Manual de Controles Internos

(*Compliance*)

Clave Gestora de Recursos Ltda.

Clave Alternativos Gestora de Recursos Ltda.

Versão 1.4 – Abril/2024

ÍNDICE

1. INTRODUÇÃO E OBJETIVO

O termo *compliance* é originário do verbo, em inglês, *to comply*, e significa "estar em conformidade com regras, normas e procedimentos".

Visto isso, que a Clave Gestora de Recursos Ltda. e a Clave Alternativos Gestora de Recursos Ltda. (em conjunto, "Gestoras") adotaram em suas estruturas as atividades de "Controles Internos" ou "*Compliance*". O diretor responsável pelo *compliance* das Gestoras ("Diretor de *Compliance*") tem como objetivo garantir o cumprimento das leis e regulamentos emanados de autoridades competentes aplicáveis às atividades de gestora, bem como as políticas e manuais das Gestoras, e obrigações de fidúcia e lealdade devidas aos fundos de investimento e demais clientes cujas carteiras de títulos e valores mobiliários sejam geridas pelas Gestoras ("Clientes"), prevenindo a ocorrência de violações, detectando as violações que ocorram e punindo ou corrigindo quaisquer de tais descumprimentos.

Este Manual de Controles Internos *(Compliance)* ("Manual de *Compliance*") foi elaborado para atender especificamente às atividades desempenhadas pelas Gestoras, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de *Compliance* é aplicável a todos os sócios, diretores, funcionários, empregados, estagiários e demais colaboradores das Gestoras (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

Este Manual de *Compliance* deve ser lido em conjunto com o Código de Ética e Conduta das Gestoras, que também contém regras que visam a atender aos objetivos aqui descritos.

Este Manual de *Compliance* está de acordo com o Código ANBIMA de Administração de Recursos de Terceiros, bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM").

2. GOVERNANÇA

2.1. *Designação de um Diretor Responsável*

A Área de *Compliance* das gestoras será liderada pelo Diretor de *Compliance*, Sr. Otávio Mendonça Barros, devidamente nomeado no contrato social de cada uma das Gestoras. Nos termos do art. 25 da Resolução da CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21"), o Diretor de *Compliance* é o diretor responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos pelas Gestoras e da referida Instrução.

O Diretor de *Compliance* exerce suas funções com plena independência e não atua em funções que possam afetar sua isenção, dentro ou fora das Gestoras. Da mesma forma, a Área de *Compliance* não está sujeita a qualquer ingerência por parte das equipes de gestão e possui autonomia para questionar os riscos assumidos nas operações realizadas pelas Gestoras.

Portanto, deve ser garantido à Área de *Compliance* amplo acesso às informações e documentos relacionados às atividades das Gestoras, de modo que possa verificar continuamente a conformidade com a legislação e as regras internas.

O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance*. Caso o mesmo tenha que se ausentar por um longo período de tempo, o Comitê de *Compliance* deverá designar um substituto ou um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada, caberá ao CEO das Gestoras fazê-lo.

O Diretor de *Compliance* tem como principais atribuições e responsabilidades:

(i) o suporte a todas as áreas das Gestoras no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades das Gestoras com as normas regulamentares (internas e externas) em vigor; e

(ii) a definição, junto ao Comitê de *Compliance*, dos planos de ação, seguida do monitoramento do cumprimento dos prazos e do nível de excelência

dos trabalhos efetuados, assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

São também atribuições do Diretor de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

(i) Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

(ii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética e Conduta", submetendo o caso à análise do Comitê de *Compliance* sempre que necessário, assim como avaliar as demais situações que não foram previstas em todas as políticas internas e manuais das Gestoras ("Políticas Internas");

(iii) Reconhecer situações novas no cotidiano da administração interna ou nos negócios das Gestoras que não foram planejadas, fazendo a análise de tais situações;

(iv) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pelas Gestoras;

(v) Verificar anualmente a adequação dos investimentos pessoais dos Colaboradores à Política de Investimentos Pessoais das Gestoras, mediante a coleta do Termo de Compromisso com a Política de Investimentos Pessoais e dos extratos de movimentações de todas as contas do Colaborador com capacidade de corretagem;

(vi) Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem das Gestoras, assim como das pessoas envolvidas no caso.

2.2. Comitê de *Compliance*

Trata-se do fórum de definição, revisão e avaliação da aderência às normas determinadas pelos órgãos de regulação e autorregulação e às normas de conduta e ética estabelecidas nas Políticas Internas das Gestoras.

O Comitê de *Compliance* é composto pelo Diretor de Risco e *Compliance*, o CEO e o Head de Operações das Gestoras.

As decisões tomadas serão formalizadas em ata ou e-mail encaminhado aos membros e participantes, de imediato.

Visando a mitigação de potenciais conflitos de interesses, não poderão votar os membros que se encontrem em posição de conflito de interesses em relação à matéria deliberada. Especificamente, os membros deste Comitê que representem alguma das áreas de Gestão não poderão votar caso a matéria em questão diga respeito diretamente a sua área de atuação, a si próprio ou a Colaboradores sob sua supervisão direta.

O Comitê de *Compliance* tem plena autonomia para executar as suas funções, detalhadas neste Manual. Sempre que julgar necessário, o Comitê poderá solicitar o apoio de consultores externos para a análise de suas questões.

Este Comitê se reúne no mínimo trimestralmente, podendo ser convocado extraordinariamente por qualquer de seus membros, sempre que julgue necessário, sendo instalado necessariamente com a presença do Diretor de *Compliance*, ou seu substituto, representando a área de *Compliance*.

Os assuntos tratados por este Comitê são estritamente confidenciais.

São atribuições do Comitê de *Compliance*, sem prejuízo de outras descritas nas Políticas Internas:

(i) Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

(ii) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

(iii) Definir, divulgar e revisar os procedimentos deste Manual, do Código de Ética e Conduta e demais Políticas Internas das Gestoras, bem como as estratégias para o desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

(iv) Apurar todas as denúncias e casos trazidos ao Comitê acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste

Manual de *Compliance*, ou no "Código de Ética e Conduta", assim como avaliar as demais situações que não foram previstas em todas as Políticas Internas, avaliando a necessidade de comunicação aos órgãos reguladores ou ao COAF;

(v) Fornecer orientação aos Colaboradores em casos de dúvidas quanto à aplicação das Políticas Internas que não puderem ser esclarecidas isoladamente pelo Diretor de *Compliance;*

(vi) Apurar situações e tomar determinadas decisões relativas a Controles Internos, Prevenção à Lavagem de Dinheiro e Não Financiamento do Terrorismo, Anticorrupção, Segurança da Informação Confidencial, Propriedade Intelectual e Continuidade do Negócio;

(vii) Deliberar acerca dos casos de caracterização de conflitos de interesse e solicitar a tomada das devidas providências;

(viii) Aprovar e revisar os controles e planos de ação propostos pelo Diretor de *Compliance;*

(ix) Analisar temas, iniciativas ou operações que possam representar risco reputacional às empresas, clientes ou funcionários;

(x) Avaliar, aprovar e monitorar terceiros a serem contratados em nome dos fundos de investimento sob gestão;

(xi) Aprovar, divulgar e revisar a Lista de Emissores de Ordens das Gestoras;

(xii) Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

(xiii) Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem das Gestoras, assim como das pessoas envolvidas no caso;

(xiv) Designar um substituto do Diretor de *Compliance*, ou um responsável temporário para cumprir suas funções, em caso de ausência prolongada do mesmo;

(xv) Definir e aplicar eventuais sanções aos Colaboradores.

