ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

POLÍTICA CORPORATIVA DE PREVENÇÃO E COMBATE A ATOS ILÍCITOS

OBJETIVO
Esta política de Prevenção a Atos Ilícitos consolida os princípios e as diretrizes do Itaú Unibanco Holding S.A. (Itaú Unibanco) para a prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo, às fraudes e aos sinistros, em consonância com a legislação e regulamentação vigentes e com as melhores práticas de mercado nacionais e internacionais.

PÚBLICO ALVO
Esta política aplica-se ao Itaú Unibanco e suas empresas controladas e coligadas, no Brasil e no exterior. Em caso de conflito entre esta política e as legislações locais onde se encontram as representações do exterior, prevalecerá o padrão mais rigoroso, desde que não infrinja a legislação loca.

INTRODUÇÃO
As instituições financeiras desempenham um papel fundamental na Prevenção e no Combate aos Atos Ilícitos, que são todas as ações ou omissões humanas conscientes e dirigidas à prática de ilícitos criminais, notadamente à lavagem de dinheiro, financiamento do terrorismo, corrupção, fraudes e sinistros.
A lavagem de dinheiro consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.
O financiamento do terrorismo se configura quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, por grupos terroristas para a prática de atos terroristas.
A corrupção consiste em sugerir, oferecer, prometer, conceder, solicitar, exigir, aceitar ou receber, direta ou indiretamente, mediante exigência ou não, a/de pessoas ou empresas dos setores público, privado e organizações do terceiro setor, bem como entre pessoas, empresas e organizações de diferentes países, vantagens indevidas de qualquer natureza (financeira ou não) em troca de realização ou omissão de atos inerentes às suas atribuições, operações ou atividades para o Conglomerado ou visando a benefícios para si ou para terceiros.
Fraude refere-se a quaisquer atividades, atitudes ou ações ilícitas que têm o propósito de enganar ou iludir alguém, utilizando-se de má-fé para benefício próprio ou de terceiros. São exemplos: omissão/manipulação de informação, apropriação de valores, adulteração de documentos, registros e demonstrações contábeis.
Sinistro refere-se a eventos atípicos que resultem em prejuízos ou desastres ao Itaú Unibanco, tais como: assaltos a agencias e clientes, extorsão mediante sequestro, furtos, acidentes, arrombamentos, entre outros.
Embargo é a proibição total ou parcial de realizar operações comerciais com determinado país, estabelecido por uma jurisdição ou por um organismo internacional em represália a determinadas ações, adotadas pela jurisdição embargada, de caráter econômico, político, social ou bélico, ações estas que contrariam os princípios estabelecidos pela jurisdição ou organismo internacional que impõe o embargo. Algumas jurisdições ou organismos internacionais também estabelecem restrições a determinadas pessoas ou companhias que atuam em atividades ilícitas.
O grande desafio é identificar e coibir operações cada vez mais sofisticadas que procuram ocultar ou dissimular a natureza, a autoria, origem, localização, disposição, movimentação ou a propriedade de bens, direitos e/ou valores provenientes direta ou indiretamente de atividades ilegais.
O Itaú Unibanco estabelece a presente política com o intuito de evitar a sua intermediação em atividades ilícitas, e o de zelar e proteger seu nome, sua reputação e imagem perante os colaboradores, clientes, parceiros estratégicos, fornecedores, prestadores de serviços, reguladores e sociedade, por meio de uma estrutura de governança orientada para a transparência, o rigoroso cumprimento de normas e regulamentos e a cooperação com as autoridades policial e judiciária. Também busca alinhar-se continuamente às melhores práticas nacionais e internacionais para prevenção e combate a atos ilícitos, por meio de investimentos e contínua capacitação de seus colaboradores.

PAPÉIS E ATRIBUIÇÕES
Conselho de Administração
Aprova as diretrizes de prevenção a atos ilícitos da Instituição e suas respectivas alterações.

Comitê de Auditoria
Supervisiona o Programa Corporativo de Prevenção a Atos Ilícitos a partir de informações compiladas e apresentadas pelas áreas, bem como de outros mecanismos de que dispõe.

Comissão Superior de Risco Operacional (CSRO)
- Define e propõe ao Conselho de Administração as diretrizes de prevenção a atos ilícitos da Instituição;
- Analisa os resultados dos processos e atividades do programa de prevenção a atos ilícitos;
- Delibera sobre situações não previstas nesta Política.

