Seguros Privados e respectivas alterações;
Decreto-Lei nº 2.848/1940 - Código Penal Brasileiro;

Instrução nº 34/2020 da Superintendência Nacional de Previdência Complementar;
Lei nº 12.846/2013;
Lei nº 9.613/1998 e respectivas alterações;
Lei nº 13.810/2019 e suas correlatas;
Normativo de Autorregulação SARB nº 011/2013 da Federação Brasileira de Bancos;
Recomendações do Grupo de Ação Financeira (GAFI);
Resolução nº 021/2012 do Conselho de Controles de Atividades Financeiras;
Resolução nº 50/2021 da Comissão de Valores Mobiliários e respectivas alterações;
Resolução nº 4.567/2017 do Conselho Monetário Nacional; e

Resolução nº 4.753/2019 do Conselho Monetário Nacional;
Wolfsberg Anti-Money Laundering Principles.

13. GLOSSÁRIO

Atos Ilícitos: são todas as ações ou omissões humanas conscientes e dirigidas a prática de ilícitos criminais - lavagem de dinheiro, financiamento do terrorismo, corrupção e fraudes.

Estreitos Colaboradores: Pessoa natural conhecida por ter qualquer tipo de estreita relação com pessoa exposta politicamente, inclusive por: i) ter participação conjunta em pessoa jurídica de direito privado; ii) figurar como mandatária, ainda que por instrumento particular da pessoa mencionada no *item i)*; ou iii) ter participação conjunta em arranjos sem personalidade jurídica; e Pessoa natural que tem o controle de pessoas jurídicas ou de arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de pessoa exposta politicamente.

Beneficiário Final: é a pessoa física que detém, em última instância, o controle da pessoa jurídica ou em nome da qual uma transação está sendo conduzida. É também considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerçam o comando de fato sobre as atividades do cliente Pessoa Jurídica.

Especial Atenção: as situações que requerem monitoramento reforçado.

Falha Voluntária: é o ato intencional de envolvimento com ações ilícitas, como por exemplo, estruturar ou aconselhar outras pessoas a estruturarem operações com o propósito de burlar as comunicações aos órgãos reguladores, ou envolver-se conscientemente com transações cujos recursos são provenientes de atos ilícitos.

Itaú Unibanco: Itaú Unibanco Holding S.A.

Pessoas Expostas Politicamente (PEPs): são os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas previstos nas normas dos órgãos reguladores, assim como seus representantes, familiares diretos ou colaterais e Estreitos Colaboradores. Também recebem diligências aprofundadas as pessoas jurídicas cujos representantes ou controladores, direto ou indireto, sejam PEPs.

PLD/CFTP: Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa.

Pontos Focais: administradores ou colaboradores indicados pelo Executivo da unidade de negócios para zelar pelo cumprimento das diretrizes corporativas de PLD/CFT pela unidade de negócios.

Retaliação: ato de perseguição, revide ou vingança praticado contra administradores ou colaboradores que manifestem suas dúvidas, suspeitas ou constatações. São exemplos de retaliação: ameaças, rebaixamento de cargo, inclusão em "block list", aplicação de suspensão, desligamento, etc.

Sinistro: eventos atípicos que resultem em prejuízos ou desastres ao Itaú Unibanco, tais como: assaltos a agencias e clientes, extorsão mediante sequestro, furtos, acidentes, arrombamentos, etc.

Aprovado pelo Conselho de Administração em Setembro de 2025.