3. PROCEDIMENTOS

3.1. *Revisão periódica e preparação de relatório*

O Diretor de *Compliance* deverá revisar pelo menos anualmente este Manual de *Compliance* para verificar a adequação das políticas e procedimentos aqui previstos e sua efetividade, submetendo tal revisão ao Comitê de *Compliance*. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as violações ocorridas no período anterior, e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pelas Gestoras.

O Diretor de *Compliance* deve encaminhar ao Comitê de *Compliance*, até o último dia do mês de janeiro de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las, que deverá seguir o formato previsto no Anexo I.

O relatório referido no parágrafo acima deverá ficar disponível para a CVM na sede das Gestoras.

3.2. *Treinamento*

As Gestoras possuem um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre as Políticas Internas, inclusive este Manual de *Compliance*, aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

O Diretor de *Compliance* deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *compliance*.

A periodicidade mínima do processo de reciclagem continuada será anual. A cada processo de reciclagem continuada, os Colaboradores assinarão termo comprovando a participação no respectivo processo.

O Diretor de *Compliance* poderá ainda promover treinamentos extraordinários sempre que houver alteração nas normas que regulam as atividades das Gestoras, ou ainda, visando tratar de casos concretos ocorridos dentro ou fora da instituição.

Os materiais, carga horária e grade horária serão definidos pelo Diretor de *Compliance*, que poderá, inclusive, contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

3.3. *Apresentação do Manual de Compliance e suas modificações*

O Diretor de *Compliance* deverá entregar uma cópia deste Manual de *Compliance*, e das Políticas Internas, para todos os Colaboradores por ocasião do início das atividades destes nas Gestoras, e sempre que estes documentos forem modificados. Mediante o recebimento deste Manual de *Compliance*, o Colaborador deverá confirmar que leu, entendeu e cumpre com os termos deste Manual de *Compliance* e das Políticas Internas, mediante assinatura do termo de adesão, até o último dia do mês subsequente ao ingresso, que deverá seguir o formato previsto no Anexo II ("Termo de Adesão").

3.4. *Atividades Externas*

Os Colaboradores devem obter a aprovação escrita do Diretor de *Compliance* antes de envolverem-se em negócios externos às Gestoras. "Atividades Externas" incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome das Gestoras ou não). Os Colaboradores que desejam ingressar ou engajar-se em tais Atividades Externas devem obter a aprovação prévia por escrito do Diretor de *Compliance*", que submeterá o caso à análise do Comitê de *Compliance* sempre que necessário, por meio da "Solicitação para Desempenho de Atividade Externa" na forma do Anexo III.

Não será necessária a prévia autorização do Diretor de *Compliance* para Atividades Externas relacionadas à caridade, organizações sem fins lucrativos, clubes ou associações civis.

3.5. *Supervisão e responsabilidades*

Todas as matérias de violações a obrigações de *compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas ao Diretor de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *compliance*, e determinar, junto ao Comitê de *Compliance*, quais as sanções aplicáveis. O Comitê de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

As Gestoras utilizam sistema terceirizado de gestão de *Compliance*, que disponibiliza uma agenda de atividades regulatórias atualizada, controles internos e testes de aderência para cumprimento das normas de regulação e autorregulação aplicáveis às Gestoras. O sistema possui, ainda, uma biblioteca digital para armazenamento de documentos e registro de eventos pela Área de *Compliance*. Portanto, os registros e arquivamentos a cargo da Área de Compliance poderão ser realizados no referido sistema, a seu critério razoável. Todas as atividades, eventos e demais registros imputados no referido sistema possuem logs de registro para fins de auditoria e *backups* constantes.

3.6. *Sanções*

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de *Compliance* e/ou das Políticas Internas serão definidas pelo Comitê de *Compliance*, a seu critério razoável, e aplicadas pelo Diretor de *Compliance*, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente, sem prejuízo da aplicação de penalidades pela CVM e do direito das Gestoras de pleitearem indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

4. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Resolução CVM 21, especialmente o Artigo 27, III e Artigo 28, II, as Gestoras adotam procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador nas Gestoras é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

4.1. *Segurança da Informação Confidencial*

As Gestoras mantêm um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios de rede, planos de continuidade entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora das Gestora,s que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

O acesso às dependências físicas das respectivas áreas das Gestoras deve ser restrito aos Colaboradores que nela atuam, salvo áreas de uso comum como salas de reunião, copa, banheiros e recepção, nas quais não devem ser tratadas informações confidenciais sem o devido cuidado com o seu vazamento. O trânsito de visitantes será sempre realizado com o acompanhamento de Colaboradores e com os devidos cuidados, caso transitem próximos às áreas de gestão.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área das Gestoras, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento de qualquer Gestora, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Gestora na qual era empregado.

Qualquer informação sobre as Gestoras, ou de qualquer natureza relativa às atividades das Gestoras, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador nas Gestoras, só poderá

ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

Todos os Colaboradores, assim como todos os terceiros contratados pelas Gestoras, deverão assinar termo de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede das Gestoras e circulem em ambientes externos às Gestoras com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses das Gestoras e de seus Clientes. 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.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno das Gestoras.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, usando uma trituradora, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores estão proibidos de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios, sem autorização prévia das áreas de *Compliance* e tecnologia, especialmente quando não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade nas Gestoras.

É proibida a conexão de equipamentos, inclusive computador próprio, na rede das Gestoras que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

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

Os recursos disponíveis, tais como internet e serviço de e-mails, se destinam a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado, e nunca deve ser prioritário em relação a qualquer utilização profissional.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação das Gestoras.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome das Gestoras, ou utilizar material, marca e logotipos das Gestoras para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

As Gestoras respeitam a privacidade de todos os Colaboradores, porém se reservam ao direito de acessar e/ou bloquear, a seu exclusivo critério, os e-mails enviados e recebidos pelos Colaboradores, em razão de sua caracterização como ferramenta de trabalho, bem como de bloquear sites da internet inapropriados ou que, segundo os seus exclusivos critérios, ofendam a moral e os bons costumes. Todos os e-mails enviados e recebidos e toda a navegação realizada pelos Colaboradores na internet, poderão ser monitorados pelo Diretor de *Compliance* ou funcionários das áreas de tecnologia e *Compliance*, com autorização expressa do Comitê de *Compliance*.

O Diretor de *Compliance* também monitorará e será avisado por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Diretor de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática nas Gestoras. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença,

deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

As Gestoras se reservam ainda o direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pelas Gestoras para a atividade profissional de cada Colaborador. O Diretor de Compliance, sob supervisão do Comitê de Compliance, poderá monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente.