Diretoria de Risco de Crédito, Modelagem e Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (DRCMPLD)
- Gerencia o Programa de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do Itaú Unibanco no Brasil e no exterior;
- Aprimora a qualidade e efetividade de seus processos e as responsabilidades sobre os processos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do Itaú Unibanco;
- Realiza a avaliação prévia dos riscos de lavagem de dinheiro e financiamento do terrorismo em produtos e serviços;
- Define as diretrizes e os critérios mínimos de classificação de riscos de lavagem de dinheiro e financiamento do terrorismo dos clientes, colaboradores, parceiros comerciais, fornecedores e prestadores de serviços;
- Acompanha e diagnostica as diferentes tipologias de lavagem de dinheiro, no sentido de antecipar tendências e propor soluções preventivas e de combate;
- Valida os procedimentos de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do Itaú Unibanco mencionados nos documentos das unidades de negócios;
- Reporta periodicamente ao Comitê de Auditoria fatos relevantes de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo do Itaú Unibanco.

Diretoria de Segurança Corporativa (DSC)
- Gerencia o Programa de Prevenção a Atos Ilícitos do Itaú Unibanco no Brasil e no exterior;
- Aprimora a qualidade e efetividade de seus processos, assegurando a integridade, disponibilidade e confidencialidade das informações; a segurança física dos colaboradores, clientes e executivos, do patrimônio; e as responsabilidades sobre os processos de Prevenção a Atos Ilícitos;
- Realiza a avaliação prévia dos riscos de fraudes em produtos e serviços;
- Define as diretrizes e os critérios mínimos de classificação de riscos de fraudes dos clientes, colaboradores, parceiros comerciais, fornecedores e prestadores de serviços;
- Acompanha e diagnostica os diferentes tipos de atos ilícitos, no sentido de antecipar tendências e propor soluções preventivas e de combate;
- Valida os procedimentos de Prevenção a Atos Ilícitos mencionados nos documentos das unidades de negócios;
- Reporta periodicamente ao Comitê de Auditoria fatos relevantes de atos ilícitos;
- Gerencia eventos extremos, únicos e raros que ameacem a estratégia, o objetivo e a viabilidade da organização, sua imagem e/ou reputação.

Unidades de Negócios
- Como primeira linha de defesa, definem e implementam procedimentos e controles aderentes a esta política com a orientação da DRCM e DSC, considerando a avaliação dos riscos no início e manutenção do relacionamento com pessoas naturais e jurídicas, naqueles processos que são executados e estão sob sua responsabilidade direta;
- Asseguram que os colaboradores realizem o treinamento de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo, fraudes e sinistros.

Jurídico
- Analisar os requerimentos legais e regulatórios de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (CFT) e seus respectivos impactos aos negócios;
- Auxiliar os gestores de negócio a elaborar planos de ação para implantação de controles de PLD/CFT;
- Apoiar a avaliação dos riscos e providências necessárias para tratamento de ocorrências de transações ou operações suspeitas de lavagem de dinheiro, fraudes e sinistros, sob a ótica jurídica.

Diretoria de Risco Operacional

Certifica a eficiência do ambiente de controle, através de programas de monitoramento, testes de controles, reportando o risco residual de modo independente, conforme definido em política interna.

Auditoria Interna
Como terceira linha de defesa, avalia anualmente a efetividade do Programa de Prevenção e Combate a Atos Ilícitos e propõe medidas para aprimorá-lo.

PROGRAMA CORPORATIVO DE PREVENÇÃO E COMBATE A ATOS ILÍCITOS

Identificação de Clientes

Trata-se de um conjunto de ações que devem ser adotadas para identificação de clientes, contemplando a captura e a confirmação de informações, atualização periódica e armazenamento dos dados cadastrais. O Itaú Unibanco não admite a abertura e manutenção de contas anônimas.

Conheça Seu Cliente - KYC

Trata-se de um conjunto de ações que devem ser adotadas para assegurar a identidade e a atividade econômica dos clientes, bem como a origem e a constituição de seu patrimônio e seus recursos financeiros.

Quanto mais precisas forem as informações coletadas e registradas no início do relacionamento, maior será a capacidade de identificação de atos ilícitos.

Para os casos que requerem Especial Atenção, como o relacionamento com Pessoas Expostas Politicamente (PEPs) e clientes onde não foi possível identificar o beneficiário final, são adotados procedimentos rigorosos específicos de análise.

É obrigatória a autorização de alçada superior para o início do relacionamento com pessoas físicas ou pessoas jurídicas classificadas como PEPs e para a manutenção do relacionamento já existente quando o cliente passar a se enquadrar nesta situação, conforme definido em política interna.

Conheça Seu Parceiro - KYP

São consideradas Parceiros as Pessoas Jurídicas que realizam acordos comerciais ou associações com uma ou várias empresas do conglomerado Itaú Unibanco e que atendem aos requisitos estabelecidos em Política interna.

Conheça Seu Parceiro trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de parceiros comerciais, incluindo correspondentes no país e no exterior. O objetivo é prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas, bem como assegurar que eles possuam procedimentos adequados de PLD/CFT, conforme definido em documento interno.

