MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS (“Manual”)

INTRABANK ASSET MANAGEMENT (“GESTORA”)

Fevereiro - 2022

ÍNDICE

1. Objetivo e Aplicabilidade

Estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a Gestora, tanto na sua atuação interna quanto na comunicação com os diversos públicos, visando ao atendimento de padrões éticos cada vez mais elevados.

A Gestora e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Manual, informando qualquer irregularidade à Diretora de Compliance e de Gestão de Risco, conforme definida no contrato social vigente da GESTORA.

2. Base Legal

(i) Item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014;
(ii) Resolução CVM nº 21, de 25 de Fevereiro de 2021, conforme alterada ("Resolução CVM nº 21");
(iii) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Ética ("Código ANBIMA de Ética");
(iv) Código de Administração de Recursos de Terceiros ("Código de ART");
(v) Código de Certificação ("Código ANBIMA de Certificação");
(vi) Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção"); e
(vii) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora

3. Responsabilidades

Cabe à GESTORA, garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade e aos seus padrões éticos e profissionais, conforme detalhado adiante.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à GESTORA contidas neste Manual e nas demais políticas e manuais internos aplicáveis, zelando para que todas as normas éticas e legais sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação à Diretora de *Compliance* e de Gestão de Risco.

As comunicações, orientações e dúvidas devem ser direcionadas à Diretora de *Compliance* e de Gestão de Risco através de *e-mail* ou telefone.

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, que, ao receberem o presente Manual, deverão assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Recebimento e Compromisso"), a fim de demonstrar que aceitam expressamente as normas, princípios, conceitos e valores aqui estabelecidos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. As principais normas aplicáveis às atividades da Gestora constam no **Anexo III** do presente Manual.

4. Manual de *Compliance*

4.1 Introdução

4.1.1 Estrutura de Governança e Mecanismos de *Compliance*

A estrutura de governança da GESTORA é formada fundamentalmente: (i) pela Diretoria de Gestão de Carteira de Valores Mobiliários; (ii) pelo Comitê de Investimento e Crédito; (iii) pela Diretoria de *Compliance* e de Gestão de Risco; e (iv) pelo Comitê de *Compliance*, Controles Internos, Ética e Risco.

As disposições referentes aos Comitê de Investimento e Crédito e Comitê de *Compliance*, Controles Internos, Ética e Risco encontram-se previstas em Regimento Interno da GESTORA.

4.1.2 Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição da Diretora de *Compliance* e de Gestão de Risco, indicada como diretora responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretora de *Compliance* e Gestão de Risco"), nos termos da Resolução CVM nº 21.

São obrigações da Diretoria de *Compliance* e Gestão de Risco, dentre outras tarefas:

- ✓ Designar o secretário das reuniões do Comitê de *Compliance*, Controles Internos, Ética e Risco;
- ✓ Acompanhar as políticas descritas neste Manual;
- ✓ Realizar, sempre que necessário, o informe de transações suspeitas junto ao Conselho de Controle de Atividades Financeiras - COAF ou o reporte negativo anual, nos termos da legislação, caso

seja aplicável;

✓ Controlar a aderência às novas leis, regulamentações, práticas e diretrizes de autorregulação aplicáveis à GESTORA, e apresentar o resultado de suas verificações no Comitê de *Compliance*, Controles Internos, Ética e Risco;

✓ Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade da GESTORA para apreciação dos administradores da GESTORA;

✓ Atender prontamente todos os Colaboradores;

✓ Auxiliar o Comitê de *Compliance*, Controles Internos, Ética e Risco em qualquer questão atinente a sua área;

✓ Identificar possíveis condutas contrárias a este Manual;

✓ Implementar a Política de Gestão de Riscos, planejando a execução e executando os procedimentos definidos pelo Comitê de *Compliance*, Controles Internos, Ética e Risco;

✓ Centralizar informações e revisões periódicas dos processos de *compliance*, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;

✓ Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;

✓ Controlar e monitorar as licenças legais, registros e certificações necessárias (registros na CVM, na ANBIMA e demais aplicáveis), bem como sua renovação/manutenção junto às autoridades;

✓ Garantir que os controles internos sejam compatíveis com os riscos da GESTORA em suas atividades, bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários;

✓ Estabelecer controles para que todos os Colaboradores da GESTORA que desempenhem funções ligadas à gestão de fundos de investimento atuem com independência e atentem ao devido dever fiduciário para com seus clientes, e que os interesses comerciais, ou aqueles de seus clientes não desviem o foco de seu trabalho;

✓ Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da GESTORA;

✓ Analisar informações, indícios ou identificar, administrar e, se necessário, levar o tema para análise e deliberação no Comitê de *Compliance*, Controles Internos, Ética e Risco, no caso de eventuais conflitos de interesses ou descumprimentos regulatórios e de políticas e normas internas da GESTORA;

✓ Elaborar relatório anual listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa – PLD/FTP e de Cadastro da GESTORA;