Todas as informações dos servidores das Gestoras, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área, sendo armazenadas com backup.

A rotina de backup contempla dois métodos em operação simultaneamente, garantindo a salvaguarda de todos os dados, sendo eles banco de dados, documentos, planilhas e diversos outros guardados na área de armazenamento dos servidores.

Em caso de divulgação indevida, ainda que involuntariamente, de qualquer informação confidencial, reservada ou privilegiada, o Diretor de *Compliance* apurará o responsável ou as causas que levaram a tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador, adotando os devidos procedimentos para que nova divulgação indevida não venha a acontecer.

Ainda, a depender da informação que foi revelada, o Comitê de *Compliance* se reunirá no menor espaço de tempo possível, de forma presencial ou eletrônica, para deliberar quais atitudes serão tomadas para a minimização de quaisquer danos que possam ocorrer diante da divulgação de determinada informação. Posteriormente, a decisão dos diretores e os motivos que levaram a tomar determinada ação serão registrados em ata e arquivados junto aos arquivos das Gestoras.

Além disso, o Comitê de *Compliance* avaliará a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; e (iii) consulta com advogado para avaliação dos riscos jurídicos e demais medidas cabíveis.

Serão realizados testes de segurança para os sistemas de informações utilizados pelas Gestoras, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

4.2. *Propriedade intelectual*

Todos os documentos desenvolvidos na realização das atividades das Gestoras ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são de propriedade intelectual das Gestoras.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual das Gestoras fora do escopo de atuação ou não destinado aos Clientes, dependerá de prévia e expressa autorização por escrito do Diretor de *Compliance*.

Uma vez rompido com as Gestoras o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

Todas as informações, documentos, cópias e extratos gerados nas atividades desempenhadas pelas Gestoras são de sua propriedade e deverão permanecer única e exclusivamente com as Gestoras. Exceto se deliberado de outra forma pelo Comitê de *Compliance*, os Colaboradores, no término de sua relação com as Gestoras, devolverão às Gestoras todos os originais e todas as cópias de quaisquer documentos recebidos ou adquiridos durante a relação mantida com as Gestoras, bem como todos os arquivos, correspondências e/ou outras comunicações recebidas, mantidas e/ou elaboradas durante a respectiva relação.

Caso o Colaborador, ao ser admitido, disponibilize às Gestoras documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão, códigos fonte ou ferramentas similares para fins de desempenho de sua atividade profissional junto às Gestoras, o Colaborador deverá assinar Termo de Propriedade Intelectual, 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 das Gestoras, sendo que o Integrante não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento das Gestoras, exceto se aprovado expressamente pelo Comitê de *Compliance*.

5. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um Cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios das Gestoras que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pelas Gestoras; *(b)* na decisão de Clientes de comprar, vender ou manter cotas de fundos de investimento administrados pelas Gestoras; e *(c)* na decisão dos Clientes de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pelas Gestoras.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso de o Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de *Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros das Gestoras, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao Diretor de *Compliance*.

O Diretor de *Compliance* submeterá ao Comitê de *Compliance* a suposta Informação Privilegiada a ele divulgada pelo Colaborador. Caso entenda que tal informação possa realmente ser classificada como privilegiada, o Comitê informará aos Colaboradores que estes estão proibidos de negociar ações ou quaisquer outros títulos de companhias cujos valores mobiliários possam ser afetados pela divulgação de tal Informação Privilegiada. No momento em que o Comitê de *Compliance* entenda que tal Informação Privilegiada não mais poderá afetar os valores das ações e/ou títulos das companhias em questão, ou a informação tenha se tornado pública, o Diretor de *Compliance* informará imediatamente a todos os Colaboradores que tais ações e/ou títulos estão liberados para negociação.

5.1. *Insider Trading e "Dicas"*

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo as próprias Gestoras e seus Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, das Gestoras ou de terceiros.

A prática de qualquer ato em violação deste Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Resolução CVM nº 44, de 23 de agosto de 2021 ("Resolução CVM 44").

É de responsabilidade do Diretor de *Compliance* verificar e processar periodicamente as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com as Gestoras, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

6. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

6.1. *Segregação física*

Caso as Gestoras venham a desenvolver atividades que apresentem conflito de interesses entre si, as áreas das Gestoras sujeitas ao conflito serão fisicamente segregadas, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas, para garantir que não exista circulação de informações que possam gerar conflito de interesses ("*chinese wall*").

Não será permitida a circulação de Colaboradores em seções que não sejam destinadas ao respectivo Colaborador.

Reuniões com terceiros não Colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não Colaborador, inclusive Clientes, sendo este encaminhado diretamente à devida sala.

É de competência do Diretor de *Compliance*, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções. Caso o Diretor de *Compliance* constate que o Colaborador tenha tentado acesso às áreas restritas com frequência acima do comum ou necessária, ou ainda sem qualquer motivo aparente, poderá aplicar as devidas sanções. Eventual infração à regra estabelecida neste Manual de *Compliance* será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Diretor de *Compliance*.

A propósito, as tarefas contábeis das empresas serão terceirizadas, de modo que sejam exercidas no local de atuação das empresas contratadas.

6.2. *Segregação eletrônica*

Adicionalmente, as Gestoras segregarão operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores de áreas conflituosas, sendo que haverá impressora e fax individuais destinados exclusivamente à utilização de tais áreas separadamente.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado, sendo certo que tal restrição/segregação será feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, as redes de computadores das Gestoras permitirãoa criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

6.3. *Segregação em relação às demais empresas nas quais os sócios e/ou diretores da Gestoras tenham participação societária*

Os sócios e diretores das Gestoras poderão deter participações societárias em outros negócios (e.g. Investimentos Anjo / Venture Capital).

Nesse sentido, com o intuito de segregar a atividade de gestão de recursos e evitar qualquer compartilhamento de informação, as Gestoras determinam que os sócios com participação funcional nas Gestoras que possuam participação societária em outras empresas atuantes no mercado financeiro e de capitais não poderão ter atuação funcional em tais empresas, devendo figurar apenas como sócios de capital.

6.4. *Especificidades dos mecanismos de controles internos*

As Gestoras, por meio do Diretor de *Compliance*, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

(i) Definição de responsabilidades dentro das Gestoras;

(ii) Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos das empresas;

(iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

(iv) Contínua avaliação dos diversos riscos associados às atividades das empresas; e

(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos das Gestoras estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de *Compliance*.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e s*oftwares* sobre os quais as Gestoras possuam licença de uso, acesso à *internet*, bem como materiais e suporte necessário, com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios das Gestoras. A esse respeito, o Diretor de *Compliance* poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro das Gestoras.

Serão realizados testes de segurança para os sistemas de informações utilizados pelas Gestoras, em periodicidade, no mínimo, anual, para garantir a

efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

7. DIVULGAÇÃO DE MATERIAL DE *MARKETING*

Todos os Colaboradores devem ter ciência de que a divulgação de materiais de *marketing* deve ser realizada estritamente de acordo com as regras emitidas pela CVM e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e que não devem conter qualquer informação falsa ou que possa levar o público a erro.

