UBS BB: Regras, Procedimentos e descricao de Controles Internos – Resolucao CVM 161

Taxonomia: 2. Market Conduct

Responsável: Responsável pela Área de Conformidade e Controle de Risco Operacional do Banco de Investimentos (Head of C&ORC IB)

Propósito deste documento:
Este documento tem como intuito detalhar as regras e procedimentos relativos à segregação de atividades e a confidencialidade no exercício da atividade de intermediação de ofertas públicas em cumprimento a Resolução CVM nº 161, de 13 de julho de 2022.

Aplicabilidade

Responsabilidades	Riscos de Conformidade e Governança
Divisão de Negócios	Banco de Investimento
Área de Negócios	Global Banking, Global Markets, Research
Entidade Legal	UBS BRASIL CORRETORA DE CÂMBIO, TÍTULOS E VALORES MOBILIÁRIOS S.A.
Localidade	Brasil

Requerimentos Chave

Este documento contém informações sobre as regras e procedimentos e descricao de Controles Internos relativos ao ambiente de controle, observancia das regras e Codigo de Etica alem da observancia de segregação de atividades e confidencialidade (incluindo testes de seguranca) que a divisão de negócios Banco de Investimento do UBS BB deve seguir.

Palavras Chaves: Segregação de Atividades, Confidencialidade, Barreiras de Informação, Conformidade, Comissão de Valores Mobiliários, Regulamentação, Riscos de Conformidade, Governança, Procedimentos e Controles.

Índice

1. Introdução

1.1. Objetivo

Em consonância com os requerimentos previstos na Resolução nº 161 publicada pela CVM em 13 de julho de 2022, este documento tem como intuito detalhar as regras e procedimentos regras, procedimentos e descrição dos controles internos observados pela UBS BRASIL CORRETORA DE CÂMBIO, TÍTULOS E VALORES MOBILIÁRIOS S.A ("UBS") no exercício da atividade de coordenação e distribuição de ofertas públicas.

2. O Ambiente de Controle

A estrutura de controles internos, riscos operacionais e conformidade do UBS foi implementada em atendimento aos requerimentos e diretrizes estabelecidos na regulamentação brasileira vigente (em especial a CVM 161, objeto do presente documento) ou decorrentes da estrutura global do grupo UBS, compreendendo a identificação, mensuração, avaliação, monitoramento, mitigação, acompanhamento e reporte de riscos.

O ambiente de controles internos do UBS abrange a cultura de toda organização, sendo que a influência desses princípios e valores sobre a consciência de risco de seus colaboradores é a base para todos os outros componentes do gerenciamento de riscos corporativos, possibilitando uma abordagem transparente, disciplinada, consistente e estruturada dos riscos presentes na condução de suas atividades. As principais vertentes do ambiente de controle são: governança, supervisão, treinamento, cultura e controle.

3. Princípios, Valores e Conceitos

3.1 Ética e Integridade

A Alta Administração do UBS estabelece os princípios e as práticas que definem os padrões de ética e a forma de fazer negócios por meio do Código de Ética.

Ao segui-lo, fomenta-se a cultura onde o comportamento responsável será enraizado de forma a que proteja os clientes, os funcionários, a reputação e a capacidade de criar um valor duradouro para os acionistas, clientes e sociedade.

O UBS possui como responsabilidade supervisionar as atividades de seus colaboradores para assegurar o cumprimento das leis e regulamentações aplicáveis, bem como os documentos internos do UBS tais como, Politicas, Procedimentos e Manuais (incluindo aqueles relacionados aos Controles Internos). Sob nenhuma hipótese, o colaborador pode participar, direta ou indiretamente, consentir, ajudar e estimular quaisquer atividades corruptas ou ilegais, incluindo, mas não se limitando a: manipulação de mercado, suborno, uso indevido de informações privilegiadas, lavagem de dinheiro ou, efetuar ou receber pagamentos, presentes ou entretenimento para realizar negócios ou obter qualquer vantagem indevida.

