ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

POLÍTICA CORPORATIVA DE PREVENÇÃO A ATOS ILÍCITOS

1. OBJETIVO

Esta política de Prevenção a Atos Ilícitos consolida os princípios e as diretrizes do Conglomerado Itaú Unibanco para a Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo, à Proliferação de Armas de Destruição em Massa (PLD/CFTP), às fraudes e aos sinistros, em consonância com a legislação e regulamentação vigentes e com as melhores práticas de mercado 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 em procedimento interno.

3. INTRODUÇÃO

As instituições financeiras desempenham um papel fundamental na Prevenção a 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. Já o Financiamento à Proliferação de Armas de Destruição em Massa se constitui quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção de serem utilizados para a proliferação de armas de destruição em massa, que podem ser biológicas, químicas e nucleares.

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 ou organizações do terceiro setor, bem como entre pessoas, empresas ou 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. 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 dedica uma diretoria exclusiva para o tratamento do tema e 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 terceirizados, 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 a atos ilícitos, por meio de investimentos e contínua capacitação de seus colaboradores.

4. RESPONSABILIDADES

Conselho de Administração (CA)
Aprova as diretrizes de prevenção a atos ilícitos da Instituição e suas respectivas alterações, com o comprometimento para com a efetividade e melhoria contínua do tema. Adicionalmente, o Conselho recebe 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.

Comitê de Auditoria (CAUD)
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. Adicionalmente, o Comitê recebe 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 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; e
- Delibera sobre situações não previstas nesta Política.

Comitê de Gestão de Riscos e Capital (CGRC)
Apoia o CA no desempenho de suas atribuições relacionadas à gestão de riscos e capital do Itaú Unibanco. Adicionalmente, recebe para ciência a Avaliação Interna de Risco.

Diretoria de Prevenção à Lavagem de Dinheiro (DPLD)
- Assegura a implementação do Programa de PLD/CFTP do Conglomerado Itaú Unibanco e de suas empresas no Brasil e no exterior;
- Elabora a Avaliação Interna de Risco do Itaú Unibanco;
- Aprimora a qualidade e efetividade de seus processos e as responsabilidades sobre os processos de PLD/CFTP do Itaú Unibanco, verificando o cumprimento da política, bem como corrigindo eventuais deficiências verificadas;
- Realiza a avaliação prévia dos riscos de lavagem de dinheiro e financiamento do terrorismo em novos produtos e serviços, incluindo a utilização de novas tecnologias;
- 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 terceirizados;
- Elabora e acompanha a implementação da abordagem baseada em risco nos processos, formalizando os em procedimentos internos, juntamente com os critérios estabelecidos para a geração de indicadores de efetividade;
- 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 PLD/CFTP do Itaú Unibanco mencionados nos documentos das unidades de negócios;
- Reporta periodicamente ao Comitê de Auditoria fatos relevantes de PLD/CFTP do Itaú Unibanco.
Cabe também ao Diretor de PLD/CFTP, as seguintes atribuições:
- Gerenciar os riscos de PLD/CFTP através das informações recebidas por meio de Comitês e, a depender do risco, casos submetidos à sua alçada;
- Aprovar a Avaliação Interna de Risco do Itaú Unibanco;
- Delegar para as devidas alçadas as aprovações das regras de procedimento destinados a conhecer seu cliente, funcionários, parceiros comerciais e prestadores de serviço terceirizados, bem como as de monitoramento, seleção e análise;
- Receber para ciência os contratos de parcerias com Instituições Financeiras sediadas no exterior, bem como com terceiros participantes de arranjos de pagamento do qual o Itaú Unibanco também participe, conforme estabelecido em regulamentação vigente;

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, incluindo a utilização de novas tecnologias;
- 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 e de suporte no Brasil e no exterior
- Como primeira linha de governança, definem e implementam procedimentos e controles aderentes a esta política com a orientação da DPLD – PLD e DSC, considerando a avaliação dos riscos no início e manutenção do relacionamento com pessoas naturais e jurídicas (sejam clientes, colaboradores, parceiros comerciais, fornecedores, prestadores de serviços ou outros relacionamentos), naqueles processos que são executados e estão sob sua responsabilidade direta;
- Asseguram que os colaboradores realizem o treinamento de PLD/CFTP, Fraudes e Sinistros.

Jurídico
- Analisa os requerimentos legais e regulatórios de PLD/CFTP e seus respectivos impactos aos negócios;
- Auxilia os gestores de negócio a elaborar planos de ação para implantação de controles de PLD/CFTP;
- Apoia 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 eficácia do ambiente de controle, através de programas de monitoramento, avaliação de testes de efetividade de controles, reportando o risco residual e acompanhamento das deficiências verificadas de modo independente, conforme definido na Política de Gerenciamento Integrado de Risco Operacional e Controles Internos e elabora Relatório de Efetividade assim como Relatório de Acompanhamento, submetendo para aprovação e ciência dos responsáveis, seguindo, no mínimo, o prazo estabelecido pela regulamentação.

