

ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23

Companhia Aberta

NIRE 35300010230

RELATÓRIO DE ACESSO PÚBLICO - POLÍTICA DE COMPLIANCE

OBJETIVO

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

INTRODUÇÃO

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

Risco de *Compliance* é o risco de sanções legais ou regulatórias, de perdas financeiras ou de danos reputacionais, decorrentes da falta de cumprimento de disposições legais e regulamentares, normas de mercado local e internacional ou de compromissos assumidos por meio de códigos de autorregulação, padrões técnicos, códigos de conduta ou políticas internas.

O Itaú Unibanco adota a estratégia de três linhas de defesa para operacionalizar sua estrutura de gerenciamento de riscos (inclusive o de *Compliance*) e para assegurar o cumprimento das diretrizes previstas nesta política, com clara divisão de papéis e responsabilidades.

1. Primeira Linha de Defesa

É representada pelas áreas de Negócio e Suporte. Seus colaboradores são os responsáveis diretos pela gestão dos riscos e aderência às normas associadas às suas atividades, bem como pela execução dos controles e pela implementação de medidas corretivas para o devido tratamento dos riscos.

2. Segunda Linha de Defesa

É representada pelas funções de controle de riscos, que são integralmente segregadas das atividades da auditoria interna e do jurídico, tendo independência no exercício de suas funções.

Possui comunicação direta tanto com os administradores, incluindo os membros do Conselho de Administração e do Comitê de Auditoria, quanto com qualquer colaborador. Tem acesso a quaisquer informações necessárias no âmbito de suas responsabilidades.

É vedada, no Brasil e no exterior, às áreas que compõem a segunda linha de defesa, a gestão de qualquer negócio ou processo que possa comprometer sua independência ou gerar conflitos de interesse. Pelo mesmo motivo, suas metas e sua remuneração não podem estar relacionadas ao desempenho das áreas de negócio.

3. Terceira Linha de Defesa

É representada pela Auditoria Interna, que fornece uma avaliação independente das atividades da instituição, por meio de técnicas de auditoria. Permite à administração aferir a adequação dos controles, a efetividade do gerenciamento dos riscos, a confiabilidade das demonstrações contábeis e o cumprimento das normas e regulamentações

DIRETRIZES

Quanto à função de *Compliance*

O gerenciamento dos riscos de *Compliance* 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, quando aplicável às normas internas.

A função de *Compliance* é executada pela Diretoria Executiva de Risco Operacional e *Compliance*, com reporte à Área de Finanças e Risco e atuação independente das demais áreas de suporte e negócio do Conglomerado.

Nas Unidades Internacionais, existem estruturas locais e independentes responsáveis pelo controle dos riscos Operacional e de *Compliance*, sob responsabilidade dos CROs locais, os quais se reportam matricialmente à Diretoria Executiva de Risco Operacional e *Compliance*.

Os apontamentos levantados pelas áreas executivas, auditorias interna e externa, reguladores e demais órgãos de supervisão e fiscalização devem ser acompanhados, para que seu efetivo tratamento seja garantido pelas áreas competentes.

Os relatórios de riscos de *Compliance* devem ser claros, objetivos e tempestivos, e devem ser reportados às comissões superiores, aos executivos das unidades de negócios, ao Vice-Presidente de Riscos, ao Comitê de Gestão de Risco e Capital, ao Comitê de Auditoria e ao Conselho de Administração, para que os níveis de exposição e enquadramento aos

limites estabelecidos sejam monitorados. Nas Unidades Internacionais, os relatórios de riscos de *Compliance* devem ser reportados aos fóruns competentes de cada Unidade.

Para contribuir com o adequado gerenciamento dos riscos, o Itaú Unibanco dispõe de uma metodologia de gestão de riscos composta por 5 etapas: identificação, priorização, resposta ao risco, monitoramento e reporte.

PRINCIPAIS PAPÉIS E ATRIBUIÇÕES

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 Corporativas", 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 políticas internas do conglomerado.
- Comunicar fato ou suspeita de violação ao disposto nesta política.

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 por todos os níveis do Conglomerado; e

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

- Prover os 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, com experiência e treinamento necessários.

- Reunir-se com a DEROC, no mínimo anualmente, como parte da avaliação da efetividade da gestão integrada de risco operacional, controles internos e *Compliance*.

- 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 reuniões periódicas e no relatório anual elaborado pela DEROC, bem como pela avaliação anual feita pelo Comitê de Auditoria.

Comitê de Auditoria

Cabe ao Comitê de Auditoria:

- Validar a Política de *Compliance* antes de seu 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, papéis 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.

Primeira Linha de Defesa

- Informar e capacitar colaboradores e prestadores de serviços terceirizados relevantes em assuntos relativos a Compliance;

- Relacionar-se com Órgãos Reguladores, Autorreguladores, Supervisores e Fiscalizadores, atendendo às suas solicitações e emitindo a eles os reportes devidos;

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

- 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;

- Definir e implantar os planos de ação para endereçamento dos apontamentos de não conformidade efetuados pelas auditorias interna e externa, Controles Internos, Compliance, reguladores, autorreguladores e demais órgãos de supervisão e fiscalização;

- Comunicar prontamente à área de Compliance sempre que identificar alterações em relação às normas e regulamentações vigentes ou riscos de Compliance não previstos pelas atividades de controle; e

- Manter a conformidade com as normas e exigências regulatórias locais e internacionais.

Segunda Linha de Defesa

Área de Riscos e Finanças

- Calcular, monitorar e controlar os limites operacionais estabelecidos pelos reguladores para garantir a aderência regulatória do Itaú Unibanco, mesmo quando não houver obrigatoriedade de envio periódico ao regulador.

Diretoria Executiva de Risco Operacional e Compliance

Cabe à Diretoria Executiva de Riscos Operacionais e Compliance, por meio das Diretorias de Compliance Corporativo e Controles Internos e Risco Operacional:

- Apoiar a primeira linha de defesa na observação de suas responsabilidades diretas;

- Disseminar os padrões de integridade e ética como parte da cultura de riscos e controles do Conglomerado, e divulgar as boas práticas e políticas relacionadas à função de Compliance;

- Orientar e aconselhar os administradores e colaboradores do Conglomerado, direcionando soluções específicas sobre o cumprimento de normas internas relacionadas ao Programa de Integridade e Ética;

- Orientar e aconselhar os administradores e colaboradores do Conglomerado, direcionando soluções específicas relacionadas ao cumprimento de normas externas;

- Avaliar os incentivos a cumprimento de regulamentações e compromissos assumidos com reguladores e reportar estes resultados aos Comitês de Remuneração e de Auditoria;

- Assegurar-se que as equipes 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;

- Categorizar os temas de Compliance conforme sua severidade e monitorar a exposição do conglomerado a esses riscos;

- Certificar a eficiência do ambiente de controle de Compliance da Primeira Linha de Defesa por meio de programas de monitoramento e testes, reportando os resultados à Alta Administração e aos órgãos reguladores, quando solicitado;

- Revisar e acompanhar os planos de ação adotados para o endereçamento dos apontamentos efetuados pelas auditorias interna e externa e órgãos reguladores;

- Reportar à Diretoria, ao Comitê de Auditoria, ao Comitê de Gestão de Risco e Capital e ao Conselho de Administração as situações relevantes e que não estejam em conformidade;
- Supervisionar as Unidades Internacionais na avaliação da aderência às diretrizes corporativas, bem como na adoção da metodologia de Compliance e monitoramento e reporte consolidado para a Matriz;
- Coordenar a implantação, o monitoramento e a evolução do Programa Corporativo de Integridade e Ética nas Unidades Internacionais; e
- Coordenar a governança de Programas de Compliance de regulamentações internacionais relevantes para o conglomerado.

Cabe exclusivamente à Diretoria de Compliance Corporativo:

- Manter evidência da aprovação deste documento pelo Conselho de Administração;
- Definir princípios e diretrizes para disseminação da Cultura de Compliance, incluindo treinamentos;
- Desenvolver e disponibilizar as metodologias, ferramentas, sistemas, infraestrutura e governança necessárias para suportar a função de Compliance nas atividades do Conglomerado e terceirizadas relevantes;
- Gerenciar o processo de captura, triagem, avaliação de impacto e monitoramento de aderência às regulamentações;
- Coordenar a governança de políticas e procedimentos do Itaú Unibanco, conforme regulamentações aplicáveis e melhores práticas de mercado;
- Realizar o monitoramento das Políticas de Investimentos Pessoais e da Política de Negociação de Valores Mobiliários de emissão do Itaú Unibanco Holding S.A.;
- Reportar tempestivamente informações relevantes, tanto dos resultados das avaliações de Compliance realizadas que tenham identificados falhas materiais, quanto de alterações significativas no ambiente regulatório;
- Enviar relatório anual ao Comitê de Auditoria e ao Conselho de Administração, contendo sumário dos resultados das atividades relacionadas aos temas de Compliance, principais conclusões, recomendações e planos de ação adotados para tratamento das deficiências identificadas;
- Gerir os programas de Integridade e Ética e Monitoramento de Práticas Abusivas (Trade Surveillance);
- Coordenar o relacionamento com reguladores, autorreguladores e demais órgãos de fiscalização e supervisão, acompanhando as ações originadas dos compromissos assumidos, facilitando o compartilhamento de informações e garantindo a consistência do posicionamento institucional.

Terceira Linha de Defesa

Verificar, 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 em documentos internos, e submeter os resultados dos seus apontamentos ao Comitê de Auditoria.

Aprovado pelo Conselho de Administração de 28/02/2019.