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas às Gestoras, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão, que ofereça qualquer serviço de consultoria ou gestão prestado pelas Gestoras, ou um produto de investimento das Gestoras no mercado de valores mobiliários (incluindo fundos geridos).

Quaisquer materiais de *marketing* devem ser previamente submetidos ao Diretor de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo sem limitação a Instrução CVM nº 400, de 29 de dezembro de 2003 ("Instrução CVM 400"), a Instrução CVM nº 476, de 16 de janeiro de 2009 ("Instrução CVM 476"), a Instrução CVM nº 555, de 17 de dezembro de 2014 ("Instrução CVM 555"), a Instrução CVM nº 578, de 30 de agosto de 2015, conforme alterada, o Código ANBIMA de Administração de Recursos de Terceiros, e diretrizes escritas emanadas da ANBIMA. O Diretor de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de *Compliance* é que qualquer material de *marketing* deve ser utilizado.

Abaixo encontra-se uma lista não exaustiva de regras aplicáveis a materiais de *marketing* de fundos de investimento.

Nos termos da Instrução CVM 555, qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

(i) ser consistente com o regulamento e com a lâmina, se houver;

(ii) ser elaborado em linguagem serena e moderada, advertindo seus leitores para os riscos do investimento;

(iii) ser identificado como material de divulgação;

(iv) mencionar a existência da lâmina, se houver, e do regulamento, bem como os endereços na rede mundial de computadores nos quais tais documentos podem ser obtidos;

(v) ser apresentado em conjunto com a lâmina, se houver;

(vi) conter as informações do item 12 do Anexo 42 da Instrução CVM 555, se a divulgação da lâmina não for obrigatória;

(vii) conter informações: (a) verdadeiras, completas, consistentes e não induzir o Cliente a erro; (b) escritas em linguagem simples, clara, objetiva e concisa; e (c) úteis à avaliação do investimento; e (d) que não assegurem ou sugiram a existência de garantia de resultados futuros ou não isenção de risco para o Cliente.

Informações factuais devem vir acompanhadas da indicação de suas fontes e ser diferenciadas de interpretações, opiniões, projeções e estimativas.

Qualquer divulgação de informação sobre os resultados de fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses, a partir da data da primeira emissão de cotas.

Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente:

(i) mencionar a data do início de seu funcionamento;

(ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e a rentabilidade acumulada nos últimos 12 (doze) meses, não sendo obrigatória, neste caso, a discriminação mês a mês, ou no período decorrido desde a sua constituição, se inferior, observado que a divulgação de rentabilidade deve ser acompanhada de comparação, no mesmo período, com índice de mercado compatível com a política de investimento do fundo, se houver;

(iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde a sua constituição, se mais recente;

(iv) divulgar a taxa de administração e a taxa de performance, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e

(v) destacar o público alvo do fundo e as restrições quanto à captação, de forma a ressaltar eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de investidores em geral.

Caso o administrador contrate os serviços de empresa de classificação de risco, deve apresentar, em todo o material de divulgação, o grau mais recente conferido ao fundo, bem como a indicação de como obter maiores informações sobre a avaliação efetuada.

Ficam incorporadas por referência, ainda, as disposições do Capítulo VI do Código ANBIMA de Administração de Recursos de Terceiros, bem como das "Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento" da ANBIMA, disponíveis publicamente no *website* desta instituição.

8. APROVAÇÃO DE CORRETORAS E *SOFT DOLLAR*

As Gestoras apresentam Política específica de Seleção e Aprovação de Corretoras.

A Clave possui um processo robusto de avaliação de corretoras, por meio do qual persegue sempre a melhor relação custo-benefício na contratação de serviços de intermediação de operações.

A equipe de *compliance* manterá uma Lista de Corretoras Pré-Aprovadas ("Lista de Corretoras Aprovadas" ou "Lista") com base nos critérios estabelecidos pelas Gestoras. Caso aprovada pelo Comitê de Seleção de Corretoras, a Corretora passará a integrar a Lista de Corretoras Aprovadas. A Área de Gestão executará ordens para os Fundos exclusivamente com as corretoras incluídas na Lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Comitê de Seleção de Corretoras atualizará a Lista de Corretoras Aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

Os custos de transação mais relevantes tais como corretagem, emolumentos e custódia, devem ser constantemente monitorados, com o objetivo de serem minimizados. Semestralmente, o Comitê de Seleção de Corretoras deve elaborar um *ranking* com critérios objetivos de corretoras levando em consideração qualidade do serviço e preço, visando encontrar a melhor equação e prezando o dever fiduciário que temos para com os nossos Investidores. A Gestora utilizará preferencialmente as corretoras melhores classificadas pertencentes à Lista.

Dentre as corretoras pertencentes à Lista de Corretoras Aprovadas, a Área de Gestão possui discricionariedade na escolha de qual corretora executará a ordem levando em consideração: (i) o custo financeiro; (ii) o ativo financeiro; (iii) o mercado de atuação; (iv) o volume financeiro a ser executado; e (v) a frequência de negociação com aquela corretora.

É vedada a solicitação da execução de ordens por intermédio de qualquer corretora não previamente aprovada no Comitê de Seleção de Corretoras ou, ainda, que se encontre suspensa ou tenha sido removida da Lista.

As equipes de Gestão e de *Compliance* devem rever o desempenho de cada corretora e considerar, entre outros aspectos: a qualidade das execuções fornecidas; o custo das execuções, acordos de *soft dollar* e potenciais conflitos de interesse.

Adicionalmente, são mantidos controles para monitorar e limitar a concentração de operações entre intermediários.

8.1. *Política de Soft Dollar*

Soft dollars podem ser definidos como quaisquer benefícios oferecidos por uma corretora a uma gestora que direcione ordens para a corretora, que podem incluir, sem limitação, *researches* e acesso a sistemas de informações de mercado como o *Bloomberg*.

Acordos de *soft dollar* poderão ser permitidos se cumprirem os seguintes requisitos:

i) Auxílio ao processo de decisão de investimento da Gestora;

ii) Benefícios revertidos, direta ou indiretamente, para os cotistas dos Fundos, em consonância com o art. 18, VI, da Resolução CVM 21;

iii) Ausência de qualquer tipo de conflito de interesse;

iv) Ausência de qualquer obrigação de as Gestoras negociarem, exclusivamente ou não, com as Corretoras que vierem a oferecer o benefício, ou qualquer outra forma de contrapartida, mesmo que seja não financeira;

v) Benefícios compatíveis com o valor pago em corretagens e outras despesas; e

vi) Aprovação pelo Diretor de Risco e *Compliance*.

A prática de *soft dollar* é aceita única e exclusivamente para as atividades diretamente relacionadas à gestão dos recursos dos Clientes e não deve criar nenhuma dependência ou concentração na execução das ordens impactando a tomada de decisão de investimentos das Gestoras.

É vedado o uso de *soft dollar* quando o benefício se reverter para as Gestoras, seja no todo ou em parte.