O Itaú Unibanco não admite o relacionamento com os denominados Bancos de Fachada (Shell Banks), ou seja, bancos constituídos em uma jurisdição onde não há qualquer presença física e que não se encontrem integrados a nenhum grupo financeiro regulamentado.

Conheça Seu Fornecedor - KYS

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de fornecedores e prestadores de serviços, visando proporcionar um adequado conhecimento dos colaboradores de modo a prevenir a contratação de empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Para clientes, parceiros, fornecedores e prestadores de serviços que apresentarem maior risco associado a atos ilícitos são aplicados critérios de identificação e diligência mais rigorosos, com a aprovação do relacionamento por nível hierárquico superior.

Conheça Seu Funcionário - KYE

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para seleção, contratação e acompanhamento de situações que possam caracterizar algum tipo de risco ou desvio, para fins de prevenção à lavagem de dinheiro, financiamento ao terrorismo e demais atos ilícitos.

Avaliação de Novos Produtos e Serviços

Os novos produtos e serviços devem ser avaliados de forma prévia, sob a ótica de PLD/CFT, conforme diretrizes estabelecidas em Política interna.

Monitoramento de Transações

As transações e operações financeiras realizadas pelos clientes, colaboradores ou não, devem ser monitoradas para apuração de situações que podem configurar indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo. Para os casos que requerem Especial Atenção, como o relacionamento com Pessoas Expostas Publicamente (PEP) e clientes onde não foi possível identificar o beneficiário final, são adotados procedimentos rigorosos específicos de análise. O monitoramento considera o perfil, origem e destino dos recursos e a capacidade financeira dos clientes.

Comunicação de Transações Suspeitas aos Órgãos Reguladores
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
O programa de treinamento de PLD/CFT é contínuo e deve ser aplicado a todos os colaboradores elegíveis, visando:
- aprofundar o conhecimento que os administradores e colaboradores têm das exigências e responsabilidades legais e regulamentares, bem como das diretrizes corporativas de PLD/CFT;
- capacitar administradores e colaboradores a identificar, prevenir, tratar e comunicar situações de risco ou com indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo nos negócios realizados.
A aplicação do programa deve ocorrer por meio de ações institucionais e nas unidades de negócios, podendo contemplar cursos presenciais ou à distância (e-learning), palestras, teleconferências, áudio-conferências, campanhas, comunicados, publicações, entre outras modalidades e formas.

5.1 Prevenção e Combate a Fraudes e Sinistros
A prevenção e combate a fraudes é responsabilidade de todos os colaboradores. As Fraudes podem ser classificadas como:
a) Infrações Disciplinares e Violações ao Código de Ética Itaú Unibanco e à Política Corporativa de Integridade e Ética, acometidas em grupo ou isoladamente:
- Adoção de práticas não autorizadas pela empresa;
- Desvios de comportamento;
- Quebra de sigilo e conflito de interesse.
b) Inobservância de Normas Legais e Regulamentares:
São todas as situações identificadas por descumprimento de normas legais e regulamentares, que coloquem em risco a imagem, o patrimônio ou a continuidade da Organização.
c) Atos Ilícitos de Qualquer Natureza:
São todas as modalidades de atos ilícitos (crimes ou contravenções penais) previstos na Legislação Penal Brasileira e que possam ocasionar prejuízos, diretos ou indiretos, ao Banco, seus colaboradores, a clientes ou terceiros. Alguns exemplos são:
- Falsificação;
- Adulteração;
- Estelionato (em todas as suas formas);
- Abertura fraudulenta de conta (contas frias) ou de contratação de produtos;
- Apropriação indébita;
- Furto;
- Roubo;
- Assalto;
- Arrombamento;
- Engenharia Social;
- Extorsão mediante sequestro;
- Fraudes por meio dos canais eletrônicos e não eletrônicos;
- Golpes.

Modelo de Atuação na Prevenção e Combate a Fraudes e Sinistros
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 para resguardar a qualidade e a integridade de suas demonstrações financeiras, por meio de controles internos, da atuação das Auditorias Interna e Externa e da supervisão pelo Comitê de Auditoria.

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 estabelecidas em Política interna.

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 de Prevenção a Fraudes e Sinistros é contínuo e deve ser aplicado a todos os colaboradores elegíveis, visando:
- aprofundar o conhecimento que os administradores e colaboradores têm dos requerimentos normativos externos e internos de prevenção e combate a fraudes e sinistros;
- capacitar administradores e colaboradores a identificar, prevenir, tratar e comunicar situações suspeitas ou relacionadas com fraudes e outros atos ilícitos.
A aplicação do programa deve ocorrer por meio de ações institucionais e nas unidades de negócio, podendo contemplar cursos à distância (e-learning) e presencial, palestras, teleconferências, áudio conferências, campanhas, comunicados, publicações, entre outras modalidades e formas.