Os novos colaboradores também participam de "Treinamento Introdutório" conduzido pela área de Conformidade e Controle de Riscos Operacionais (C&ORC), onde são explicados os princípios do UBS, as políticas relevantes, o Código de Ética, os treinamentos mandatórios, a política de investimento pessoal, o ambiente regulatório, as barreiras de informação, a política de combate à corrupção, a atividade transnacional ("Cross-Border"), a certificação, o conceito de informações confidenciais, as políticas e conceitos básicos de Proteção de Dados (Lei Geral de Proteção de Dados-LGPD) e os canais de denúncias, permitindo a todos a discussão do conteúdo e o esclarecimento de dúvidas.

Adicionalmente, todos os colaboradores têm acesso de consulta às políticas de forma irrestrita: as políticas são disponibilizadas na intranet do UBS no Brasil e aquelas que representem risco material para o UBS, conforme critérios da estrutura de risco operacional, também são publicadas no repositório global, acessível a todos os colaboradores pela intranet.

3.2 Código de Ética

O Código de Ética é de observância obrigatória por todos os colaboradores no UBS. É o que se espera de todos. Ele abrange o relacionamento com clientes, contrapartes,

acionistas, agências reguladoras, parceiros de negócios e colegas. É a base das políticas, diretrizes e procedimentos.

O desconhecimento do Código não é uma opção e, portanto, não há desculpa para violá-lo. Eventuais descumprimentos do Código sujeitam o responsável a ação disciplinar, que inclui, mas não se limita, a possibilidade de seu desligamento.

Eventuais violações ao Código são tratadas segundo política e procedimentos próprios, havendo, também, área específica fora do Brasil dedicada ao assunto, que acompanha os processos juntamente com os times locais de Conformidade e Recursos Humanos. O propósito dessa estrutura é prover uma abordagem definida e clara para (i) responder de maneira justa e consistente às violações do Código de Ética, políticas internas, procedimentos e diretrizes; (ii) garantir o cumprimento das obrigações legais e regulamentares.

3.3 Segregação entre Áreas de Controle e de Negócios

No Conglomerado, as áreas de negócios encontram-se segregadas de áreas de controles, observando regras de segregação de ambientes físico e lógico, de forma a mitigar potenciais situações de conflito de interesse.

A gestão de negócios, como primeira linha de defesa, é a responsável primária pelas exposições em riscos e deve manter processos e sistemas eficientes para o seu gerenciamento, incluindo controles internos abrangentes e procedimentos devidamente documentados.

Já o controle de riscos (segunda linha de defesa) é executado por áreas específicas e independentes, sob a coordenação do Diretor de Risco e Conformidade (“CRO”), estando segregadas das áreas de negócio e de auditoria interna.

Os colaboradores do Conglomerado UBS trabalham em um ambiente complexo de negócios e estão expostos a inúmeros potenciais conflitos de interesse internos e externos. A Alta Administração adota políticas e procedimentos destinados a minimizar ou prevenir tais conflitos, compreendendo por exemplo:

- Barreiras de Informações,
- Segregação física e lógica,
- Finanças pessoais,

- Presentes, gratificações, entretenimento, tratamento preferencial, suborno e propinas,
- Atividades externas, incluindo negócios, política e outras atividades,

4. Barreiras de Informação e Restrição de Acesso Físico

4.1. O que são Barreiras de Informação?

As Barreiras de Informação são medidas organizacionais implementadas que ajudam na prevenção da divulgação não autorizada, da utilização abusiva de informações protegidas e na gestão de conflitos de interesses.

Elas são aplicadas usando segregação física e restringindo o acesso a locais de interesse e/ou sistemas.

As Barreiras de Informação permitem que algumas áreas do Banco de Investimento do Grupo UBS continuem suas atividades normais, apesar de outras áreas estarem em posse de informações protegidas.

