ITAÚ UNIBANCO HOLDING S.A.

VERSÃO PARA DIVULGAÇÃO PÚBLICA

RELATÓRIO DE ACESSO PÚBLICO - POLÍTICA DE COMPLIANCE

RESUMO

Estabelece os fundamentos associados à função de *Compliance* (conformidade).

1. OBJETIVO E PÚBLICO-ALVO

Estabelecer as diretrizes e principais atribuições associadas à função de *Compliance,* observando as boas práticas de mercado e regulamentações aplicáveis.

Esta política se aplica ao Itaú Unibanco Holding e suas empresas controladas no Brasil e as empresas no exterior.

2. INTRODUÇÃO

A função de *Compliance* tem como objetivo a prevenção e a mitigação de exposição do Itaú Unibanco a situações de não conformidade com normas e compromissos (Risco de *Conformidade*), sendo responsável pela governança, certificação de aderência, conduta e transparência.

Risco Regulatório ou de Conformidade é o risco de sanções, perdas financeiras ou danos reputacionais decorrentes da falta de cumprimento de disposições legais e regulamentares, normas de mercado local e internacional, compromissos com reguladores, compromissos públicos, códigos de autorregulação e códigos de conduta aderidos pelo Itaú Unibanco.

O risco de conformidade é gerenciado através de processo estruturado que visa a identificar as alterações no ambiente regulatório, analisar os impactos nas áreas da instituição e monitorar as ações voltadas para a aderência às exigências normativas e demais compromissos mencionados no parágrafo anterior

3. FUNÇÃO DE COMPLIANCE

A função de Compliance é executada diretamente pela Diretoria de *Compliance & OpRisk* (DCOR) e por outras diretorias da Área de Riscos, sob coordenação da DCOR, e de forma integrada com os demais riscos incorridos pela instituição.

4. DIRETRIZES

a) O gerenciamento dos riscos de conformidade deve contemplar os processos, produtos e serviços existentes ou novos, inclusive os serviços terceirizados relevantes. Tais processos, produtos e serviços devem ser periodicamente testados e avaliados quanto à aderência às normas aplicáveis, aos compromissos firmados junto aos reguladores e aos requisitos relacionados ao Código de Ética e Conduta.

b) Os responsáveis pela função de *Compliance* possuem comunicação direta tanto com os administradores, incluindo os membros do Conselho de Administração e do Comitê de Auditoria, quanto com qualquer colaborador, e tem acesso a quaisquer informações necessárias no âmbito de suas responsabilidades.

c) Os relatórios e indicadores do risco de *Compliance* devem ser claros, objetivos e tempestivos, sendo reportados às comissões superiores, aos executivos das unidades de negócios, ao executivo de Riscos,

ao Comitê de Gestão de Risco e Capital, ao Comitê de Auditoria e ao Conselho de Administração, para que o nível de exposição e enquadramento aos limites estabelecidos sejam monitorados.

d) Os apontamentos de não conformidade identificados por quaisquer áreas do Conglomerado, reguladores e demais órgãos de supervisão e fiscalização devem ser acompanhados para que seja garantido o seu efetivo tratamento pelas áreas competentes. A DCOR deve estimular a responsabilidade individual e coletiva dos colaboradores sobre a gestão e a governança dos riscos e das atividades de *Compliance* da organização.

e) Nas Unidades Internacionais, estruturas locais e independentes responsáveis pelo *Compliance,* sob responsabilidade dos *Compliance Risk Officers* (CROs) locais, exercem sua função sob supervisão dos CROs Regionais que, por sua vez, se reportam ao CRO Global.

5. PRINCIPAIS PAPÉIS E ATRIBUIÇÕES

5.1. Conselho de Administração

Cabe ao Conselho de Administração:

- Aprovar:

a) as diretrizes, estratégias e políticas referentes ao *Compliance*, com o objetivo de garantir o claro entendimento dos papéis e responsabilidades para todos os níveis do Conglomerado; e

b) a posição da DCOR na estrutura organizacional da instituição de forma a evitar possíveis conflitos de interesses, principalmente com as áreas de negócios.

- Prover meios necessários para que as atividades relacionadas à função de *Compliance* sejam exercidas adequadamente, incluindo disponibilidade de recursos para alocação de pessoal em quantidade suficiente e com treinamento e experiência necessária.

- Assegurar a:

a) adequada gestão desta política;

b) efetividade e a continuidade da aplicação desta política;

c) comunicação desta política a todos os colaboradores e prestadores de serviços terceirizados relevantes;

d) disseminação de padrões de integridade e conduta ética como parte da cultura da instituição; e

e) adoção de medidas corretivas para falhas de *Compliance* identificadas.