MANUTENÇÃO E GUARDA DE INFORMAÇÕES E REGISTROS
As informações e registros das operações e serviços prestados devem ser mantidos em sua forma original ou em arquivos eletrônicos, conforme prazos e responsabilidades estabelecidos pela legislação vigente.

TRANSPARÊNCIA NO RELACIONAMENTO COM OS CLIENTES
Os clientes do Itaú Unibanco possuem acesso, por intermédio de diversos canais, às suas informações financeiras, incluindo os recursos investidos, produtos contratados e limites concedidos. Com isso, o próprio cliente é um parceiro forte e atuante na prevenção e no combate a Atos Ilícitos.
O Itaú Unibanco também alerta continuamente seus clientes, por meio dos canais de relacionamento, sobre as possibilidades de ocorrência de Atos Ilícitos e as ações e os cuidados que devem ser tomados para preveni-los.

CANAIS DE COMUNICAÇÃO DE ATOS ILÍCITOS
Os administradores e os colaboradores do Itaú Unibanco devem comunicar imediatamente as situações 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:

Superintendência de Inspetoria e Prevenção de Fraudes:
- Telefone externo: 0800-723-0010
- Telefone interno: 0300 100 0341
- Site: www.itau.com.br/atendimento-itau/para-voce/denuncia;
- E-mail interno: caixa INSPETORIA;
- E-mail externo: inspetoria@itau-unibanco.com.br e fornecedor_relatos@itau-unibanco.com.br;
- Malote: destinatário: Gerência de Inspetoria/São Paulo;
- Endereço de correspondência:
A/C Inspetoria
Rua Volkswagen, 10, Jabaquara

CEP 04344-020 – SP – São Paulo
Nas unidades internacionais as comunicações devem ser encaminhadas aos canais locais ou *"Compliance Officers* da Unidade*"*

Comitê de Auditoria:
- E-mail interno: caixa COMITE 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 PM
CEP 04344-902 – SP – São Paulo

Nas unidades internacionais as comunicações devem ser encaminhadas aos canais locais ou "Compliance Officers da Unidade"
Estes canais devem ser divulgados e também podem ser utilizados pelos clientes, prestadores de serviços e público em geral.

PROTEÇÃO A DENUNCIANTES
Administradores e colaboradores não podem praticar atos de Retaliação contra aquele que, de boa-fé denunciar ou manifestar queixa, suspeita, dúvida ou preocupação relativas a possíveis violações às diretrizes desta Política; e fornecer informações ou assistência nas apurações relativas a tais possíveis violações.
Administradores e colaboradores devem preservar a confidencialidade das informações relativas às apurações de possíveis violações às diretrizes desta Política.
Os Canais de Denúncias aceitam manifestações anônimas e preservam o anonimato dos denunciantes.
Serão aplicadas sanções disciplinares a administradores ou colaboradores que tentarem ou praticarem retaliação contra quem, de boa-fé, comunicar possíveis violações às diretrizes desta Política.
Também deverão ser aplicadas sanções a administradores ou colaboradores que, comprovadamente, utilizarem de má-fé ao comunicarem possíveis violações às diretrizes desta Política ou comunicarem fatos sabidamente falsos.

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, sinistros, 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 e Ética sendo passível a aplicação de medidas disciplinares previstas em normativos internos da Instituição. Padrões Disciplinares.

DOCUMENTOS RELACIONADOS
Esta política deve ser lida e interpretada em conjunto com os seguintes documentos:
Normas Externas Relacionadas
Decreto-Lei nº 2.848/40 - Código Penal Brasileiro.
Carta-Circular nº 3.430/10 do Banco Central do Brasil.

Carta-Circular nº 3.542/12 do Banco Central do Brasil.
Circular nº 3.461/09 do Banco Central do Brasil.
Circular nº 3.462/09 do Banco Central do Brasil.
Circular nº 3.517/10 do Banco Central do Brasil.
Circular nº 3.583/12 do Banco Central do Brasil.
Circular nº 445/12 da Superintendência de Seguros Privados.
Circular nº 3.654/13 do Banco Central do Brasil.
Instrução nº 301/99 da Comissão de Valores Mobiliários e respectivas alterações.
Instrução nº 18/14 da Superintendência Nacional de Previdência Complementar.
Leis Federais nº 9.613/98 e nº 12.683/12.
Lei Anticorrupção nº 12.846/13.
Normativo de Autorregulação SARB nº 011/2013 da Federação Brasileira de Bancos.
Recomendações do Grupo de Ação Financeira (GAFI).
Resolução nº 2.025/93 do Conselho Monetário Nacional.
Resolução nº 2.747/00 do Conselho Monetário Nacional.
Resolução nº 4.567/17 do Banco Central
Resoluções COAF nº 006/99 e 021/12.
Wolfsberg Anti-Money Laundering Principles

Aprovado pelo Conselho de Administração de 31.10.2019.