Auditoria Interna
Como terceira linha de governança, o escopo da auditoria interna abrange o exame e a avaliação da adequação e eficácia da governança, do gerenciamento de riscos e controles internos da organização, da qualidade na execução das responsabilidades atribuídas para atingir as metas estabelecidas pela organização, conforme definido na Política de Auditoria Interna (Global).

5. AVALIAÇÃO INTERNA DE RISCO

O Itaú Unibanco elabora anualmente a sua Avaliação Interna de Risco, documento este que tem por objetivo identificar, mensurar e mitigar o risco de utilização de seus produtos e serviços na prática de lavagem de dinheiro e do financiamento ao terrorismo.

Com base nessa Avaliação é aplicada uma abordagem baseada em risco, metodologia esta que garante que as medidas de prevenção e mitigação da lavagem de dinheiro e do financiamento do terrorismo sejam proporcionais aos riscos identificados, pois, aonde os riscos forem mais altos, serão adotadas medidas reforçadas para administrar e mitigar tais riscos e, onde os riscos forem menores, serão utilizadas medidas simplificadas.

O detalhamento das diretrizes que fundamentam a abordagem baseada em risco está formalizado em procedimento interno.

6. AVALIAÇÃO DE EFETIVIDADE

O Itaú Unibanco elabora anualmente Relatório de Efetividade, de modo a avaliar a efetividade das políticas, procedimentos e controles internos de PLD/CFTP. Os planos de ação endereçados a solucionar as deficiências identificadas, por meio da referida Avaliação, deverão ser acompanhados por meio de um Relatório de Acompanhamento. Adicionalmente, a Avaliação de Efetividade deverá conter, no mínimo,

informações que descrevam a metodologia adotada; os testes aplicados; a qualificação dos avaliadores e as deficiências identificadas.

7. 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. Tal programa deverá ser aplicado, de forma independente e autônoma, no Brasil e nas Unidades Internacionais, conforme definido em procedimento interno. Deverá conter minimamente:

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

Políticas e Procedimentos

O Itaú Unibanco possui políticas, regras e procedimentos estruturados para determinar suas diretrizes quanto ao combate a atos ilícitos, as quais estão em conformidade com leis e regulamentos locais, bem como com os perfis de risco dos clientes; da instituição; das operações, transações, produtos e serviços; e dos funcionários, parceiros comerciais e prestadores de serviços terceirizados. Referidos documentos são revisados e aprovados periodicamente de acordo com a alçada previamente estabelecida e estão disponíveis para todos os funcionários.

Identificação de Clientes

Trata-se de um conjunto de ações que devem ser adotadas para a identificação e qualificação de clientes, bem como de seus administradores e representantes, contemplando a captura, verificação e validação de suas informações, com o objetivo de conhecer sua verdadeira identidade. Os dados cadastrais obtidos deverão ser atualizados e armazenados de acordo com os prazos estabelecidos.

Adicionalmente, para realizar uma completa identificação e qualificação do cliente, devem ser seguidos os procedimentos definidos em políticas internas, de obtenção de informações, que permitam verificar a sua condição como Pessoa Exposta Politicamente (PEP), bem como de análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como beneficiário final.

O Itaú Unibanco não admite a abertura e manutenção de contas anônimas.

As regras que detalham estes item estão descritas na POLÍTICA CORPORATIVA DE CADASTRO DE CLIENTES

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. A coleta destas informações deve permitir a avaliação da capacidade financeira do cliente. Quanto mais precisas forem as informações coletadas e registradas no início do relacionamento, maior será a capacidade de identificação de atos ilícitos.

Com base em uma abordagem baseada no risco de LD/FT, para os clientes classificados com maior risco e para os casos que requerem Especial Atenção, como o relacionamento com PEPs e clientes onde não foi possível identificar o beneficiário final, são adotados procedimentos rigorosos específicos de análise.

É obrigatória a avaliação sobre o interesse no início ou na manutenção do relacionamento com pessoas físicas ou pessoas jurídicas classificadas como PEPs por um detentor de cargo ou função de nível hierárquico superior ao do responsável pela autorização do relacionamento, conforme definido em procedimento interno.

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 na Política de Governança de Parcerias Comerciais.

Este pilar contempla um conjunto de regras, procedimentos e controles que devem ser adotados para identificar e qualificar adequadamente os parceiros comerciais, incluindo correspondentes no país e no exterior. Estes parceiros devem ser classificados em categorias de risco considerando as atividades por eles exercidas.

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/CFTP, conforme definido em procedimento 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.

As diretrizes que tratam este item estão em procedimento interno.