✓ Encaminhar aos órgãos de administração da GESTORA, até o último dia útil do mês de abril de cada ano, relatório referente ao ano civil imediatamente anterior à data de entrega, contendo: (a) as

conclusões dos exames efetuados; (b) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (c) a manifestação do Diretor de Gestão a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las, devendo referido relatório permanecer disponível à CVM na sede da GESTORA;

✓ Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;

✓ Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;

✓ Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de *compliance* previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

✓ Garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;

✓ Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;

✓ Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance*, Controles Internos, Ética e Risco, registrando suas decisões em atas;

✓ Aplicar as eventuais sanções aos Colaboradores, conforme definidas pelo Comitê de *Compliance*, Controles Internos, Ética e Risco; e

✓ Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- Investimentos pessoais;
- Transações financeiras com clientes fora do âmbito da GESTORA;
- Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
- Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
- Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
- Participações em alguma atividade política.

A Diretora de *Compliance* e de Gestão de Risco poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de *compliance* e de risco, com as atribuições a serem definidas caso a caso, a depender da necessidade da GESTORA em razão de seu crescimento e de acordo com a senioridade do Colaborador.

Ademais, a GESTORA, conforme já mencionado acima, possuirá também um Comitê de *Compliance*, Controles Internos, Ética e Risco, com suas atribuições e características previstas em Regimento Interno da GESTORA.

4.2 Garantia de Independência

A Diretoria de *Compliance* e de Gestão de Risco e o Comitê de *Compliance*, Controles Internos, Ética e Risco exercem suas atividades de forma completamente independente das outras áreas da GESTORA e poderão exercer seus poderes e autoridade com relação a qualquer Colaborador.

4.3 Dúvidas ou Ações Contrárias aos Princípios e Normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da GESTORA, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de *compliance* e princípios que orientam as ações da GESTORA.

Toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso da Diretora de *Compliance* e de Gestão de Risco, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da GESTORA, deve ser dirigida pela pessoa aplicável à Diretora de *Compliance* e de Gestão de Risco.

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento à Diretora de *Compliance* e de Gestão de Risco. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. O Colaborador que se omitir de tal obrigação poderá sofrer, além de ação disciplinar, demissão por justa causa, conforme regime jurídico e observadas as disposições constantes deste Manual.

Caso a violação ou suspeita de violação recaia sobre a própria Diretora de *Compliance* e de Gestão de Risco, o Colaborador deverá informar diretamente aos demais administradores da GESTORA.

4.4 Acompanhamento das Políticas descritas neste Manual

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da GESTORA, que cheguem ao conhecimento da Diretora de *Compliance* e de Gestão de Risco, de acordo com os procedimentos estabelecidos neste Manual, esta utilizará os registros e sistemas de monitoramento eletrônico referidos

neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pela Área de *Compliance* e Controles Internos da GESTORA, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso a Área de *Compliance* e Controles Internos julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se tratam de ferramentas de trabalho disponibilizadas pela GESTORA.

Adicionalmente, será realizado um monitoramento **anual**, pela Área de *Compliance* e Controles Internos, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pela Área de *Compliance* e Controles Internos, para que sejam verificados os arquivos eletrônicos, inclusive *e-mails*, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

Ainda, a Área de *Compliance* e Controles Internos deverá verificar, **anual**, os níveis de controles internos e *compliance* junto a todas as áreas da GESTORA, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas da GESTORA, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

A Diretora de *Compliance* e de Gestão de Risco poderá utilizar as informações obtidas em tais monitoramentos para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

Além dos procedimentos de supervisão periódica, a Área de *Compliance* e Controles Internos poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

4.5 Mecanismos Adicionais de *Compliance* e Controles Internos

Além da aplicação das políticas e controle de seus procedimentos em si, são também importantes mecanismos de *compliance* e controles internos da GESTORA:

✓ A disseminação e o conhecimento do conteúdo dos termos e dos documentos internos da GESTORA aplicáveis acima, atestado com a assinatura do Termo de Conhecimento e Aceitação do Código de Ética e Conduta Profissional da GESTORA e das demais Políticas, Manuais e Documentos Internos por todos os Colaboradores, o qual é parte integrante do Código de Ética e Conduta Profissional

da GESTORA;

- ✓ Controle da regularidade das certificações;
- ✓ Teste e Relatório de Aderência Anual;
- ✓ Teste do Sistema de Informações Anual: conforme descrito na Política de Segurança da Informação e Segurança Cibernética, os testes periódicos dos sistemas de informações, em especial para os mantidos em meio eletrônico, efetuados pela Diretora de *Compliance* e de Gestão de Risco, devem: (i) assegurar que os recursos humanos e computacionais estão adequados ao porte e à área de atuação da GESTORA; (ii) garantir o adequado nível de confidencialidade e acessos às informações confidenciais; (iii) assegurar que os recursos computacionais sejam protegidos contra adulterações; e (iv) assegurar que a manutenção de registros permita a realização de auditorias e inspeções;
- ✓ Implementação de Regras e Guarda de Evidências: monitorar a adequada implementação de procedimentos necessários para o cumprimento das normas, e das políticas internas, bem como a adequada manutenção de mecanismos de guarda de evidências que demonstre a sua aplicação;
- ✓ Salvaguarda de Informações: manter, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela regulação aplicável, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais pelas respectivas imagens digitalizadas.