Existem três barreiras de informação estabelecidas dentro do UBS Banco de Investimento:

- *Global Banking (área responsável pela coordenação e distribuição de ofertas públicas)*
- *Global Research (área de análise de valores mobiliários, disciplinada pela Resolução CVM 20)*
- *Credit Risk Control*

4.2. Classificações dos Funcionários em relação às Barreiras de Informação

A todos os colaboradores e administradores (“Funcionários”) é atribuída uma classificação em relação a cada uma das Barreiras de Informação dentro do Grupo UBS. A descrição das classificações existentes e os critérios para se classificar os Funcionários em relação a cada uma das Barreiras de Informação constam da Política de Barreiras de Informação do Grupo UBS.

4.3. Restrição de Acesso Físico e Lógico

De acordo com as Políticas Globais do Grupo UBS, os Funcionários: (i) nunca devem compartilhar sua credencial de acesso físico; (ii) nunca devem permitir que indivíduos entrem em áreas restritas se não tiverem certeza que eles estão autorizados; (iii) devem acompanhar e/ou supervisionar visitantes diligentemente; (iv) devem praticar os princípios de *clean-desk* (mesa limpa); (v) devem proteger as informações físicas do Grupo UBS de acordo com as suas classificação e sempre destruir documentos não públicos usando os trituradores do escritório ou caixas de descarte seguras; (vi) questionar qualquer pessoa que se comporte de forma suspeita e reporta-la à organização de segurança local; e (vii) nunca tentar contornar as medidas de segurança física estabelecidas.

Não obstante a presença de barreiras de informações físicas para pessoas não autorizadas, todos os Funcionários responsáveis pela coordenação e distribuição de valores mobiliários devem estar vigilantes ao permitir o acesso a áreas dentro das Barreiras de Informações aprimoradas.

Restrições de natureza sistêmica/eletrônica também são mantidas, destacando-se:

- Separação física e eletrônica do negócio/função relevante em um nível acordado e implementado pela administração e área de Sala de Controle;

- Separação adequada do negócio/função relevante em termos de suporte administrativo e operacional (incluindo sistemas e restrições de acesso lógico a aplicativos e pastas compartilhadas); e

- Armazenamento seguro e acesso limitado a Informações Protegidas, tanto em cópia impressa quanto em formato eletrônico.

4.4. Reporte de Incidentes, Deficiências e/ou Vulnerabilidades

É responsabilidade de cada Funcionário relatar incidentes de segurança, incluindo violações de políticas e procedimentos para a organização de segurança local.

Uma vez identificadas deficiências e/ou vulnerabilidades, essas devem ser efetivamente comunicadas, atribuídas à um responsável, rastreadas e remediadas.

5. Informações Protegidas e Confidenciais e função da Sala de Controle

5.1. Informações Protegidas

As Informações Protegidas incluem informações comerciais confidenciais e aquelas não publicadas e sensíveis ao preço. Não incluem dados pessoais confidenciais relacionados aos Funcionários do Grupo UBS.

5.2. Informações Não Publicadas e Sensíveis aos Preços (UPSI)

Informações Não Publicadas e Sensíveis aos Preços (UPSI), são todas aquelas de natureza factual que não sejam públicas relacionadas direta ou indiretamente com um emitente de instrumentos financeiros e que, se forem públicas, possam afetar o preço desses instrumentos financeiros. Também significa informações que os investidores considerariam relevantes para determinar se devem comprar, vender, manter ou votar relacionadas a esses instrumentos financeiros. Essas informações também podem ser referidas como informações materiais não públicas (MNPI).

5.3. Informações Comerciais Confidenciais

Informações Comerciais Confidenciais são aquelas que não são inéditas e sensíveis a preços, mas, no entanto, não são públicas e são transmitidas, produzidas, desenvolvidas ou mantidas em circunstâncias que indicam que deveriam ser classificadas como confidenciais.