Quaisquer acordos envolvendo *soft dollars* devem ser previamente aprovados pelo Diretor de Risco e *Compliance*.

9. POLÍTICA DE *KNOW YOUR CLIENT* (KYC) E PREVENÇÃO À LAVAGEM DE DINHEIRO

O termo "lavagem de dinheiro" abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. As Gestoras e seus Colaboradores devem obedecer todas as regras de prevenção à lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613, de 03 de março de 1998, conforme alterada ("Lei 9.613/98"), e a Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM 50"), cujos principais termos estão refletidos neste Manual de *Compliance*.

O Diretor de *Compliance* será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro.

O Diretor de *Compliance* estabelecerá o devido treinamento dos Colaboradores das Gestoras – na forma deste Manual de *Compliance* – para que estes estejam aptos a reconhecer e a combater a lavagem de dinheiro, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

As Gestoras adotam os seguintes procedimentos permanentes de controle e vigilância, no limite de suas atribuições, visando minimizar o risco de ocorrência de lavagem de dinheiro nas diversas operações financeiras sob sua responsabilidade, a saber:

(i) Análise, pela área de *Compliance*, das movimentações financeiras que possam indicar a existência de crime, em razão de suas características, valores, formas de realização e instrumentos utilizados, ou que não apresentem fundamento econômico ou legal;

(ii) Evitar realizar qualquer operação comercial ou financeira por conta de terceiros, a não ser que seja transparente, justificada e sólida, além de viabilizada ou executada através de canais bancários;

(iii) Evitar operações com pessoas ou entidades que não possam comprovar a origem do dinheiro envolvido;

(iv) Evitar operações financeiras internacionais complexas, que envolvam muitas movimentações de dinheiro em países diferentes e/ou entre bancos diferentes;

(v) Avaliação das políticas e práticas de prevenção e combate à lavagem de dinheiro adotada por terceiros/parceiros das Gestoras;

(vi) Verificação da adequação ao perfil das Gestoras dos Clientes oriundos dos distribuidores de cotas de fundos de investimento cujas carteiras sejam geridas pelas Gestoras;

(vii) Registro e guarda das informações relativas às operações e serviços financeiros dos Clientes;

(viii) Comunicação ao Conselho de Controle de Atividades Financeiras ("COAF") e à CVM, no prazo legal, de propostas e/ou operações consideradas suspeitas ou atípicas, a menos que não seja objetivamente permitido fazê-lo;

(ix) Comunicação ao COAF e à CVM de operações em espécie, ou cujo montante atinja os patamares fixados pelos reguladores;

(x) Revisão periódica dos procedimentos e controles de prevenção e combate à lavagem de dinheiro e de controles internos;

(xi) Adoção de procedimento de especial atenção a PEP, conforme definido abaixo; e

(xii) Ter adequado conhecimento dos Colaboradores e fazê-los conhecer políticas e normativos aderentes aos órgãos reguladores.

As Gestoras adotam procedimentos que permitem o monitoramento das faixas de preços das cotas de fundos geridos distribuídas, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas, e se for o caso, comunicados aos órgãos competentes.

9.1. *Cadastro de clientes e atualização*

A Resolução CVM nº 50 determina aos sujeitos obrigados que mantenham procedimentos escritos para o cadastro dos seus Clientes como parte integrante do processo de "Know Your Client". Assim, caso o perfil de atuação das Gestoras seja alterado, de modo a que estas passem a atuar com a gestão

de carteiras e/ou distribuição de cotas de fundos por ela geridos, aplicar-se-á o procedimento previsto nesta seção, sendo que, neste caso, as Gestoras deverão manter as informações cadastrais dos seus clientes, observando o conteúdo mínimo disposto nos Anexos da Resolução CVM nº 50.

A critério exclusivo das Gestoras, nos casos em que entender necessário, poderão ser requeridas, adicionalmente à documentação e informações previstas acima, visitas *due diligence* na residência, local de trabalho ou instalações comerciais do Cliente.

Após a análise e verificação, pela área de *compliance*, dos documentos e informações fornecidos pelo Cliente, o Diretor de *Compliance* decidirá pela aprovação ou recusa do cadastro do Cliente. O fornecimento da totalidade dos documentos e informações solicitados não é garantia da aprovação do cadastro do Cliente, podendo as Gestoras recusarem o cadastramento de Clientes a seu exclusivo critério.

O cadastro de cada cliente ativo (assim entendido aquele que tenha efetuado movimentações ou apresente saldo no período de 24 (vinte e quatro) meses posteriores à última atualização), deve ser atualizado em intervalos não superiores a 24 (vinte e quatro) meses.

O processo de atualização deve ser evidenciado por meio de fichas cadastrais e/ou cartas assinadas pelos Clientes, *logs* de sistemas, gravações telefônicas, entre outros comprovantes de confirmação de dados. Nenhuma operação deve ser realizada para a carteira de Clientes cujo cadastro esteja incompleto.

Quaisquer dúvidas relativas a cadastro e suas atualizações devem ser submetidas ao Diretor de *Compliance*.

9.2. *Procedimentos relacionados às contrapartes*

As Gestoras são responsáveis por tomar todas as medidas necessárias, segundo a legislação e regulamentação aplicável, incluindo, mas não limitado a, Lei 9.613/98, Resolução CVM nº 50 e Ofício-Circular nº 5/2015/SIN/CVM, as regras de cadastro, *know your client* - KYC ("conheça seu cliente"), *know your employee* – KYE ("conheça seu funcionário") e *know your partner* – KYP ("conheça seu parceiro") presentes neste Manual de *Compliance* e as melhores práticas adotadas pelas entidades autorreguladoras do mercado, para estabelecer e documentar a verdadeira e completa identidade, situação

financeira e o histórico de cada contraparte nas operações realizadas pelos fundos de investimento.

Nesse sentido, além dos clientes de suas carteiras, as Gestoras buscam analisar e monitorar, para fins de cumprimento às normas de prevenção à lavagem de dinheiro, as contrapartes com quem venha negociar os ativos que pretende adquirir, visando uma eficaz prevenção de quaisquer atividades inidôneas em seus ativos sob gestão.

9.3. *Pessoas politicamente expostas*

Os procedimentos para a identificação e negociação com pessoas consideradas expostas politicamente ("PEP") são tratados na Resolução CVM nº 50 e na Lei nº 9.613/98, e alterações posteriores, e demais normas editadas pelo BACEN, Conselho Monetário Nacional e GAFI/FATF.

O Anexo A da Resolução CVM nº 50 define a PEP como aquela que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas e políticas relevantes, eletivas ou não-eletivas, no Brasil ou em outros países, territórios e dependências estrangeiros, pertencentes a outros países também, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

Incluem-se os ocupantes de cargo, emprego ou função pública relevante exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível, dirigentes de empresas públicas ou dirigentes de partidos políticos. Devem ser também identificados os familiares da PEP, seus parentes, na linha direta, até o segundo grau, assim como o cônjuge, companheiro e enteado (Anexo A da Resolução CVM nº 50).