4.6 Disposições Gerais e Sanções

Todos os Colaboradores devem estar comprometidos com a cultura de *compliance* e reportar imediatamente à Diretora de *Compliance* e de Gestão de Risco qualquer suspeita e/ou evidência de desconformidade por eles verificada.

É responsabilidade de todos os Colaboradores da GESTORA o cumprimento das normas legais, infralegais e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da GESTORA, devendo comunicar imediatamente a ocorrência de violações e/ou indícios de violação à Diretora de *Compliance* e de Gestão de Risco.

Os controles internos e monitoramentos de conformidade determinados neste Manual são prerrogativa exclusiva dos integrantes da Área de *Compliance* e Controles Internos, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade.

Quando constatada uma violação, o violador será convocado a prestar esclarecimentos ao Comitê de *Compliance*, Controles Internos, Ética e Risco. Caberá ao Comitê de *Compliance*, Controles Internos, Ética e Risco tomar as medidas necessárias. As sanções decorrentes de uma violação serão definidas pelo Comitê de *Compliance*, Controles Internos, Ética e Risco. As sanções que poderão ser aplicadas

são: advertência, com impacto no bônus do Colaborador e, no caso de o Colaborador receber mais de 03 (três) advertências, ocorrerá o desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da GESTORA, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da GESTORA.

Nesse último caso, nos termos do Art. 482 da Consolidação das Leis Trabalhistas – CLT, sem prejuízo do direito da GESTORA de pleitear indenização pelos eventuais prejuízos sofridos, perdas e danos e/ou lucros cessantes, por meio de medidas legais.

4.7 Recrutamento e Seleção

A contratação de futuros Colaboradores pela GESTORA considerará a qualificação adequada para cada posição a ser ocupada, e avaliará não somente a formação técnica dos candidatos, mas também suas experiências em trabalhos anteriores.

Não serão admitidas na GESTORA as práticas de discriminação, perseguição ou represálias por motivos de idade, raça, cor, religião, sexo, gravidez, nacionalidade, cidadania, opção sexual, deficiência física, estado civil, características genéticas de uma pessoa ou qualquer outra característica protegida por lei.

Especificamente para os Colaboradores envolvidos na área de gestão de carteira de valores mobiliários com alçada para tomada de decisões de investimento e desinvestimento, a contratação do futuro Colaborador pela GESTORA estará condicionada à devida certificação do Colaborador, conforme melhor detalhado na Política de Certificação contida neste Manual.

5. Política de Confidencialidade

5.1 A quem se aplica?

A todos os Colaboradores.

5.2 Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política de Confidencialidade, informando quaisquer irregularidades à Diretora de *Compliance* e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de *Compliance*, Controles Internos, Ética e Risco, o qual decidirá sobre eventuais medidas cabíveis. A Diretora de *Compliance* e de Gestão de Risco deve garantir o pleno atendimento a esta Política de Confidencialidade, sendo a responsável por temas relacionados à confidencialidade.

5.3 Sigilo e Conduta

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no **Anexo II** a este Manual ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve ser divulgada fora da GESTORA.

Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de *compliance* da GESTORA.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins desta Política de Confidencialidade, independente destas informações estarem contidas em discos, pen-drives, fitas, *e-mails*, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a GESTORA, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da GESTORA, incluindo:

- ✓ Informações que identifiquem dados pessoais, patrimoniais ou estratégicos;
- ✓ Informações que sejam objeto de acordo de confidencialidade celebrado com terceiros;
- ✓ Informações que identifiquem ações estratégicas – dos negócios da empresa, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão dos negócios, clientes e fundos de investimentos geridos pela GESTORA, ou reduzir sua vantagem competitiva;
- ✓ Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente que digam respeito às atividades da GESTORA e que sejam devidamente identificadas como sendo confidenciais, constituam propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- ✓ Informações que sejam assim consideradas face a determinação legal, previsão legal e/ou regulamentar;
- ✓ Informações que o Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível;
- ✓ *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- ✓ Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e fundos geridos pela GESTORA;
- ✓ Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela GESTORA;
- ✓ Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- ✓ Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da GESTORA e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações),

informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da GESTORA e que ainda não foi devidamente levado à público;

- ✓ Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
- ✓ Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
- ✓ Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da GESTORA ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento. A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados.

Sem prejuízo da colaboração da GESTORA com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada à Diretora de *Compliance* e de Gestão de Risco, para que esta avalie e submeta ao Comitê de *Compliance*, Controles Internos, Ética e Risco, o qual decidirá a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading*, Dicas ou *Front-running*.