A avaliação destes itens pelo Conselho de Administração será realizada com base em reportes e reuniões periódicas entre a Área de Risco e o Conselho de Administração e seus comitês de assessoramento e no relatório anual coordenado pela DCOR, bem como por avaliação feita pelo Comitê de Auditoria.

5.2. Comitê de Auditoria

Cabe ao Comitê de Auditoria:

- Validar a Política de *Compliance* antes do envio para aprovação do Conselho de Administração.

- Avaliar, no mínimo anualmente, a estrutura de *Compliance*, em relação aos seguintes aspectos:

a) Definição clara das atribuições, papeis e responsabilidades da função de *Compliance*, evitando possíveis conflitos de interesses, principalmente com as áreas de negócios da instituição;

b) Posicionamento em nível hierárquico adequado, independente e segregado de áreas operacionais e de negócio, com mandato devidamente exercido quanto à definição de escopo, execução do trabalho e comunicação de seus resultados;

c) Estrutura organizacional consistente com as necessidades do Conglomerado e alocação de pessoal em quantidade suficiente, adequadamente treinado e com experiência necessária para o exercício das atividades relacionadas às respectivas funções;

d) Efetividade da gestão de *Compliance*; e

e) Aderência da estrutura à regulação aplicável.

- Verificar a realização da:

a) comunicação desta Política a todos os colaboradores e prestadores de serviços terceirizados relevantes;

b) disseminação de padrões de integridade e conduta ética como parte da cultura da instituição; e

c) adoção de medidas corretivas para falhas identificadas.

5.3. Primeira Linha

As áreas de negócio e suporte devem:

- Manter a conformidade com as normas e exigências regulatórias.

- Definir e implantar os planos de ação para endereçamento dos apontamentos de não conformidade.

- Comunicar prontamente à área de *Compliance* sempre que identificar alterações ou descumprimentos em relação às normas e regulamentações vigentes ou riscos de *Compliance*.

- Informar e capacitar colaboradores e prestadores de serviços terceirizados relevantes acerca de assuntos relativos à *Compliance*, com apoio da DCOR.

- Relacionar-se com os Órgãos Reguladores, Autorreguladores, Supervisores e Fiscalizadores, conforme estabelecido na Política sobre Relacionamento com Órgãos Reguladores, Autorreguladores, Supervisores e Fiscalizadores;

- Identificar, mensurar e gerenciar os eventos de risco de *Compliance* que possam influenciar o cumprimento dos objetivos estratégicos e operacionais do Conglomerado; e

- Manter um efetivo ambiente de controle consistente com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio das operações realizadas, de forma a assegurar o efetivo gerenciamento dos riscos de *Compliance*, mantendo a exposição aos riscos em níveis aceitáveis conforme o apetite de risco estabelecido para o Conglomerado.

5.4. Segunda Linha

Representada pelas diretorias da Área de Riscos, responsáveis pelas atividades de controle de riscos, que são integralmente segregadas das atividades da auditoria interna e do jurídico, sendo independentes no exercício de suas funções.

Essas diretorias não podem gerir negócios ou processos que possam comprometer a sua independência ou gerar conflitos de interesse. Suas metas e remuneração não podem estar relacionadas ao desempenho das áreas de negócio

Cabe à Área de Riscos, sob coordenação da DCOR:

- Apoiar a primeira linha na observação de suas responsabilidades diretas.

- Disseminar os padrões de integridade e ética como parte da cultura do Conglomerado e divulgar as boas práticas e políticas relacionadas à função de *Compliance*.

- Orientar e aconselhar os administradores e colaboradores do Conglomerado, sobre o cumprimento de normas internas relacionadas ao Programa de Integridade e Ética, e sobre o cumprimento de normas externas, relatando possíveis irregularidades ou falhas identificadas.

- Assegurar-se que as equipes de responsáveis pela execução das funções de *Compliance* tenham autoridade apropriada e que são adequadas, tanto em recursos quanto em conhecimento, através de programa estruturado de treinamento.

- Gerir os riscos de conformidade por meio de indicadores de performance, monitoramentos regulatórios, testes e controles, inclusive testes automatizados com uso de dados, denúncias internas e externas, priorizando os riscos conforme sua severidade reportando os resultados à Alta Administração e, quando solicitado, aos Órgãos Reguladores.

- Revisar e acompanhar os planos de ação adotados para o endereçamento dos apontamentos efetuados pelos órgãos reguladores e pelo auditor independente no relatório de descumprimento de dispositivos legais e regulamentares.

- Coordenar as atividades relativas à função de conformidade com a auditoria interna e com a estrutura de gerenciamento de riscos, por meio de reuniões periódicas e, no segundo caso, execução conjunta de atividades operacionais e reportes.

- Disseminar para as UIs as melhores práticas e metodologia de *Compliance* adotadas pela Matriz, incluindo aquelas relacionadas ao Programa Corporativo de Integridade e Ética.

- Coordenar a governança de Programas de *Compliance* de regulamentações internacionais relevantes para o Conglomerado.

Cabe exclusivamente à DCOR:

i. Definir princípios e diretrizes para disseminação da gestão do risco de *Compliance*, incluindo treinamentos.

ii. Gerenciar o processo de monitoramento de aderência às novas regulamentações, com o apoio da Superintendência de *Risk Shared Services* (RISS)

iii. Relatar sistemática e tempestivamente ao Conselho de Administração, diretamente ou por meio de seus comitês de assessoramento, informações relevantes tanto dos resultados das avaliações de *Compliance* realizadas que tenham identificados falhas materiais quanto de alterações significativas no ambiente regulatório.

iv. Gerir o Programa de Integridade e Ética, interagindo com Inspetoria e Ombudsman conforme necessário.

v. Coordenar o relacionamento com reguladores e demais órgãos de fiscalização e supervisão com gestão centralizada, acompanhando os planos de ação formalizados, facilitando o compartilhamento de informações e garantindo a consistência do posicionamento institucional.

vi. Desenvolver e disponibilizar as metodologias, ferramentas, sistemas, infraestrutura e governança necessárias para suportar a função de *Compliance* nas atividades do Conglomerado.

vii. Coordenar a governança de políticas e procedimentos do Itaú Unibanco, conforme regulamentações aplicáveis, mantendo evidências de aprovação de todos os documentos pelas alçadas estabelecidas, incluindo, a aprovação desta Política.

viii. Enviar ao Comitê de Auditoria, ao Comitê de Gestão de Risco e Capital e ao Conselho de Administração Relatório de Conformidade anual contendo sumário dos resultados das atividades relacionadas aos temas de *Compliance*, principais conclusões, recomendações e planos de ação adotados para tratamento das deficiências identificadas.

Nas Unidades Internacionais cabe aos CROs Locais as responsabilidades dos itens acima conforme governança estabelecida em procedimento interno.

5.5. Terceira Linha

Representada pela Auditoria Interna que verifica de forma independente e periódica, a adequação dos processos e procedimentos de identificação e gerenciamento dos riscos, incluindo o gerenciamento integrado de risco operacional, controles internos e *Compliance*, conforme as diretrizes estabelecidas na Política de Auditoria Interna e submete os resultados dos seus apontamentos ao Comitê de Auditoria.

5.6. Comuns a Todas as Áreas do Itaú Unibanco

- Realizar os treinamentos de integridade e ética e de gestão de riscos disponibilizados pelo Itaú Unibanco.

- Assinar anualmente o Termo “Políticas de Integridade Corporativa” atestando seu conhecimento e concordância com o estabelecido nesta Política.

- Definir, implantar e cumprir políticas e procedimentos para aderência a regulamentações.

- Atender às disposições estabelecidas pelas normas externas e políticas internas do Conglomerado.

- Comunicar fato ou suspeita de violações ao Código de Ética e Conduta, à Política de Integridade, Ética e Conduta ou à esta política.

6. NORMAS EXTERNAS RELACIONADAS

Basel Committee on Banking Supervision - *Compliance* and the *Compliance* function in Banks (April 2005)

Resolução nº 4.968/21 do Conselho Monetário Nacional: dispõe sobre a implementação e implantação de sistema de controles internos

Resolução nº 4.557/17 do Conselho Monetário Nacional: dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital

Resolução nº 4.595/17 do Conselho Monetário Nacional: dispõe sobre a política de conformidade (*Compliance*) das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Resolução nº 65/21 do Banco Central do Brasil: dispõe sobre a política de conformidade (*Compliance*) das administradoras de consórcio e das instituições de pagamento.

Resolução nº 416/21 do Conselho Nacional de Seguros Privados: dispõe sobre o Sistema de Controles Internos, a Estrutura de Gestão de Riscos e a atividade de Auditoria Interna.

Aprovado pelo Conselho de Administração de Maio de 2024.