A Circular do BACEN nº 3.461, de 24 de julho de 2009, e alterações posteriores, dispõe sobre os procedimentos a serem observados pelos agentes financeiros para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PEP, os quais devem ser estruturados de forma a possibilitar a caracterização de pessoas consideradas PEP e identificar a origem dos fundos envolvidos nas transações dos Clientes assim identificados.

Recomenda-se aos sujeitos obrigados a especial, reforçada e contínua atenção no exame e cumprimento das medidas preventivas, sobretudo no que se refere às relações jurídicas mantidas com PEP, nos seguintes termos:

(i) Supervisão de maneira mais rigorosa a relação de negócio mantido com PEP;

(ii) Dedicação de especial atenção a propostas de início de relacionamento e a operações executadas com PEP, inclusive as oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política;

(iii) Manutenção de regras, procedimentos e controles internos para identificação de Clientes que se tornaram após o início do relacionamento com a instituição ou que seja constatado que já eram PEP no início do relacionamento com a instituição e aplicar o mesmo tratamento dos itens acima; e

(iv) Manutenção de regras, procedimentos e controles internos para identificação da origem dos recursos envolvidos nas transações dos Clientes e dos beneficiários identificados como PEP.

Adicionalmente, recomenda-se a observação de outros fatores de risco, antes da aprovação de uma conta de PEP:

(i) Transparência da fonte do dinheiro e dos bens para assegurar que estes não resultaram de recursos do Estado;

(ii) Avaliação se a finalidade da conta e o nível de atividade proposto estão de acordo com o perfil financeiro geral da pessoa;

(iii) Cargo político atual ou anteriormente exercido e sua duração;

(iv) O nível de acesso da PEP a fundos estatais;

(v) Avaliação da transparência e da complexidade da estrutura e da posse da conta; e

(vi) O regime político e socioeconômico do país de origem, seu nível de corrupção e controle de drogas.

9.4. *Comunicações*

Se algum Colaborador perceber ou suspeitar da prática de atos relacionados à lavagem de dinheiro ou outras atividades ilegais por parte de qualquer Cliente, este deverá imediatamente reportar suas suspeitas ao Diretor de *Compliance*, que deverá, então, instituir investigações adicionais, para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão. Entre outras possibilidades, uma atividade pode ser considerada suspeita se:

(i) operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;

(ii) operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;

(iii) operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;

(iv) operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

(v) operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

(vi) operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);

(vii) operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

(viii) operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;

(ix) operações liquidadas em espécie, se e quando permitido;

(x) transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;

(xi) operações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do Cliente ou de seu representante;

(xii) depósitos ou transferências realizadas por terceiros, para a liquidação de operações de Cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;

(xiii) pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do Cliente;

(xiv) situações em que não seja possível manter atualizadas as informações cadastrais de seus Clientes;

(xv) situações e operações em que não seja possível identificar o beneficiário final; e

(xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas.

As Gestoras deverão dispensar especial atenção às operações em que participem as seguintes categorias de Clientes:

(i) clientes não-residentes, especialmente quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador;

(ii) clientes com grandes fortunas geridas por áreas de instituições financeiras voltadas para clientes com este perfil (*private banking*); e

(iii) pessoas politicamente expostas.

As Gestoras deverão analisar as operações em conjunto com outras operações conexas e que possam fazer parte de um mesmo grupo de operações ou guardar qualquer tipo de relação entre si.

Os Colaboradores não devem divulgar suas suspeitas ou descobertas em relação a qualquer atividade, para pessoas que não sejam o Diretor de *Compliance*. Qualquer contato entre as Gestoras e a autoridade relevante sobre atividades suspeitas deve ser feita somente pelo Diretor de *Compliance*. Os Colaboradores devem cooperar com o Diretor de *Compliance* durante a investigação de quaisquer atividades suspeitas.

As Gestoras devem manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que as Gestoras previnam qualquer danificação, falsificação, destruição ou alteração indevida dos livros e registros por meio de adoção de métodos necessários e prudentes.

Consideram-se operações relacionadas com terrorismo ou seu financiamento aquelas executadas por pessoas que praticam ou planejam praticar atos terroristas, que neles participam ou facilitam sua prática, bem como por entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas e as pessoas ou entidades que atuem sob seu comando.

10. ENVIO DE INFORMAÇÕES ÀS AUTORIDADES GOVERNAMENTAIS

As leis e regulamentações brasileiras exigem que o gestor de investimentos entregue informações periódicas e/ou informações eventuais relacionadas à sua atividade de gestão de ativos nos mercados de capitais do Brasil. Algumas destas informações serão apresentadas à CVM ou ANBIMA e outros serão apresentados às companhias em que os fundos de investimento (ou outro veículo de investimento) investem ou aos cotistas desses fundos de investimento.

Estas informações incluem, sem limitação, (i) as comunicações previstas na Resolução CVM 44, sobre posições detidas nas companhias que integram as carteiras dos veículos de investimento, nos termos ali especificados; (ii) atualização anual do formulário de referência, conforme exigido pelo artigo 17 da Resolução CVM 21, o qual contém, sem limitação, informações sobre os fundos geridos, valores sob gestão e tipos de investidores; (iii) revisão periódica de seus manuais, códigos e políticas, os quais devem ser disponibilizados no website da Gestora; e (iv) informações exigidas pela legislação e regulamentação que trata da prevenção à lavagem de dinheiro.

O Anexo IV contém uma lista não exaustiva das informações periódicas exigidas pela legislação e pela regulamentação da CVM e ANBIMA na data deste Manual de *Compliance*.

11. PROCEDIMENTOS OPERACIONAIS

As Gestoras atuam em conformidade com os padrões e valores éticos elevados, principalmente observando e respeitando as normas expedidas pelos órgãos reguladores e suas Políticas Internas. Na condução de suas operações, as Gestoras deverão:

(i) observar o princípio da probidade na condução de suas atividades;

(ii) prezar pela capacitação para o desempenho das atividades;

(iii) agir com diligência no cumprimento das ordens, observado o critério de divisão das ordens (quando for o caso);

(iv) obter e apresentar aos seus clientes informações necessárias para o cumprimento das ordens;

(v) adotar providências para evitar a realização de operações em situação de conflito de interesses, assegurando tratamento equitativo a seus clientes; e

(vi) manter, sempre, os documentos comprobatórios das operações disponíveis, tanto para os órgãos fiscalizadores, como para os investidores, pelos prazos legais.

11.1. *Registro de operações*

As operações serão registradas nos sistemas dos administradores fiduciários dos fundos de investimento cujas carteiras sejam geridas pelas Gestoras e no sistema das Gestoras com o intuito de controlar e conferir as carteiras disponibilizadas por estes administradores.

11.2. *Liquidação das Operações*

As operações serão liquidadas pelos próprios fundos de investimentos, obedecidos os critérios estabelecidos pelos administradores fiduciários e instituições financeiras onde as operações foram realizadas.

12. MANUTENÇÃO DE ARQUIVOS

Conforme determinação da Resolução CVM 21, todos os documentos e informações contidos na base de dados das Gestoras, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções, deverão ser mantidos, em meio físico ou eletrônico, por no mínimo 5 (cinco) anos, ou por prazo superior caso solicitado pela CVM. A área de *Compliance* informará as demais áreas sobre períodos de manutenção que excedam o prazo mencionado neste Manual.

Nos casos em que existam mais de 1 (um) tipo de registro, ou seja, naqueles em que são utilizadas mais de 1 forma de evidenciar informações, as Gestoras podem optar pela manutenção de apenas uma destas pelo prazo estabelecido neste Manual.

Nenhuma informação ou documento mantido na base de dados das Gestoras pode ser descartado permanentemente da base de dados sem a autorização prévia do Diretor de *Compliance*.

13. PLANO DE CONTINUIDADE DO NEGÓCIO

Na execução de suas atividades, as Gestoras estão sujeitas a riscos relacionados à ocorrência de eventos que possam comprometer, dificultar ou mesmo impedir a continuidade das operações das Gestoras, tais como catástrofes naturais, ataques cibernéticos, sabotagens, roubos, vandalismos e problemas estruturais.

Este plano de continuidade do negócio busca descrever os procedimentos, estratégias, ações e infraestrutura empregados pelas Gestoras para garantir a continuidade das suas atividades em situações de contingência.

O responsável pelo cumprimento do plano de continuidade do negócio e pela ativação do plano de contingência é o Diretor de *Compliance*.

13.1. Estrutura e procedimentos de contingência

As Gestoras garantirão a continuidade de suas operações no caso de um desastre ou qualquer outra interrupção drástica dos negócios.

Os servidores das Gestoras podem ser acessados de forma virtual via *cloud*, de forma que todas as informações podem ser acessadas remotamente de qualquer lugar com acesso à internet.

Em caso de emergência nas sedes das Gestoras que impossibilite o seu uso, os Colaboradores trabalharão remotamente, a partir de seu ambiente residencial ou lugar a ser definido na oportunidade pelos Diretores de *Compliance* e de Gestão.

Todos os colaboradores possuem uma cópia do plano de continuidade do negócio que descreve todas as ações a serem seguidas em caso de desastre.

13.2. Plano de contingência

O plano de contingência será acionado toda vez que, por qualquer motivo, o acesso às dependências das Gestoras fique inviabilizado.

Nesses casos, os Diretores de *Compliance* e de Gestão, de comum acordo, devem determinar a aplicação dos procedimentos de contingência, autorizando os Colaboradores a trabalharem remotamente, no ambiente residencial do Colaborador, ou em lugar a ser definido na oportunidade pelo

Comitê de *Compliance*, o qual possua conexão própria e segura. Os Colaboradores utilizarão os notebooks das Gestoras e terão acesso a todos os dados e informações necessárias por meio do servidor na nuvem, de modo a manterem o regular exercício de suas atividades.

Após a normalização do acesso às Gestoras, os Colaboradores deverão apresentar ao Diretor de *Compliance* relatório de atividades executadas durante o período de contingência.

13.3. Atualização do plano de continuidade do negócio

Os procedimentos, estratégias e ações constantes do plano de continuidade do negócio serão testados e validados, no mínimo, a cada 12 (doze) meses, ou em prazo inferior, se exigido pela regulamentação em vigor.

14. SEGURANÇA CIBERNÉTICA

As Gestoras adotam mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

As Gestoras contrataram, às suas próprias expensas, empresa terceirizada para suporte às atividades de tecnologia de informação, fornecendo a estrutura tecnológica necessária para a execução de seus objetos sociais, bem como para prestação de serviços relacionados à segurança cibernética.

O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é o Diretor de *Compliance*.

14.1. Avaliação dos riscos

No exercício das suas atividades, as Gestoras poderão estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

i) *Malwares*: softwares desenvolvidos para corromper computadores e redes:

   a. Vírus: software que causa danos à máquina, rede, outros softwares e bancos de dados;

   b. Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

   c. *Spyware*: software malicioso para coletar e monitorar o uso de informações; e

   d. *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

a. *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

b. *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e

e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

14.2. Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, as Gestoras adotam as seguintes medidas de prevenção e proteção:

i) Controle de acesso adequado aos ativos das Gestoras, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos das Gestoras;

ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis;

iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

iv) Rotinas de backup;

v) Criação de logs e trilhas de auditoria sempre que permitido pelos sistemas;

vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;

vii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais; e

viii) Restrição à instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

14.3. Monitoramento

As Gestoras possuem mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, as Gestoras mantêm inventários atualizados de hardware e software, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos às Gestoras, como computadores não autorizados ou softwares não licenciados.

Além disso, as Gestoras mantêm os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de backup são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, as Gestoras analisam regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

14.4. Plano de resposta

Caso seja identificado um potencial incidente relacionado à segurança cibernética, o Diretor de *Compliance* deverá ser imediatamente comunicado.

Num primeiro momento, o Diretor de *Compliance* se reunirá com os demais diretores das Gestoras para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes às Gestoras, serão tomadas, em conjunto com os assessores de tecnologia da informação das Gestoras, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações das Gestoras, serão observados os procedimentos previstos no plano de continuidade do negócio, descrito no item 12 acima.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos das Gestoras.

Qualquer suspeita de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais medidas serão tomadas, inclusive, a depender da gravidade do caso, convocar

extraordinariamente o Comitê de Compliance, os quais determinarão quais clientes ou investidores deverão ser notificados com relação à violação.

Caso haja qualquer situação ou evidência de que quaisquer dos Dados Pessoais tratados pelas Gestoras tenham sido expostos de alguma forma, e que isso acarrete risco relevante à privacidade dos titulares dos dados, as Gestoras tomarão todas as medidas necessárias à mitigação dos riscos e reparação da situação, incluindo a comunicação às autoridades competentes e aos Titulares. Por sua vez, na comunicação às autoridades deverá ser mencionada a descrição da natureza dos Dados Pessoais afetados, as informações sobre os Titulares envolvidos, a indicação das medidas de segurança de informação utilizadas para a proteção dos Dados Pessoais, os riscos relacionados ao incidente e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

14.5. Reciclagem e revisão

As Gestoras manterão o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

O Diretor de *Compliance*, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

***

ANEXO I - Modelo de Relatório Anual de *Compliance*

São Paulo, _____ de janeiro de _____.

Aos Diretores,

Ref.: Relatório Anual de *Compliance*

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos da a Clave Gestora de Recursos Ltda. e a Clave Alternativos Gestora de Recursos Ltda. (em conjunto, "Gestoras"), nos termos do Manual de Controles Internos *(compliance)* das Gestoras ("Manual de *Compliance*"), e do Artigo 25 da Resolução nº 21, de 25 de fevereiro de 2021, da Comissão de Valores Mobiliários ("Resolução CVM 21"), e na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de *Compliance* e da Resolução CVM 21 ("Diretor de *Compliance*"), informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20____.

Por favor, encontrem abaixo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de deficiências e cronogramas de saneamento; e (iii) minha manifestação, na qualidade de responsável por ajustar a exposição a risco das carteiras das Gestoras, assim como pelo efetivo cumprimento da "Política de Gestão de Riscos" das Gestoras, a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

I. Conclusão dos exames efetuados:

II. Recomendações e cronogramas de saneamento:

III. Manifestação sobre verificações anteriores:

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____

Otávio Mendonça Barros

Diretor de *Compliance* e Risco da Clave Gestora de Recursos Ltda. e da Clave Alternativos Gestora de Recursos Ltda.

ANEXO II - Termo de Adesão

Eu, ..., portador da Cédula de Identidade nº ..... e/ou Carteira de Trabalho e Previdência Social nº ..... série ....., declaro para os devidos fins que:

1. Estou ciente da existência do "Manual de Controles Internos *(compliance)*" ("Manual de *Compliance*") da a Clave Gestora de Recursos Ltda. e a Clave Alternativos Gestora de Recursos Ltda. (em conjunto, "Gestoras") e de todas as políticas internas das Gestoras, inclusive o "Código de Ética e Conduta", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" ("Políticas Internas"), que recebi, li e tenho em meu poder.

2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pelas Gestoras, e comprometo-me a comunicar, imediatamente, aos diretores das Gestoras qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.

3. Tenho ciência e comprometo-me a observar integralmente os termos da política de confidencialidade estabelecida no Manual de *Compliance* das Gestoras, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.

4. O não-cumprimento do Código de Ética e Conduta e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pelas Gestoras e/ou os respectivos sócios e diretores, oriundos do não-cumprimento do Manual de *Compliance* e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.

5. Participei do processo de integração e treinamento inicial das Gestoras, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Gestoras, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-

las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.

6. As normas estipuladas no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pelas Gestoras, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.

7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei as Gestoras a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual de *Compliance*, salvo conflitos decorrentes de participações em outras empresas, descritos na "Política de Investimento Pessoal", os quais tenho ciência que deverão ser especificados nos termos previstos no Manual de *Compliance*:

_____

_____

_____

_____

São Paulo, ... de ..... de 20..... .

_____

[DECLARANTE]

ANEXO III - Solicitação para Desempenho de Atividade Externa

1. Nome da instituição na qual será realizada a Atividade Externa / descrição da Atividade Externa:

_____
_____

2. Você terá uma posição de diretor ou administrador? [ ] sim [ ] não

3. Descreva suas responsabilidades decorrentes da Atividade Externa:

_____
_____

4. Tempo estimado que será requerido de você para desempenho da Atividade Externa (em bases anuais):

_____

5. Você ou qualquer parte relacionada irá receber qualquer remuneração ou contraprestação pela Atividade Externa: [ ] sim [ ] não

Se sim, descreva:_____

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da a Clave Gestora de Recursos Ltda. e a Clave Alternativos Gestora de Recursos Ltda. (em conjunto, "Gestoras"), e que não interfere com suas atividades nas Gestoras, não compete ou conflita com quaisquer interesses das Gestoras. O Colaborador declara e garante, ainda, que irá comunicar ao diretor de *compliance* das Gestoras quaisquer conflitos de interesses que possam surgir com relação à Atividade Externa acima descrita.

São Paulo, _____ de _____ de 20_____.

_____

[Colaborador]

Resposta do Diretor de *Compliance:*

[ ] Solicitação Aceita

[ ] Solicitação Negada

_____

Otávio Mendonça Barros

Diretor de *Compliance* da Clave Gestora de Recursos Ltda. e da Clave Alternativos Gestora de Recursos Ltda.

ANEXO IV - Informações Periódicas Exigidas pela Regulamentação[1]

INFORMAÇÕES	PRAZO	DESTINATÁRIO	FORMA DE ARQUIVAMENTO
Enviar à CVM o Anexo E da Resolução CVM 21 devidamente preenchido, contendo informações sobre os Veículos de Investimento sob gestão, profissionais, estrutura administrativa e operacional etc.	Até o dia 31 de março de cada ano, com base nas posições de 31 de dezembro do ano anterior	CVM	Internet (por meio do site da CVM)
O Diretor de *Compliance* deverá encaminhar relatório dos controles internos, regras e procedimentos estabelecidos neste Manual de *Compliance* (e.g. testes de segurança nos sistemas, medidas para manter as informações confidenciais, programas de treinamento).	Até 31 de janeiro de cada ano, com base nas informações do ano civil imediatamente anterior	Diretoria	Físico ou Eletrônico
Confirmar que as informações cadastrais continuam válidas.	Entre os dias 1º e 31 de maio de cada ano	CVM	Site da CVM
Informar sobre sua equipe de gestão de investimento, especialmente alterações sofridas.	Mensalmente	ANBIMA	Internet (através do banco de dados de ANBIMA)

INFORMAÇÕES	PRAZO	DESTINATÁRIO	FORMA DE ARQUIVAMENTO
Confirmar que os profissionais da equipe de gestão de investimento são certificadas pela ANBIMA e que as informações de NAV e valor das cotas dos fundos de investimento foram enviadas.	Até 31 de março, com base nas informações de 31 de dezembro do ano anterior	ANBIMA	Site da ANBIMA
Reportar ao COAF e CVM, se for o caso, a não ocorrência de propostas, transações ou operações passíveis de serem comunicadas nos termos da Lei 9.613/98, tendo por base o ano imediatamente anterior.	Até 31 de janeiro de cada ano, com base no ano imediatamente anterior	COAF	SISCOAF
Voto adotado nas assembleias de acionistas dos veículos de investimento.	5 dias subsequentes à assinatura	Administrador	Forma e horários previamente estabelecidos pelo Administrador
Em cada momento em que o conjunto de veículos de investimento gerenciado pelo mesmo gestor de investimento ultrapassar, para cima ou para baixo, os patamares de 5%, 10%, 15%, e assim sucessivamente, de qualquer classe de valores mobiliários emitidos por uma companhia listada.	Imediatamente após a ocorrência do evento	Companhia listada que emitiu os valores mobiliários	Carta ou qualquer outro modo definido pela administração do(s) fundo(s) de investimento

INFORMAÇÕES	PRAZO	DESTINATÁRIO	FORMA DE ARQUIVAMENTO
Suspeita de lavagem de dinheiro ou atividades de financiamento de terrorismo, conforme definido na Lei 9.613/98.	24 horas após a ocorrência do evento	COAF	SISCOAF
Registrar a versão mais completa e atualizada da Política de Voto junto à ANBIMA.	No momento da adesão e sempre que atualizada	ANBIMA	Via Sistema SSM da ANBIMA
Registrar a versão mais completa e atualizada do Manual de Gerenciamento de Liquidez junto à ANBIMA.	No momento da adesão e no prazo de 15 (quinze) dias sempre que houver atualização	ANBIMA	Via Sistema SSM da ANBIMA

[1] Esta lista de normativos é meramente indicativa e exemplificativa e não exime o Colaborador da necessidade de conhecer, e manter-se sempre atualizado, dos demais normativos inerentemente aplicáveis, direta ou indiretamente, aos serviços das Gestoras.

* * *