Insider Trading e "Dicas"

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da GESTORA, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

Front-running significa a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a GESTORA, mas também após o seu término.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável, incluindo eventual demissão por justa causa.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento da Diretora de *Compliance* e de Gestão de Risco, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação à Diretora de *Compliance* e de Gestão de Risco anteriormente mencionada.

Na atividade de gestão, a GESTORA considera que o controle do fluxo de informações é o risco mais relevante em termos de controle estratégico para o negócio. A mitigação de tal risco se dá através de procedimentos operacionais de segurança, ligados ao uso de equipamentos internos (mitigado através dos contratos/sistemas fornecidos pelos prestadores de serviço), e, através de procedimentos internos que parametrizam o comportamento dos Colaboradores, descritos neste Manual.

Não caracteriza descumprimento desta Política de Confidencialidade a divulgação de Informações Confidenciais mediante prévia autorização da Diretora de *Compliance* e de Gestão de Risco, após deliberação do Comitê de *Compliance*, Controles Internos, Ética e Risco, em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, seja em âmbito municipal, estadual ou federal, bem como, quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente a Diretora de *Compliance* e de Gestão de Risco acerca da possibilidade de compartilhamento da Informação Confidencial, a qual deverá se manifestar formalmente sobre o caso, podendo inclusive levar tal dúvida ao Comitê de *Compliance*, Controles Internos, Ética e Risco.

6. Políticas de Treinamento

Treinamento Inicial e Processo de Reciclagem: A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, bem como de reciclagem **anual** dos seus Colaboradores, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais

programas de reciclagem.

Responsabilidade: Equipe de Compliance e Risco, a qual poderá contratar profissionais especializados para conduzirem os treinamentos.

Implementação e Conteúdo: Deve abordar as atividades da Gestora, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Manual (especialmente aquelas relativas à confidencialidade, segurança das informações e segurança cibernética), bem como aquelas descritas no Código de Ética, na Política de Investimentos Pessoais e na Política de Prevenção a Lavagem de Dinheiro da Gestora e, ainda, as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo IV** deste Manual.

7. Política de Segurança da Informação e Segurança Cibernética

7.1 Introdução

As medidas de segurança da informação e segurança cibernética têm por finalidade minimizar as ameaças aos negócios da GESTORA e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da GESTORA são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A Política de Segurança da Informação e Segurança Cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela GESTORA.

A coordenação direta das atividades relacionadas à Política de Segurança da Informação e Segurança Cibernética ficará a cargo da Diretora de *Compliance* e de Gestão de Risco, que será a responsável, inclusive, por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

7.2 A quem se aplica?

A todos os Colaboradores.

7.3 Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política de Segurança da Informação e Segurança Cibernética, informando quaisquer irregularidades à Diretora de *Compliance* e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de *Compliance*, Controles Internos, Ética e Risco, o qual decidirá sobre eventuais medidas cabíveis.

A Diretora de *Compliance* e de Gestão de Risco deve garantir o atendimento a esta Política de Segurança da Informação e Segurança Cibernética, sendo a responsável por temas de segurança da informação e segurança cibernética.

7.4 Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na GESTORA:

✓ Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando ele for de fato necessário;
✓ Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
✓ Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da GESTORA:

✓ As Informações Confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
✓ A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;
✓ A concessão de acessos às Informações Confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Desta forma, há a segregação lógica das informações, de modo que e somente os Colaboradores autorizados têm acesso às pastas virtuais respectivas às suas atividades desenvolvidas na GESTORA;
✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
✓ Segregação de instalações, equipamentos e informações comuns, quando aplicável; e
✓ A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados à Diretora de *Compliance* e de Gestão de Risco pelo responsável pelo Departamento de

Tecnologia da GESTORA.

7.5 Procedimentos de Segurança Cibernética

7.5.1 Identificação e Avaliação de Riscos (*Risk Assesment*)

No âmbito de suas atividades, a GESTORA identificou os seguintes principais riscos internos e externos que precisam de proteção:

✓ Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria GESTORA, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
✓ Sistemas: informações sobre os sistemas utilizados pela GESTORA e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
✓ Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da GESTORA; e
✓ Governança da Gestão de Risco: a eficácia da gestão de risco pela GESTORA quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a GESTORA identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

✓ *Malware* – *softwares* desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
✓ Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);
✓ Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
✓ Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no disposto acima, a GESTORA avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

7.5.2 Ações de Prevenção e Proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados e de

serviços que a GESTORA adota, sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamento relevantes. A GESTORA adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso.

A GESTORA trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário. Ainda, a concessão de acesso pela GESTORA fora implementada de modo que pode ser revogada rapidamente, se necessário.

Os eventos de *login* e alteração de senhas são auditáveis e rastreáveis. A GESTORA criará logs e trilhas de auditoria sempre que os sistemas permitam.

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos *e-mails* que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas **trimestralmente**, conforme aviso fornecido pelo responsável pelo Departamento de Tecnologia da GESTORA.