Conheça Seu Fornecedor - KYS

Trata-se de um conjunto de regras, procedimentos e controles que devem ser adotados para identificar e qualificar adequadamente os fornecedores e prestadores de serviços terceirizados. Estes agentes devem ser classificados em categorias de risco considerando as atividades por eles exercidas.

O objetivo é prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Para **clientes**, **parceiros comerciais**, **fornecedores** e **prestadores de serviços terceirizados** 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 identificar e qualificar adequadamente os colaboradores e/ou candidatos, a fim de subsidiar a sua seleção e contratação, bem como acompanhar 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. Estes colaboradores devem ser classificados em categorias de risco considerando as atividades por eles exercidas.

Avaliação de Novos Produtos e Serviços-

Os novos produtos e serviços, incluindo a utilização de novas tecnologias, quando aplicável, devem ser avaliados de forma prévia, sob a ótica de PLD/CFTP, conforme as diretrizes estabelecidas na Política de Avaliação de Produtos (Global).

Cumprimento às Sanções

Trata-se de um conjunto de regras, procedimentos e controles relacionados a sanções, embargos e restrições políticas e econômicas que podem ser aplicáveis a operações comerciais com pessoas, instituições e países/regiões envolvidos com atividades de terrorismo, narcotráfico, conflitos bélicos, violação dos direitos humanos ou outras impropriedades e ilegalidades em consonância com a legislação e regulamentação vigentes e com as melhores práticas.

De acordo com procedimento interno, o Itaú Unibanco estabelece diretrizes de embargos totais a países e segue listas restritivas impostas por autoridades emissoras de sanções.

Monitoramento, Seleção e Análise de Operações ou Situações Suspeitas

Todas as transações e operações financeiras, inclusive as propostas, 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. O monitoramento considera o perfil, origem e destino dos recursos e a capacidade financeira dos clientes.

De acordo com a abordagem baseada em risco, para clientes de maior exposição de LD/FT deverá ser aplicado um conjunto de regras ou parâmetros mais rigorosos ou ainda um acompanhamento mais frequente ou aprofundado de suas atividades.

Adicionalmente, o processo de Monitoramento, Seleção e Análise deve ocorrer de forma independente e autônoma na área de PLD/CFTP, que deve ser segregada do departamento comercial, de acordo com as determinações legais e regulamentares.

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/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. Referido programa visa:
- Aprofundar o conhecimento das exigências e responsabilidades legais e regulamentares, bem como das diretrizes corporativas de PLD/CFTP;
- Capacitar sobre a melhor forma para a identificação, prevenção, tratamento e comunicação de situações de risco ou com indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo nos negócios realizados;
- Promover a cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, à proliferação de armas de destruição em massa.
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.

As diretrizes que tratam este item estão em procedimento interno.

7.2. Prevenção e Combate a Fraudes

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, ou local no caso de Unidades Internacionais, conforme aplicável e que possam ocasionar prejuízos, diretos ou indiretos, ao Banco, seus colaboradores, a clientes ou terceiros. Alguns exemplos são:
- Falsificação;
- Estelionato (em todas as suas formas, inclusive por meios eletrônicos);
- Apropriação indébita;
- Furto;
- Quebra de sigilo bancário;
- Roubo;
- Extorsão mediante sequestro.

Modelo de Atuação na Prevenção e Combate a Fraudes

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.

As diretrizes que tratam este item estão em procedimento interno.

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 estabelecidas na Política de Avaliação de Produtos.

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.

8. MANUTENÇÃO E GUARDA DE INFORMAÇÕES E REGISTROS

Todas as informações relacionadas aos pilares acima descritos, bem como os 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.

9. 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 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.

10. 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
- Telefone: (11) 2757-6753;
- E-mail interno: PREVENCAO A LAVAGEM DE DINHEIRO.
- 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:
- 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
Av. Dr. Hugo Beolchi, 900 piso -1 – Torre Eudoro Villela – São Paulo (SP) – CEP 04310-030
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 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.

11. 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.

12. 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 em política interna.

13. 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.

14. 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.

15. 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.
Bancos de Fachada (Shell Banks): banco constituído em uma jurisdição onde não há qualquer presença física e que não se encontre integrado em um grupo financeiro regulamentado.
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 são aquelas que envolvem, mas não se limitando a:
- I - propostas de início de relacionamento e operações com Pessoas Expostas Politicamente ;
- II - indícios de burla aos procedimentos de identificação e de comunicação;
- III - clientes e operações em que não seja possível identificar o beneficiário final;
- IV - transações oriundas de países que aplicam insuficientemente as recomendações do Grupo de Ação Financeira - GAFI; e
- V - situações em que não seja possível manter atualizadas as informações cadastrais de clientes.

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 relevantes, assim como seus representantes, familiares diretos ou colaterais até o segundo grau, o cônjuge, companheiro, companheira, enteado, enteada, bem como os Estreitos Colaboradores. Também são considerados PEPs, 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 "lista negra", 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 de Julho de 2024.