5.4. Conduta no Tratamento de Informações Protegidas

Em caso de possível ou efetivo recebimento de Informações Protegidas por erro, por meio de comunicações normais com clientes ou com propósito legítimo de negócio, deve ser dado o tratamento adequado às informações recebidas conforme políticas e

procedimentos globais do Grupo UBS. Isso inclui notificar imediatamente a área de Sala de Controle (“*Control Room”)* regional, quando necessário.

Os Funcionários só devem receber ou ter acesso às informações necessárias para o bom desempenho de suas atividades e não devem compartilhar essas informações com ninguém, dentro ou fora do Grupo UBS, que não tenha uma necessidade comercial legítima de ter acesso a tais dados.

5.5. Responsabilidades da área de “Sala de Controle”

Dentre outras funções, a área de Sala de Controle auxilia na gestão da informação sensível dentro da instituição por meio do registro de operações e eventos sobre os quais o Grupo UBS possua Informação Protegida, Informação Confidencial ou UPSI e situações em que um indivíduo esteja cruzado em relação a uma barreira de informação.

5.6. Treinamentos para Funcionários com acesso a Informações Protegidas e Confidenciais

O Grupo UBS possui programa de treinamento de Funcionários relacionado a Informações Protegidas e Confidenciais denominado “Conduta de Mercado” que aborda, dentre outros temas, (i) conceitos de Informação Protegida e Confidencial, (ii) o tratamento e cuidado que tais informações devem ter e (iii) os canais de reporte aplicáveis. O treinamento é realizado em periodicidade anual.

5.7. Avaliação Periódica de Ameaças e Vulnerabilidade

O UBS possui uma política local e o suporte da estrutura global do Chefe de Segurança da Informação (*Chief Information Security Office* -”CISO"), que realiza o gerenciamento dos riscos relacionados à Segurança da Informação e Segurança Cibernética, implementa mecanismos de proteção e respostas a incidentes e determina procedimentos para monitoramento de ameaças e vulnerabilidades, tais como monitoramento de rede, teste de vulnerabilidades, prevenção ao vazamento de informações.

A área possui um processo contínuo de coleta, processamento, análise e disseminação de informações relacionadas à segurança da informação que podem indicar situações de risco atuais ou em potencial. Seu objetivo é identificar oportunidades de melhoria dos mecanismos de proteção, detecção e resposta a ameaças.

Além do processo de avaliação de risco, o UBS também conduz avaliações técnicas pontuais para questões de risco de segurança cibernética.

O UBS conta também com a área de Operações Cibernéticas (*Cyber Operations)*, que realiza o monitoramento contínuo de ameaças cibernéticas, identifica ameaças e gerência as ações para contenção e eliminação de eventuais ataques.

O UBS possui controles para identificar vazamento de dados confidenciais. A solução de Prevenção de vazamento de dados busca por padrões e identificadores em dados enviados para fora do UBS que possam indicar vazamento de informação.

Preventivamente, o UBS periodicamente realiza buscas por vulnerabilidades que, quando identificadas, são classificadas de acordo com o risco associado e necessitam de plano de remediação.

6. Vigência

A área de Conformidade e Controle de Risco Operacional do Banco de Investimentos é responsável por assegurar que este documento seja revisado a cada 12 meses ou, antecipadamente, sempre que necessário, de modo que reflita os processos estabelecidos e que esteja em acordo com as regulamentações locais e os requisitos das Políticas do UBS relacionadas.

7. Violações da Política

O descumprimento das exigências previstas neste Manual, e consequentemente das Políticas do UBS relacionadas, pode estar sujeito à estrutura de violação da área de

Conformidade ("*Compliance*"), conforme a "Política de Violações de *Compliance*", que pode resultar em ação disciplinar, até e inclusive demissão.

8. Políticas Relacionadas

1-P-004686 – Information Barriers Policy (Política de Barreiras de Informação)

1-P-011810 – Group Data Ethics Policy (Codigo de Etica)