O acesso remoto a arquivos e sistemas internos ou na nuvem (*cloud*) é permitido, pois estes contam com controles adequados. O acesso ao acervo digital conta com dupla verificação. Quando o Colaborador acessa o office365 para logar, é enviado um código de segurança no seu celular, garantindo a autenticidade.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a GESTORA deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A GESTORA ainda conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais. A GESTORA deve, adicionalmente, proibir o acesso a determinados *websites* e a execução de *softwares* e/ou aplicações não autorizadas.

A GESTORA mantém proteção atualizada contra *malware* nos seus dispositivos e *software* antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras **semanais** para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da GESTORA. Ainda, serão realizados trimestralmente testes de invasão externa, *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da GESTORA e circulem em ambientes externos à

GESTORA com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como Informações Confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pela Diretora de *Compliance* e de Gestão de Risco.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da GESTORA. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na GESTORA.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A GESTORA adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Contingência e Continuidade dos Negócios da GESTORA. O *backup* de todos os dados e informações da GESTORA é realizado **diariamente** na nuvem.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo Informações Confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Art. 18 da Resolução CVM nº 21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da GESTORA e devem ser observadas integralmente.

A GESTORA possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A GESTORA mantém inventários atualizados de *hardware* e *software*, e

verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da GESTORA deve diligenciar para manter os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. Os logs e trilhas de auditoria criados devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

7.5.3 Monitoramento e Testes

A GESTORA adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **anual**:

✓ Monitoramento, por amostragem, do acesso dos Colaboradores a *sites*, blogs, fotologs, *webmails*, entre outros, bem como os *e-mails* enviados e recebidos;
✓ Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela GESTORA para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da GESTORA; e
✓ Verificação, por amostragem, das informações de acesso ao espaço do escritório, a *desktops*, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Área de *Compliance* e Risco poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

7.5.4 Plano de Identificação e Resposta

7.5.4.1 Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da GESTORA (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretora de *Compliance* e Gestão de Risco prontamente. A Diretora de *Compliance* e Gestão de Risco levará tal questão ao Comitê de *Compliance*, Controles Internos, Ética e Risco, que determinará quais membros da administração da GESTORA e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Comitê de *Compliance*, Controles Internos, Ética e Risco determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

7.5.4.2 Procedimentos de Resposta

A Diretora de *Compliance* e Gestão de Risco responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da GESTORA de acordo com os critérios abaixo:

- ✓ Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
- ✓ Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- ✓ Determinação dos papéis e responsabilidades do pessoal apropriado;
- ✓ Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- ✓ Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
- ✓ Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da GESTORA, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
- ✓ Determinação do responsável (ou seja, a GESTORA ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo da Diretora de *Compliance* e Gestão de Risco, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

7.6 Processos e Controles de Segurança da Informação

Para assegurar que as informações sejam adequadamente protegidas, a GESTORA definiu os seguintes processos/controles:

7.6.1 Identificação da Informação

O Colaborador que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

7.6.2 Classificação da Informação

Algumas informações podem enquadrar-se como Informações Confidenciais.

Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

7.6.3 Controles para Informações Classificadas como "Informações Confidenciais"

O acesso às Informações Confidenciais deve ser controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão da Diretora de *Compliance* e de Gestão de Risco, e, se reputado necessário, da assessoria jurídica da GESTORA.

7.6.4 Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento e descarte.

O Colaborador responsável pela informação gerada deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte. Em caso de dúvida, o Colaborador deverá consultar a Diretora de *Compliance* e de Gestão de Risco.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

7.6.5 Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

7.6.6 Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na GESTORA são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia da Diretora de *Compliance* e de Gestão de Risco.

A GESTORA poderá, a qualquer momento e mediante prévia aprovação da Diretora de *Compliance* e de Gestão de Risco:

- ✓ Inspecionar conteúdo e registrar o tipo de uso dos *e-mails* feitos pelos usuários;
- ✓ Disponibilizar esses recursos a terceiros, caso entenda necessário; e
- ✓ Solicitar aos usuários justificativas pelo uso efetuado.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao

impedimento de acesso não autorizado pelo ex-Colaborador.

7.6.7 Boas Práticas de Utilização

A utilização da rede, internet, *e-mail* e dispositivos móveis na GESTORA e/ou pelos seus Colaboradores em comunicações de trabalho devem se guiar pelas seguintes regras:

- ✓ Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- ✓ Somente imprimir as mensagens quando realmente necessário;
- ✓ Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para evitar vírus ou códigos maliciosos;
- ✓ No caso de recebimento de mensagens que contrariem as regras estabelecidas pela GESTORA, nunca as repassar, alertando o responsável da sua área e a Diretora de *Compliance* e de Gestão de Risco, se for o caso;
- ✓ Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho; e
- ✓ Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de *e-mail*.

7.6.8 Vedações

É vedado ao usuário:

- ✓ Enviar *e-mail* ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais, sendo proibido, sobretudo, conteúdo pornográfico, racista, subversivo ou ofensivo à moral e aos princípios éticos;
- ✓ Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da GESTORA, ou qualquer outra informação sobre a GESTORA, seus negócios, produtos, equipamentos ou Colaboradores, sem prévia aprovação para isso. Em caso de exigência de alguma autoridade ou entidade autorreguladora, solicitar orientação à Diretora de *Compliance* e de Gestão de Risco;
- ✓ Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;
- ✓ Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados residentes na rede da GESTORA;
- ✓ Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da GESTORA;
- ✓ Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pela Diretora de *Compliance* e de Gestão de Risco;

✓ Contratar provedores de acesso sem autorização prévia autorização da Diretora de *Compliance* e de Gestão de Risco;

✓ Redirecionar caixa postal pessoal (*e-mail* de outros provedores) para a sua caixa postal de correio eletrônico na GESTORA e vice-versa.

7.6.9 Bloqueio de Acesso a Sites

A Diretora de *Compliance* e de Gestão de Risco, juntamente com os responsáveis pelo Departamento de Tecnologia da GESTORA, são responsáveis por monitorar os acessos feitos a *sites* através de computadores de propriedade da GESTORA, para reporte de eventual mau uso ao Comitê de *Compliance*, Controles Internos, Ética e Risco e bloqueio de acesso a sites proibidos.

7.6.10 Sites de Armazenamentos de Arquivos

O acesso a sites de armazenamento de arquivos em "nuvem" é permitido.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à GESTORA.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da GESTORA, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas à Diretora de *Compliance* e de Gestão de Risco, que poderá ou não conceder a exceção.

7.7 Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de segurança da informação devem ser reportados à Diretora de *Compliance* e de Gestão de Risco, que adotará as medidas cabíveis. Nesse sentido, cabe mencionar que a GESTORA possui um Plano de Contingência e Continuidade dos Negócios, que mais bem detalha como os incidentes devem ser tratados.

7.7.1 Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à GESTORA, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, *e-mails*, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da GESTORA, razão

pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na GESTORA, devendo todos os documentos permanecer em poder e sob a custódia da GESTORA, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da GESTORA, salvo se autorizado expressamente pela GESTORA e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à GESTORA documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à GESTORA, o Colaborador deverá assinar declaração nos termos do **Anexo IV** ao presente Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da GESTORA, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da GESTORA, exceto se aprovado expressamente pela GESTORA.

7.7.2 Rastreamento

É permitido o uso pessoal dos equipamentos de informática e de comunicação de propriedade da GESTORA utilizados pelos Colaboradores para a realização das atividades profissionais. Lembrando que, como tais recursos (*e-mails*, sistemas, computadores, telefones etc.) pertencem à GESTORA, estes são rastreáveis e sujeitos a monitoramento, nos termos já dispostos neste Manual, bem como podem se tornar públicos em caso de auditoria, exigência judicial e/ou regulatória.

7.8 Treinamento

A Diretora de *Compliance* e de Gestão de Risco organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de *compliance* (conforme descrito abaixo).

7.9 Revisão e Atualização

Esta Política de Segurança da Informação e Segurança Cibernética deverá ser revisada e atualizada, caso necerráio, **anualmente**, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatórias e/ou complementações.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

8. Política de Anticorrupção

8.1 Introdução e Abrangência das Normas de Anticorrupção

A GESTORA está sujeita às normas e leis de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e ao Decreto nº 8.420/15 ("Normas de Anticorrupção"), as quais estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados "agentes públicos" para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a GESTORA e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

8.2 Definição

Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo

Brasil, assim definidos:

✓ Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

✓ Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

✓ Comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

✓ No tocante a licitações e contratos:

o frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

o impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

o afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

o fraudar licitação pública ou contrato dela decorrente;

o criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

o obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

o manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

✓ Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

8.3 <u>Normas de Conduta</u>

É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização

prévia da Diretora de *Compliance* e de Gestão de Risco.

Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou Colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

8.4 Proibição de Doações Eleitorais

A GESTORA não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, a GESTORA e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

8.5 Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, a GESTORA será representada por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a GESTORA contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a GESTORA deverão elaborar relatórios de tais Audiências, e os apresentar à Diretora de *Compliance* e de Gestão de Risco imediatamente após sua ocorrência.

9. Política de Certificação

9.1 Introdução

A GESTORA aderiu e está sujeita às disposições do Código ANBIMA de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

Tendo em vista a atuação preponderante da Gestora como gestora de recursos de terceiros, a Gestora identificou, segundo o Código de Certificação, que a Certificação de Gestores ANBIMA ("CGA") e a Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE") são as certificações descritas no Código de Certificação pertinente às suas atividades, aplicáveis aos profissionais com alçada/poder

discricionário de investimento, nos termos do Art. 27 do Código de Certificação.

Nesse sentido, a Gestora definiu que apenas o Colaborador com alçada/poder discricionário de investimento (compra e venda) de posições sem aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e ou à CGE, a depender do investimento gerido, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em fundos de investimento de renda fixa, ações, cambiais, multimercados e fundos de índice e a CGE é aplicável aos profissionais que atuam em Fundos Imobiliários, Fundos de Investimento em Direitos Creditórios e Fundos de Índice.

Em complemento, a Gestora destaca que a CGA e a CGE são certificações de cunho pessoais e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pela Diretora de *Compliance* e de Gestão de Risco, sendo certo que caso o Colaborador esteja exercendo a atividade elegível de CGA ou CGE na Gestora, conforme acima indicada e a certificação não esteja vencida a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com a Gestora e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA ou CGE na Gestora, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível de CGA ou CGE, conforme o caso.

Desse modo, a Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos no Código ANBIMA de Certificação.

9.2 <u>Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA</u>

A Área de *Compliance* e Controles Internos mantém controle dos Colaboradores da GESTORA com as seguintes informações:

- ✓ Dados profissionais;
- ✓ Data de admissão;
- ✓ Data de desligamento, quando aplicável;
- ✓ Atividade exercida;
- ✓ Área de atuação;
- ✓ Cargo;
- ✓ Tipo de gestor, quando aplicável;
- ✓ Endereço eletrônico individual;
- ✓ Se dispõe de certificação ANBIMA e a sua validade.

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a equipe de Compliance, Risco e PLD deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como identificar se o Colaborador recém contratado possui alguma certificação ANBIMA, ainda que não exerça qualquer atividade elegível, uma vez que, em caso positivo, a Gestora deverá inserir o Colaborador no Banco de Dados da Gestora.

O Diretor de Gestão deverá esclarecer à equipe de Compliance, Risco e PLD se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de investimento ou se atuarão na distribuição dos fundos de investimento sob gestão da Gestora junto aos investidores, conforme o caso.

Caso seja identificada a necessidade de certificação, a equipe de Compliance, Risco e PLD deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

A equipe de Compliance, Risco e PLD também deverá checar se os Colaboradores que estejam se desligando da Gestora estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Gestora, sendo, para estes, obrigatória a inclusão do desligamento no Banco de Dados da Anbima. A referida inclusão será facultativa para estagiários e terceiros contratados, salvo se as informações tiverem sido incluídas pela Gestora no Banco de Dados da Anbima.

A equipe de Compliance, Risco e PLD deve incluir no Banco de Dados as informações cadastrais de todos os Colaboradores que tenham qualquer certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização.

Todas as atualizações obrigatórias no Banco de Dados da ANBIMA devem ocorrer **até o último dia útil do mês subsequente à data do evento** que deu causa a atualização, nos termos do Art. 12, §1º, inciso I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela equipe de Compliance, Risco e PLD, conforme disposto abaixo.

9.3 Rotina de Verificação

Mensalmente, a Diretora de *Compliance* e de Gestão de Risco verificará as informações contidas no Banco de Dados da ANBIMA, a fim de assegurar que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código ANBIMA de Certificação.

Ainda, o Diretor de Gestão deverá contatar a equipe de Compliance, Risco e PLD a fim de informá-los,

prontamente, caso haja algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso, bem como se houve algum tipo de alteração nos cargos e funções dos Colaboradores que atuem na atividade de distribuição diretamente junto aos investidores.

Colaboradores que não tenham CGA ou CGE (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Art. 16 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Gestora sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela equipe de Compliance, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Gestão por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, a Diretora de *Compliance* e de Gestão de Risco deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretora, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, **anualmente**, deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

Por fim, serão objeto do treinamento **anual** de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Gestora, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos, reforçando que somente os Colaboradores com CGA e CGE podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Gestora, devendo os demais buscar aprovação junto ao Diretor de Gestão; e (iii) treinamento direcionado aos Colaboradores da equipe de Compliance e Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

9.4 Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do art. 9º, §1ª, inciso V, do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se

certifiquem, devendo para tanto assinar a documentação prevista no **Anexo I** a este Manual denominado "Termo de Afastamento", comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do **Anexo I** aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas ao Comitê de *Compliance*, Controles Internos, Ética e Risco, que deve monitorar a regularização.

Quaisquer outras situações identificadas aplicáveis à matéria devem ser objeto de análise, aprovação, formalização ou eventual assunção de risco no âmbito do Comitê de *Compliance*, Controles Internos, Ética e Risco.

10. Política de Treinamento Contínuo

A Política de Treinamento contínuo tem como objetivo estabelecer as regras que orientam o treinamento dos Colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas políticas e manuais internos da GESTORA. Todos os Colaboradores receberam o devido treinamento acerca de todas as políticas e procedimentos. Assim, serão proporcionados aos Colaboradores uma visão geral das políticas e manuais internos da GESTORA, de forma que os mesmos se tornem aptos a exercerem suas funções aplicando conjuntamente todas as normas neles dispostas.

Ainda, com o intuito de promover o constante aperfeiçoamento dos Colaboradores e a melhoria constante das funções dos Colaboradores, cursos de atualização que sejam relacionados às atividades desenvolvidas são incentivados e poderão ser parcialmente patrocinados pela GESTORA.

Poderão ser ministradas a todos os Colaboradores da GESTORA palestras internas, a fim de dar ciência sobre (i) as políticas adotadas pela GESTORA; (ii) a regulamentação vigente e aplicável aos negócios da GESTORA e, ainda, (iii) eventuais fragilidades detectadas, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela GESTORA. Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do Colaborador em lista de presença. Não sendo possível a participação do Colaborador, sua ausência deverá ser justificada à Diretora de *Compliance* e de Gestão de Risco, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela GESTORA, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da GESTORA, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Os treinamentos relacionados ao conteúdo das políticas e manuais internos da GESTORA serão realizados, com periodicidade mínima anual, pela Diretora de *Compliance* e de Gestão de Risco sendo obrigatórios a todos os Colaboradores e controlados por lista de presença. Quando do ingresso de um novo Colaborador, a Diretora de *Compliance* e de Gestão de Risco aplicará o devido treinamento de forma individual para o novo Colaborador.

A Diretora de *Compliance* e de Gestão de Risco poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas e manuais internos da GESTORA, bem como com relação à regulamentação aplicável em vigor às atividades desenvolvidas pela GESTORA.

11. Vigência e Atualização

Este Manual será revisado **anualmente**, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	**Versão**	**Responsáveis**
Fevereiro de 2022	1ª Versão e Atual	Diretora de *Compliance* e de Gestão de Risco

Anexo I
TERMO DE RECEBIMENTO E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, DECLARO para os devidos fins:

✓ Ter recebido, na presente data, o Manual de Regras, Procedimentos e Controles Internos atualizado ("Manual") da INTRABANK Asset Management Ltda. ("GESTORA");

✓ Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;

✓ Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da GESTORA, incorporando-se às demais regras internas adotadas pela GESTORA; e

✓ Estar ciente do meu compromisso de comunicar à Diretora de *Compliance* e de Gestão de Risco da GESTORA qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

[*local*], [*data*].

_____

[**COLABORADOR**]

Anexo II
TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, doravante denominado Colaborador, e INTRABANK Asset Management Ltda., inscrita no CNPJ/ME sob o nº. 42.621.928/0001-33 ("GESTORA").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da GESTORA, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da GESTORA, incluindo:

a) *Know-how,* técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela GESTORA;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados,

mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[*local*], [*data*].

_____

[**COLABORADOR**]

INTRABANK ASSET MANAGEMENT LTDA.

Testemunhas:

1._____
Nome:
CPF/ME:

2._____
Nome:
CPF/ME:

ANEXO III
PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS
ATIVIDADES DA INTRABANK ASSET MANAGEMENT LTDA.

1. Instrução CVM Nº 50, de 31 de agosto de 2021;
2. Instrução CVM nº 472, de 31 de outubro de 2008;
3. Instrução da CVM nº 356, de 17 de dezembro de 2001;
4. Instrução CVM nº 555, de 17 de dezembro de 2014;
5. Resolução CVM nº 21;
6. Ofício-Circular/CVM/SIN/Nº 05/2014;
7. Código ANBIMA de Administração de Recursos de Terceiros;
8. Código ANBIMA de Certificação;
9. Código ANBIMA de Ética; e
10. Lei 9.613/98, conforme alterada.

Anexo IV
TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____ ("Colaborador"), DECLARO para os devidos fins:

✓ que a disponibilização pelo Colaborador à INTRABANK Asset Management Ltda. ("GESTORA"), nesta data, dos documentos contidos no *pen drive* da marca [•], número de série [•] ("Documentos"), bem como sua futura utilização pela GESTORA, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

✓ ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da GESTORA, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da GESTORA, exceto se aprovado expressamente pela GESTORA.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no *pen drive* da marca [•], número de série [•], que ficará com a GESTORA e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente Termo.

[*local*], [*data*].

_____

[**COLABORADOR**]

Apêndice
Lista dos Arquivos Gravados nos *Pen Drives*

Anexo V
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/ME sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de alçada/poder final de decisão de investimentos e/ou desinvestimentos dos fundos sob gestão da INTRABANK Asset Management Ltda., inscrita no CNPJ/ME sob o nº. 42.621.928/0001-33 ("GESTORA") por prazo indeterminado:

[ ] até que me certifique, conforme o caso, pela CGA ou pela CGE, no caso de atividade de gestão de recursos de terceiros com alçada/poder discricionário de investimento, a depender do tipo de fundo de investimento gerido; e

[ ] ou caso o Conselho de Certificação me conceda a isenção de obtenção da CGA ou da CGE.

[*local*], [*data*].

_____
[**COLABORADOR**]

_____
INTRABANK ASSET MANAGEMENT LTDA.

Testemunhas:

1._____
Nome:
CPF/ME:

2._____
Nome:
CPF/ME: