Política Institucional	
Área Gestora ***Compliance* e Gestão de Riscos**	Versão **02**
Assunto **Manual de Controles Internos (*Compliance*)**	Data de Publicação **24/06/2025**
Abrangência **Limitada à CapSigma Investment Partners Ltda.**	

MANUAL DE CONTROLES INTERNOS (*COMPLIANCE*)

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, a **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Gestora") adotou em sua estrutura as atividades de "Controles Internos" ou "*Compliance*". O diretor responsável pelo *compliance* ("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 da Gestora, e obrigações de fidúcia e lealdade devidas aos fundos de investimento e demais clientes cujas carteiras de títulos e valores mobiliários sejam geridas pela Gestora ("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 pela Gestora, 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 da Gestora (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

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

Este Manual de *Compliance* está de acordo com os códigos e políticas da ANBIMA, incluindo, mas não se limitando ao Código de Administração e Gestão de Recursos de Terceiros e suas Regras e Procedimentos bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM") e pela *Securities and Exchange Commission* dos Estados Unidos ("SEC").

2. PROCEDIMENTOS

2.1. *Designação de um Diretor Responsável*

A área de *compliance* da Gestora é liderada pelo Diretor de *Compliance*, devidamente nomeado no contrato social da Gestora.

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

O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance*, e caso tenha que se ausentar por um longo período de tempo, deverá ser substituído ou deverá designar um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada, caberá aos sócios da Gestora fazê-lo.

O Diretor de *Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Gestora no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Gestora com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível de excelência dos trabalhos efetuados e 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) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

(iii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética", assim como avaliar as demais situações que não foram previstas em todas as políticas internas da Gestora ("Políticas Internas");

(iv) Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

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

(vi) Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

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

(viii) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Gestora;

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

2.2. *Sistema de Gerenciamento de Compliance*

A Gestora utiliza um sistema de trade e compliance fornecido por um terceiro. O sistema adotado pela Gestora permite a parametrização e execução de rotinas de testes de compliance. O monitoramento de atualizações regulatórias e autorregulatórias, assim como o desenho e a operação dos controles internos, é realizado diretamente pela equipe de compliance. O sistema não possui biblioteca digital nem funcionalidade de armazenamento de documentos. Todos os documentos relevantes são armazenados com segurança no ambiente em nuvem da Gestora, com controles de acesso implementados e observância dos prazos de retenção conforme as exigências legais e regulatórias aplicáveis.

Além disso, todas as atividades, eventos e demais registros imputados no referido sistema possuem *logs* de registro para fins de auditoria e *backups* automáticos.

2.3. *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. 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 pela Gestora.

O Diretor de Compliance deverá elaborar, ao menos uma vez por ano, um Relatório de Revisão de Compliance, em conformidade com a Regra 206(4)-7 do *Investment Advisers Act* de 1940, com a Resolução CVM nº 21 de 25 de fevereiro de 2021 ("Resolução CVM 21") e com os princípios aplicáveis do Código da ANBIMA.

Esse relatório deverá incluir, entre outros assuntos relevantes:

(i) um sumário dos testes e verificações realizados para avaliar a efetividade do programa de compliance da Gestora;
(ii) as recomendações do Diretor de Compliance quanto a eventuais deficiências identificadas, bem como os respectivos prazos para sua correção; e
(iii) uma declaração emitida pelo Diretor de Compliance, na qualidade de responsável pelo monitoramento da exposição a riscos da Gestora e pela implementação efetiva da Política de Gestão de Riscos da Gestora, a respeito dos achados identificados e das medidas corretivas planejadas ou implementadas, conforme o cronograma de remediação estabelecido.

O Relatório de Revisão de Compliance deverá ser submetido ao Comitê Executivo e permanecer disponível para inspeção pelas autoridades regulatórias competentes. Toda a documentação que fundamenta as conclusões do relatório deverá ser mantida por, no mínimo, cinco (5) anos, em conformidade com a Regra 204-2 do Investment Advisers Act e com os requisitos regulatórios brasileiros.

2.4. *Treinamento*

A Gestora possui 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, e o Diretor de Compliance deverá manter todos os registros pelo prazo legalmente exigido.

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.

2.5. *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 na Gestora, 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 que deverá seguir o formato previsto no Anexo II ("Termo de Adesão").

2.6. *Atividades Externas*

Os Colaboradores devem obter a aprovação escrita do Diretor de *Compliance* antes de envolverem-se em negócios externos à Gestora. "Atividades Externas" incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome da Gestora 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* por meio da "Solicitação para Desempenho de Atividade Externa" na forma do Anexo II deste manual.

Não será necessária a prévia autorização do Diretor de *Compliance* para Atividades Externas relacionadas à caridade, organizações sem fins lucrativos, clubes ou associações civis, desde que não represente conflito de interesses com a Gestora e/ou com a função exercida pelo Colaborador na Gestora.

2.7. *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 quais as sanções aplicáveis.

2.8. *Sanções*

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de *Compliance* e/ou das Políticas Internas serão definidas e aplicadas pelo Diretor de *Compliance*, a seu critério razoável, 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 da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

3. POLÍTICA DE CONFIDENCIALIDADE, MNPI E TRATAMENTO DA INFORMAÇÃO

A Gestora adota procedimentos robustos para assegurar a proteção de informações confidenciais e de Informações Relevantes Não Públicas (Material Non-Public Information – MNPI), em conformidade com a Resolução CVM nº 21, o Código da ANBIMA, a Regra 204A-1 e a Regra 204-2 do Investment Advisers Act de 1940, bem como as orientações correlatas emitidas pela SEC.

Informações Relevantes Não Públicas (MNPI) referem-se a quaisquer informações ainda não divulgadas ao público e que um investidor razoável consideraria relevantes ao tomar uma decisão de investimento. Isso inclui, mas não se limita a, dados financeiros não públicos, decisões de investimento ainda não divulgadas, eventos societários relevantes ou informações confidenciais de clientes. O uso indevido ou a divulgação não autorizada de MNPI é estritamente proibido e poderá resultar em sanções disciplinares e consequências legais nos termos das legislações brasileiras e norte-americanas aplicáveis ao mercado de capitais.

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

3.1. *Segurança da Informação Confidencial e Proteção de MNPI*

3.1.1. Controle de Acesso e Princípios de Confidencialidade

A Gestora mantém 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 da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

A Gestora implementou "barreiras de informação" (também conhecidas como Chinese Walls) para restringir o acesso entre áreas que possam lidar com Informações Relevantes Não Públicas (MNPI) — como a equipe de investimentos — e aquelas responsáveis por relacionamento com clientes, compliance ou atividades de back-office.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da Gestora, 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. No diretório do SharePoint, as pastas às quais um usuário não possui acesso não são visíveis em sua interface, garantindo a confidencialidade e limitando a

exposição a informações. Em caso de desligamento da Gestora, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Gestora.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

3.1.2. Tratamento e Circulação de Informações Confidenciais

Todos os Colaboradores, assim como todos os terceiros contratados pela Gestora, deverão assinar documento 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 da Gestora que contenham Informação Confidencial e/ou MNPI e circulem em ambientes externos à Gestora 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 da Gestora 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 da Gestora.

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. de maneira a evitar sua recuperação.

3.1.3. Descarte Seguro e Procedimentos de Tratamento de Dados

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *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.

3.1.4. Uso de Recursos de TI e Política de Comunicação

A Gestora não permite o uso de serviços de nuvem pessoais, aplicativos de mensagens ou e-mails particulares para armazenar, transmitir ou discutir informações confidenciais.

É proibida a conexão de equipamentos na rede da Gestora 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.

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 da Gestora.

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

3.1.5. Monitoramento de Rede, Registros de Acesso e Supervisão

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 na Gestora. 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.

A Gestora se reserva no 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 pela Gestora para a atividade profissional de cada Colaborador.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor em nuvem da Gestora. Nesse servidor, as informações são segregadas por área, sendo armazenadas com backup. Os backups de todos os sistemas são criptografados, realizados diariamente e armazenados em infraestrutura de nuvem segura.

A rotina de backup garante 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 de qualquer informação confidencial, o Diretor de *Compliance* apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador. A Gestora manterá todos os registros digitais em conformidade com a Regra 204-2 da SEC, pelo prazo mínimo de cinco anos.

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

3.2. Propriedade intelectual e Divulgações Externas

Todos os modelos, relatórios, sistemas e metodologias desenvolvidos pelos Colaboradores durante seu período na Gestora permanecem como propriedade intelectual da empresa. Qualquer divulgação não autorizada ou uso externo é estritamente proibido e passível de sanções legais.

A utilização e divulgação de qualquer bem e informação confidencial/MNPI sujeito à propriedade intelectual da Gestora 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 a Gestora o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

3.3. Proteção de Dados e Privacidade

Em conformidade com a Lei brasileira nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e com o Regulamento S-P do Investment Advisers Act dos EUA, a Gestora adota medidas para assegurar a privacidade e a proteção de informações pessoais não públicas relacionadas a seus Clientes, Colaboradores, prestadores de serviços e demais partes interessadas.

Todos os dados pessoais são tratados exclusivamente para finalidades compatíveis com as atividades da Gestora e estão sujeitos a salvaguardas técnicas e administrativas adequadas. O acesso é restrito a profissionais autorizados e regulado por rígidos controles internos. Terceiros contratados pela Gestora que tenham acesso a dados pessoais estão contratualmente vinculados a obrigações equivalentes de proteção de dados.

Os titulares dos dados podem exercer seus direitos previstos na legislação aplicável, incluindo acesso, retificação e exclusão, mediante solicitação ao departamento de Compliance. Qualquer acesso não autorizado, perda ou suspeita de violação de informações pessoais deve ser imediatamente reportado ao Compliance e será tratado conforme os procedimentos de resposta a incidentes da Gestora.

4. POLÍTICA DE INSIDER TRADING

O uso indevido ou a divulgação não autorizada de Informações Relevantes Não Públicas (MNPI) é estritamente proibido tanto pela legislação dos Estados Unidos quanto pela legislação brasileira. Nos Estados Unidos, tal conduta é tratada principalmente pela Seção 10(b) e pela Regra 10b-5 do Securities Exchange Act de 1934, bem como pela Seção 204A do Investment Advisers Act de 1940, que exige que os assessores de investimentos registrados estabeleçam e implementem políticas escritas destinadas a prevenir o uso indevido de MNPI. No Brasil, o insider trading é regulado pela Lei nº 6.385/76, conforme alterada ("Lei do Mercado de Capitais"), e pela Resolução CVM nº 44.

Em conformidade com esses marcos regulatórios, a Gestora adota a presente Política de Negociação com Informação Privilegiada (Insider Trading Policy), com o objetivo de assegurar que seus Colaboradores atuem com integridade, mantenham a confidencialidade e cumpram suas obrigações fiduciárias ao lidarem com informações sensíveis.

O *insider trading* é definido como o ato de negociar valores mobiliários com base em MNPI, em violação a um dever de confidencialidade, confiança ou obrigação fiduciária. Considera-se informação relevante aquela que um investidor razoável entenderia como importante ao tomar uma decisão de investimento, e não pública quando ainda não tiver sido amplamente divulgada ao mercado. Essa conduta inclui tanto (i) o uso de MNPI em benefício próprio ou de terceiros (direta ou indiretamente); quanto (ii) a divulgação ou transmissão de MNPI a outras pessoas (prática conhecida como tipping), nas quais o destinatário possa razoavelmente utilizar a informação para negociar valores mobiliários ou disseminá-la ainda mais.

É proibido a qualquer Colaborador da Gestora praticar os atos mencionados anteriormente em benefício próprio, em benefício da própria Gestora ou de terceiros.

A prática de *insider trading* e *tipping* é vedada nos termos:

- Da Lei brasileira nº 6.385/76, que tipifica como crime o uso de informação relevante, ainda não divulgada, que deva permanecer em sigilo e seja capaz de proporcionar vantagem indevida mediante negociação de valores mobiliários; e

- Da legislação federal norte-americana de valores mobiliários, incluindo a Seção 10(b) do Securities Exchange Act de 1934, a Regra 10b-5, e a Seção 204A do Investment Advisers Act de 1940, que exigem que os assessores de investimentos adotem políticas voltadas à prevenção do uso indevido ou da divulgação indevida de MNPI.

Violações a essas disposições podem acarretar responsabilidade civil, administrativa e criminal, incluindo aplicação de multas, sanções regulatórias e penas de reclusão.

Cabe ao Diretor de Compliance verificar periodicamente e tratar as notificações recebidas sobre eventual uso de informação privilegiada por parte dos Colaboradores, bem como práticas de *insider trading* e *tipping*. Os casos envolvendo o uso de informação privilegiada, *insider trading* ou *tips* devem ser analisados não apenas durante a vigência do vínculo profissional do Colaborador com a Gestora, mas também após o encerramento da relação, sendo o ocorrido reportado às autoridades competentes, conforme o caso.

5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

5.1. *Segregação física*

Considerando que a Gestora atua exclusivamente na atividade de gestão de carteiras, sem exercer funções de administração fiduciária ou distribuição de fundos, não é exigida, pela regulamentação aplicável, a segregação física das áreas do escritório. Ainda assim, a Gestora mantém segregação funcional adequada, com responsabilidades claramente definidas e procedimentos internos destinados a mitigar potenciais conflitos de interesse.

O acesso às áreas operacionais do escritório é restrito a Colaboradores autorizados, de acordo com suas respectivas funções e responsabilidades. A circulação de terceiros, incluindo Clientes e prestadores de serviços, é permitida apenas mediante agendamento prévio e limitada a salas de reunião designadas, garantindo a confidencialidade das informações sensíveis.

O Diretor de Compliance é o responsável por supervisionar o cumprimento dos protocolos internos de acesso e segregação. Tentativas reiteradas ou injustificadas de acesso por Colaboradores a áreas restritas poderão resultar na aplicação de medidas disciplinares, conforme previsto neste Manual de Controles Internos.

Adicionalmente, as atividades contábeis da Gestora são terceirizadas, sendo realizadas nas dependências da empresa prestadora de serviços contratada, como uma camada adicional de independência e controle.

5.2. *Segregação eletrônica*

Adicionalmente, a Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone fixo 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 da área de administração de recursos e os demais Colaboradores, sendo que haverá impressora e fax destinados exclusivamente à utilização da área de administração de recursos.

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, a rede de computadores da Gestora permitirá a 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.

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

Os sócios e diretores da Gestora poderão deter participações societárias em outros negócios.

Nesse sentido, com o intuito de segregar a atividade de gestão de recursos e evitar qualquer compartilhamento de informação, a Gestora determina que os sócios que possuam participação societária em outras empresas atuantes no mercado financeiro e de capitais não poderão ter atuação funcional em tal empresa, devendo figurar apenas como sócios de capital. Além disso, tais Colaboradores devem comunicar essa participação ao Diretor de Compliance e mantê-lo atualizado sobre quaisquer alterações em seu status.

5.4. *Especificidades dos mecanismos de controles internos*

A Gestora, 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 da Gestora;

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

(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 da empresa; e

(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Gestora 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 identifique 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 *softwares* sobre os quais a Gestora possua 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 da Gestora. 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 da Gestora.

6. 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 SEC, 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 à Gestora, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão, que ofereça qualquer serviço de consultoria ou gestão prestado pela Gestora, ou um produto de investimento da Gestora no mercado de valores mobiliários (incluindo fundos geridos). Para fins de conformidade com as normas da SEC, materiais de marketing também incluem qualquer comunicação, direta ou indireta, realizada pela Gestora que ofereça serviços de assessoria de investimentos a pessoas dos Estados Unidos ou a investidores de fundos privados, incluindo comunicações por meio de sites, e-mails, mídias sociais, podcasts, webinars e apresentações.

Quaisquer materiais de marketing devem ser previamente submetidos ao Diretor de Compliance, que verificará sua conformidade com as diversas normas aplicáveis, incluindo, mas não se limitando à Regra de Marketing da SEC[1], às resoluções da CVM e ao Código da ANBIMA. O Diretor de Compliance poderá, sempre que necessário, contar com o apoio de assessores externos para avaliar a aderência a essas normas. Somente mediante aprovação prévia e por escrito do Diretor de Compliance é que qualquer material de marketing poderá ser utilizado.

Como parte de seu programa de compliance, a Gestora implementou controles específicos para garantir que todos os materiais de marketing distribuídos a pessoas nos Estados Unidos ou relacionados a atividades de assessoria a investidores norte-americanos estejam integralmente alinhados à Regra de Marketing da SEC. Esses controles incluem um processo formal de revisão e aprovação prévia pelo Diretor de Compliance, que verifica a exatidão, consistência e completude de todas as declarações, com especial atenção às relacionadas a desempenho, retornos hipotéticos ou históricos de gestoras anteriores, bem como ao uso de depoimentos ou recomendações de terceiros. A Gestora mantém políticas e procedimentos documentados que sustentam o uso adequado desse tipo de conteúdo, assegurando que ele seja apropriado ao público-alvo e que não transmita uma impressão enganosa. Todo material que faz referência a desempenho passado é apresentado líquido de taxas, com os devidos *disclaimers* e informações contextuais, a fim de evitar apresentação seletiva ou desequilibrada. Adicionalmente, qualquer menção a classificações de terceiros ou declarações de Clientes é cuidadosamente analisada para garantir a transparência exigida, incluindo a divulgação de eventuais relações de remuneração, quando aplicável.

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

Nos termos da Resolução CVM de 23 de dezembro de 2022, conforme aditada ("Resolução CVM 175"), qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

[1] SEC, Regra 206(4)-1 do Investment Advisers Act de 1940, 17 C.F.R. § 275.206(4)-1

(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; e

(v) 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 VII das Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros, disponíveis publicamente no *website* da ANBIMA.

7. APROVAÇÃO DE CORRETORAS E POLÍTICA DE *SOFT DOLLAR*

A equipe de *compliance* manterá uma lista de corretoras aprovadas com base nos critérios estabelecidos pela Gestora. O *trader* executará ordens exclusivamente com corretoras constantes na referida lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Diretor de *Compliance* 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 time de gestão da Gestora 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.

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 dólar*, se aplicáveis, e potenciais conflitos de interesse.

7.1. *Política de Soft Dollar*

A Gestora não realiza quaisquer acordos de *soft dollar* e não autoriza o uso de comissões pagas pelos Clientes para obtenção ativa de pesquisas, dados de mercado ou quaisquer outros produtos ou serviços fornecidos por corretoras. Essa prática é categoricamente proibida pelas políticas internas da Gestora, sem exceções.

Soft dollars podem ser definidos como quaisquer benefícios oferecidos por uma corretora a um gestor que direciona ordens à referida corretora, os quais podem incluir, sem limitação, pesquisas e acesso a sistemas de informação de mercado, como o Bloomberg.

No entanto, no curso ordinário das negociações, a Gestora poderá ter acesso a pesquisas de terceiros ou a sistemas de dados de mercado fornecidos por corretoras por meio de estruturas de comissão agrupada (*bundled commission arrangements*). Esses benefícios são considerados permitidos sob a cláusula de *safe harbor* da Seção 28(e) do Securities Exchange Act dos Estados Unidos de 1934. Em todos os casos, a Gestora atua com boa-fé na busca pela melhor execução (*best execution*) e sempre no melhor interesse de seus Clientes.

Todas as decisões de investimento são tomadas em conformidade com o dever de melhor execução (*best execution*) da Gestora e com o objetivo exclusivo de atender aos melhores interesses de seus Clientes. Nenhum incentivo, benefício ou serviço recebido de corretoras influencia a independência ou objetividade do processo decisório da Gestora em matéria de investimentos.

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

8.1. Política de KYC

A Gestora mantém um Programa abrangente de Conheça seu Cliente (KYC) e Prevenção à Lavagem de Dinheiro (PLD), alinhado à legislação brasileira aplicável (Lei nº 9.613/98), à Resolução CVM nº 50 e ao Investment Advisers Act de 1940 dos Estados Unidos. O programa é baseado em risco e proporcional à atuação da Gestora como gestora de recursos, não englobando atividades de distribuição.

A Gestora não mantém relação comercial direta com os investidores dos fundos sob sua gestão coletiva. Nesses casos, apoia-se nos administradores e distribuidores formalmente contratados para a execução integral das obrigações de KYC e PLD, incluindo a identificação do beneficiário final (UBO), o monitoramento de transações e a verificação de listas de sanções. Esses terceiros estão sujeitos à devida diligência de Conheça seu Parceiro (KYP), conforme estabelecido na política de prestadores de serviços da Gestora.

- *Veículos não exclusivos*

Nos fundos não exclusivos, o papel da Gestora se limita à obtenção de documentação cadastral básica por meio dos distribuidores contratados, conforme exigido pela Resolução CVM nº 50.

Os administradores e distribuidores são contratualmente responsáveis por implementar políticas e controles internos adequados para:
(i) manter atualizados os registros dos investidores;
(ii) monitorar a consistência das transações e identificar potenciais indícios de lavagem de dinheiro ou financiamento ao terrorismo (LD/FT);
(iii) identificar e monitorar pessoas politicamente expostas (PEPs);
(iv) detectar estruturas de alto risco (como ações ao portador, trusts, private banking);

(v) avaliar a adequação das transações em função do perfil e da capacidade econômica declarada do investidor;
(vi) aplicar fatores de risco geográficos, econômicos e transacionais na classificação de risco dos investidores; e
(vii) reportar atividades suspeitas às autoridades competentes, conforme a regulamentação aplicável.

Nos fundos de investimento brasileiros, a Gestora realiza diligência KYP por meio de prestador de serviço terceirizado local, que assegura que todos os prestadores contratados adotem e cumpram tais padrões, dispondo de recursos tecnológicos e humanos adequados.

- *Relação direta*

A Gestora considera que há relação comercial direta nas seguintes situações:

(i) contas individualizadas (managed accounts) em que é contratada diretamente como consultora de investimentos;
(ii) veículos de investimento exclusivos nos quais interage diretamente com o investidor e não há envolvimento de distribuidor.

Nesses casos, a Gestora realiza integralmente os procedimentos de KYC e PLD, incluindo:

- Identificação e verificação do investidor e de seus beneficiários finais;
- Avaliação do perfil econômico do investidor, origem dos recursos e fatores de risco geográfico;
- Verificação de listas de sanções e de PEPs;
- Classificação baseada em risco e monitoramento contínuo da relação.

A Gestora está terminantemente proibida de prestar serviços de gestão de investimentos a qualquer indivíduo, entidade, embarcação ou jurisdição incluída na lista de Nacionais Especialmente Designados (Specially Designated Nationals – SDN) do OFAC ou sujeita a sanções impostas por qualquer autoridade regulatória ou governamental aplicável.

8.2. 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. A Gestora e seus Colaboradores devem obedecer a 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.

8.2.1. Controle de PLD no Ativo

A negociação de ativos e valores mobiliários em nome de fundos de investimento, veículos e contas administradas também deve estar sujeita à análise, avaliação e monitoramento sob a ótica de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT). A responsabilidade pela condução da devida diligência de PLD/FT no momento da aquisição dos ativos, bem como pelo monitoramento contínuo dessas posições, recai sobre as equipes de Gestão de Carteiras e de Investimentos, como primeira linha de defesa, e sobre o departamento de Compliance, como segunda linha de defesa.

As operações envolvendo valores mobiliários listados, operações de crédito privado e investimentos em *private equity*, se aplicável, deverão ser avaliadas com base em critérios de PLD/FT, considerando o perfil da empresa investida, incluindo seus acionistas, administradores, diretores, objeto social e racional da operação — sempre levando em conta os riscos inerentes de cada transação e os respectivos fatores mitigadores.

Adicionalmente, ao final de cada dia de negociação, o Gestor de Carteira realiza uma verificação manual das operações executadas, comparando os preços praticados com o preço médio de mercado ou o preço de fechamento fornecido pelo administrador do fundo, com o apoio da equipe de back office. Caso haja qualquer indício de que uma transação possa ter sido executada a um preço incompatível com as condições de mercado, o departamento de Compliance solicitará a documentação de suporte e as evidências necessárias para justificar o preço aplicado.

8.2.2. Supervisão Baseada em Risco

Como principal diretriz do seu programa de prevenção à lavagem de dinheiro e financiamento ao terrorismo, a Gestora adotou o método de supervisão baseado em risco, o que significa que a Gestora, no limite de suas atribuições, identificará, analisará, compreenderá e buscará mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo inerentes às suas atividades por meio da adoção de uma abordagem baseada em risco, para garantir que as medidas de prevenção sejam proporcionais aos riscos identificados.

A Gestora classificará todos os seus produtos oferecidos, serviços prestados, canais de distribuição, ambientes de negociação e clientes (isto é, os fundos de investimento geridos pela Gestora), segmentando-os minimamente em baixo, médio e alto risco. Para isso, serão levados em consideração, dente outros, os seguintes fatores:

(i) O tipo de fundo;

(ii) A sua atividade;
(iii) A localização geográfica dos ativos investidos pelo fundo;
(iv) As instituições intermediárias (distribuidoras) das cotas dos fundos;
(v) Os demais prestadores de serviços do fundo integrantes do segmento do mercado financeiro e de capitais; e
(vi) A contraparte das operações realizadas.

Além disso, a Gestora atuará de forma preventiva com base nos critérios acima listados para a análise prévia de novas tecnologias, serviços e produtos baseados no risco que eles poderão expor no futuro.

A Gestora adota procedimentos internos para a seleção e monitoramento de administradores, funcionários, e prestadores de serviços relevantes contratados. Para informações mais detalhadas, vide as políticas da Gestora aplicáveis.

A metodologia de supervisão baseada em risco da Gestora será analisada pelo Diretor de *Compliance* em seu relatório anual, de forma a considerar a efetividade dos controles internos, levando em consideração os seguintes critérios: **(i)** a implementação de um ambiente contínuo de conhecimento das operações dos fundos geridos pela Gestora e o monitoramento de suas operações; e **(ii)** A prevenção, detecção e combate a operações atípicas ou que possam configurar como lavagem de dinheiro ou financiamento ao terrorismo.

Caberá à alta administração da Gestora a aprovação da metodologia interna de supervisão baseada e risco, bem como o seu monitoramento e reavaliação através da análise do relatório anual.

Para fins desse Manual de *Compliance*, o Diretor de *Compliance* pode solicitar quaisquer documentos e/ou informações que sejam necessárias para o desempenho de suas atividades, devendo as fazê-lo de forma escrita, com prazo de resposta de até 15 (quinze) dias, podendo ser este prazo prorrogável quando for necessário, a critério do Diretor de *Compliance*.

Além da supervisão baseada em risco, A Gestora adota os seguintes procedimentos permanentes de controle e vigilância, 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 da Gestora;

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

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

(viii) Comunicação ao COAF e aos órgãos reguladores aplicáveis de operações em espécie, ou cujo montante atinja os patamares fixados pelos reguladores;

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

(x) Adoção de procedimento de especial atenção a PPE, conforme definido abaixo;

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

(xii) Aplicação de procedimentos de verificação das informações cadastrais proporcionais ao risco de utilização dos produtos, serviços e canais de distribuição para a lavagem de dinheiro e financiamento do terrorismo;

(xiii) Classificação dos fundos de investimento ativos geridos pela Gestora por grau de risco, classificando os, no mínimo, em baixo, médio e alto nível;

(xiv) Comunicação ao COAF de todas as situações e operações detectadas ou propostas de operações que possam constituir-se em sérios indício de lavagem de dinheiro ou financiamento ao terrorismo, assim como da inexistência de tais operações e/ou situações; e

(xv) Monitoramento e cumprimento das sanções impostas por resoluções do CSNU, imediatamente e sem aviso prévio aos destinatários, seguindo os procedimentos previstos no artigo 27 da Resolução CVM 50.

8.3. *Procedimentos relacionados às contrapartes*

A Gestora é responsável por tomar todas as medidas necessárias, segundo a legislação e regulamentação aplicável, incluindo, mas não limitado a, Lei 9.613/98, Resolução CVM 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, a Gestora busca 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.

8.4. *Pessoas politicamente expostas*

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

O Anexo B da Resolução CVM 50 dista aqueles indivíduos que são considerados PEP, sendo possível genericamente designá-los como aqueles que "desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, 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. Também se recomenda a fiscalização de familiares da PPE, seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro, enteados e colaboradores próximos.

A Circular do BACEN nº 3.978, de 23 de janeiro de 2020, 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 PPE, os quais devem ser estruturados de forma a possibilitar a

caracterização de pessoas consideradas PPE 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 PPE, nos seguintes termos:

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

(ii) Dedicação de especial atenção a propostas de início de relacionamento e a operações executadas com PPE, 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 PPE 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 PPE.

8.5. *Foreign Corrupt Practices Act (FCPA)*

A Gestora proíbe rigorosamente qualquer oferta, promessa, autorização ou pagamento, direto ou indireto, de dinheiro ou de qualquer coisa de valor a agentes públicos estrangeiros, figuras políticas ou entidades, com o objetivo de obter ou manter negócios, influenciar decisões ou garantir qualquer vantagem indevida. Essa proibição aplica-se a todos os Colaboradores e terceiros que atuem em nome da Gestora, independentemente do valor envolvido ou de costumes locais.

Para os fins desta Política, considera-se "Pessoa Abrangida" qualquer dirigente ou empregado de governo estrangeiro, órgão público, empresa estatal, banco central, fundo soberano, partido político ou qualquer candidato a cargo público fora dos Estados Unidos.

Qualquer prática desse tipo configura uma violação grave à legislação norte-americana, conforme previsto no *Foreign Corrupt Practices Act (FCPA)* de 1977, e poderá acarretar responsabilidade criminal. Não serão admitidas exceções sem análise prévia e aprovação expressa por escrito do Diretor de Compliance.

8.6. *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 PPE não possam ser concluídas; e

(xvii) todas as demais operações que possam configurar indícios de lavagem de dinheiro ou financiamento ao terrorismo mencionadas no artigo 20 da Resolução CVM 50 e na regulamentação aplicável;

A Gestora deverá 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.

A Gestora deverá 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 a Gestora 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.

A Gestora deve manter atualizados os livros e registros autênticos, exatos, completos e atualizados, incluindo documentos relacionados a todas as transações ocorridas nos

últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pelos órgãos reguladores, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que a Gestora previna 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.

8.7. Treinamento em Prevenção à Lavagem de Dinheiro (PLD)

O Diretor de Compliance deverá oferecer, ao menos a cada doze (12) meses, treinamento adequado a todos os Colaboradores sobre as regras de prevenção à lavagem de dinheiro estabelecidas nesta Política e na legislação e regulamentação aplicáveis. Tal treinamento é obrigatório para todos os Colaboradores, e a participação é registrada por meio de lista de presença. No processo de integração de um novo Colaborador, o departamento de Compliance deverá realizar treinamento individual sobre o tema.

9. 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 pela 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.

Da mesma forma, nos termos da regulamentação norte-americana, os assessores de investimentos registrados na SEC estão sujeitos a obrigações contínuas de reporte, divulgação e manutenção de registros, conforme previsto no *Investment Advisers Act* de 1940.

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

10. CONDUTA ÉTICA E PROCEDIMENTOS OPERACIONAIS

A Gestora atua em conformidade com elevados padrões éticos e valores institucionais, observando rigorosamente as normas emitidas pelos órgãos reguladores e suas Políticas Internas. No exercício de suas atividades, a Gestora compromete-se a:

(i) observar o princípio da probidade na condução de suas operações;
(ii) assegurar treinamento contínuo e adequado para o desempenho das atividades;
(iii) atuar com diligência na execução de ordens, observando critérios de rateio quando aplicável;
(iv) obter e apresentar aos clientes as informações necessárias para a adequada execução das ordens;
(v) adotar medidas para prevenir operações envolvendo conflitos de interesses, garantindo tratamento equitativo aos clientes; e
(vi) manter a documentação comprobatória das operações disponível para os órgãos de supervisão e para os investidores, conforme os prazos legais aplicáveis.

10.1. Registro das Operações de Investimento

Todas as operações de investimento são registradas nos sistemas dos administradores e custodiantes dos veículos sob gestão da Gestora. Paralelamente, a Gestora mantém um registro próprio e independente dos portfólios por meio de sistema terceirizado de controle de carteira, com o objetivo de conciliar e validar as informações disponibilizadas por tais prestadores de serviço. Esses registros seguem os parâmetros da Resolução CVM 175 e das regras da ANBIMA, sendo submetidos a reconciliações periódicas, auditorias e revisões internas de compliance.

10.2. Registro de Comunicações Eletrônicas Relacionadas às Operações

Em conformidade com a Regra 204-2(a)(7) e (a)(10) do Investment Advisers Act de 1940 e a regulamentação brasileira aplicável, a Gestora mantém registros de comunicações eletrônicas relacionadas a decisões de investimento, instruções de negociação, atividades de gestão de portfólio e quaisquer outras comunicações relevantes para a assessoria de investimentos.

O escopo de retenção inclui, mas não se limita a:

- E-mails enviados ou recebidos através do domínio corporativo;
- Mensagens via Bloomberg, quando aplicável;
- Comunicações internas e externas por plataformas de mensagens autorizadas;

- WhatsApp corporativo, desde que formalmente aprovado e arquivado;
- Notas de reuniões ou registros de chats com discussões sobre investimentos.

Para garantir a integridade e a disponibilidade dessas comunicações:

- Somente canais autorizados podem ser utilizados para fins operacionais ou de investimento;
- Todas as comunicações são arquivadas, indexadas e armazenadas em sistema seguro, com recursos de auditoria;
- O acesso é restrito por perfil de usuário e monitorado via logs de acesso;
- O prazo de retenção mínimo é de cinco (5) anos, conforme exigências da CVM e da SEC;
- É proibido, sob pena de sanção disciplinar, o uso de aplicativos de mensagens pessoais (e.g., WhatsApp pessoal, Telegram, e-mail privado) para comunicações profissionais.

10.3. Liquidação das Operações

A liquidação das operações de investimento é realizada diretamente pelos administradores fiduciários, custodiantes e instituições financeiras responsáveis pela execução das ordens, conforme os procedimentos operacionais e os ciclos de liquidação específicos de cada mercado em que os veículos investem.

A Gestora não exerce funções de custódia ou liquidação. No entanto, monitora ativamente o processo de liquidação por meio da reconciliação diária das ordens executadas, posições de portfólio e movimentações financeiras, utilizando seus próprios sistemas e serviços terceirizados. Qualquer divergência identificada entre os registros internos e os dos administradores ou custodiantes é imediatamente investigada e reportada às equipes de Compliance e Operações.

Todos os procedimentos de liquidação seguem os padrões estabelecidos nas jurisdições aplicáveis, incluindo, mas não se limitando a: Brasil, Estados Unidos, México, Chile, Colômbia e demais países da região. A Gestora também assegura que todas as contrapartes envolvidas na liquidação sejam devidamente autorizadas e reputadas.

10.4. Política de Rateio de Ordens

A Gestora mantém uma Política específica de Seleção e Rateio de Investimentos, autônoma, que estabelece os princípios, critérios e procedimentos para seleção, alocação e monitoramento dos ativos nos veículos sob sua gestão. Essa política visa assegurar tratamento justo e equitativo entre os diferentes clientes, prevenindo conflitos de interesse na gestão de múltiplos fundos ou contas com estratégias semelhantes.

Quando aplicável, as ordens são agregadas para ganho de eficiência na execução e redução de custos. A alocação dos ativos é realizada com base em critérios previamente estabelecidos, verificáveis e equitativos, assegurando que cada conta receba sua parte proporcional de acordo com o tamanho inicial da ordem e demais fatores relevantes. A Gestora não favorece qualquer cliente ou veículo em detrimento de outro e reforça seu dever fiduciário de atuar sempre no melhor interesse dos investidores.

Toda a documentação relacionada à agregação e alocação de ordens é mantida pela Gestora pelo prazo mínimo exigido pelas normas regulatórias aplicáveis e está disponível para consulta pelas autoridades competentes. O departamento de Compliance é responsável por monitorar o cumprimento desses procedimentos e realizar revisões periódicas conforme descrito na política correspondente.

11. PLANO DE CONTINUIDADE DO NEGÓCIO

Na execução de suas atividades, a Gestora está sujeita a riscos relacionados à ocorrência de eventos que possam comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, 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 pela Gestora 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*.

11.1. Estrutura e procedimentos de contingência

A Gestora garantirá a continuidade de suas operações no caso de um desastre ou qualquer outra interrupção drástica dos negócios.

Os servidores da Gestora 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 na sede da Gestora 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.

11.2. Plano de contingência

O plano de contingência será ativado em qualquer situação que comprometa de forma material a capacidade da Gestora de operar no curso normal de suas atividades, incluindo, mas não se limitando a: inacessibilidade física das instalações do escritório, incidentes de segurança cibernética, falhas generalizadas de infraestrutura (como interrupções de energia, internet ou telecomunicações), desastres naturais, pandemias, atos de terrorismo ou qualquer outra emergência ou crise que afete a disponibilidade de pessoal, sistemas ou serviços críticos prestados por terceiros. Este plano foi elaborado com o objetivo de assegurar a continuidade das operações essenciais, a proteção dos dados dos clientes e o cumprimento dos deveres fiduciários da Gestora, em conformidade com a regulamentação aplicável.

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 pelos Diretores de *Compliance* e de Gestão, o qual possua conexão própria e segura. Os Colaboradores utilizarão os notebooks da Gestora 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 à Gestora, os Colaboradores deverão apresentar ao Diretor de *Compliance* relatório de atividades executadas durante o período de contingência.

11.3. 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. O registro do teste será arquivado nas dependências da Gestora.

12. SEGURANÇA CIBERNÉTICA

A Gestora adota mecanismos de segurança cibernética para garantir a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados em suas operações. Esses mecanismos seguem os padrões estabelecidos na Regra 206(4)-7 do Investment Advisers Act de 1940, nas diretrizes da Lei Geral de Proteção de Dados brasileira ("LGPD") e no Guia de Cibersegurança da ANBIMA.

O Diretor de Compliance é responsável pela governança e supervisão do programa de segurança cibernética, em coordenação com o prestador de serviços externos de tecnologia da informação (TI) contratado pela Gestora. Esse prestador é responsável pela implementação, monitoramento e aprimoramento contínuo das salvaguardas técnicas e procedimentais, bem como por assegurar a conformidade com as regras e procedimentos de cibersegurança.

12.1. Avaliação dos riscos

No exercício das suas atividades, a Gestora poderá 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 pessoas 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 se 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.

A Gestora realiza periodicamente uma avaliação formal de riscos que inclui: (i) o mapeamento dos dados coletados e armazenados (como dados de investidores, colaboradores, clientes e parceiros); (ii) a classificação dos dados quanto à sensibilidade e

criticidade; (iii) a identificação dos ativos e sistemas tecnológicos utilizados; (iv) a análise de ameaças e vulnerabilidades cibernéticas internas e externas; (v) a verificação dos controles atualmente implementados e sua efetividade; (vi) os impactos operacionais e reputacionais potenciais; e (vii) a avaliação da estrutura de governança relacionada à gestão de riscos cibernéticos. Essa avaliação é atualizada ao menos anualmente ou sempre que houver alterações estruturais ou regulatórias relevantes.

12.1.1. Risco de Terceiros e Compartilhamento de Dados

Fornecedores e prestadores de serviço com acesso a dados sensíveis passam por processo de due diligence e devem assumir, contratualmente, o compromisso com padrões adequados de segurança cibernética, incluindo obrigação de notificação em caso de incidentes e conformidade com a LGPD. A Gestora assegura a revogação imediata dos acessos assim que houver o encerramento contratual.

12.2. 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, a Gestora adota as seguintes medidas de prevenção e proteção:

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

(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*).

12.2.1. Política de Uso de Dispositivos Pessoais (BYOD – Bring Your Own Device)

A configuração da conta de e-mail corporativo da Gestora em qualquer dispositivo pessoal (como celulares ou tablets) por parte do Colaborador está condicionada à instalação prévia de um aplicativo de segurança aprovado pela equipe de tecnologia. Esse aplicativo permite à Gestora realizar a limpeza remota de todos os dados corporativos armazenados no dispositivo em caso de roubo, perda ou extravio.

Além da funcionalidade de limpeza remota, o aplicativo monitora continuamente parâmetros específicos de segurança do dispositivo — como o nível de atualização do sistema operacional e o status da proteção por senha — podendo, caso os padrões mínimos de segurança não sejam atendidos, restringir automaticamente o acesso aos dados corporativos.

Os Colaboradores recebem instruções sobre boas práticas de segurança para dispositivos pessoais tanto durante o processo de integração (*onboarding*) quanto nos treinamentos anuais de compliance. Essas práticas incluem, entre outras, a instalação de software antivírus, o uso de redes privadas virtuais (VPN) e a ativação de autenticação multifator em todas as contas pessoais. A adesão a essas práticas é essencial para manter os padrões de segurança da informação da Gestora e mitigar riscos cibernéticos.

12.3. Monitoramento

A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Gestora mantém inventários atualizados de hardware e software, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou softwares não licenciados.

Além disso, a Gestora mantém 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, a Gestora analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

12.4. Plano de resposta a incidente

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 da Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação. O Diretor de Compliance poderá envolver o prestador de serviços de TI caso entenda necessário.

Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, 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 da Gestora, 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; e (iii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

O Diretor de Compliance será responsável pela elaboração de um relatório de incidente de segurança cibernética, o qual deverá incluir:

- Identificação e classificação do incidente;
- Medidas imediatas de contenção;
- Avaliação legal e contratual dos impactos e obrigações decorrentes;
- Ativação do Plano de Continuidade de Negócios, caso a integridade operacional tenha sido afetada;
- Análise da causa raiz e documentação do ocorrido;
- Revisão pós-incidente.

12.5. Treinamento e Conscientização

O treinamento em segurança cibernética é obrigatório para todos os Colaboradores no momento da admissão e, posteriormente, de forma anual. O conteúdo do treinamento abrange:

- Ameaças de engenharia social e *phishing*;
- Uso de senhas seguras e autenticação multifator;
- Manuseio seguro de dispositivos e informações sensíveis;
- Procedimentos para reporte de incidentes suspeitos;
- Responsabilidades previstas na política de cibersegurança.

Iniciativas adicionais de conscientização incluem:

- Campanhas simuladas de *phishing*.

12.6. Reciclagem e revisão

A Gestora manterá 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 resultados da avaliação de riscos, testes de invasão (*penetration tests*), registros de incidentes e atualizações regulatórias. A documentação das revisões, decisões e melhorias será devidamente arquivada.

***

ANEXO I
Termo de Adesão

Eu, _____, portador(a) da Cédula de Identidade nº _____, declaro para os devidos fins que:

1. Estou ciente da existência do "Manual de Controles Internos *(compliance)*" da **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Manual de *Compliance*" e "Gestora", respectivamente) e de todas as políticas internas da Gestora, inclusive o "Código de Ética", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" (conjuntamente com o Manual de Compliance, as "Políticas Internas"), que recebi, li e tenho em meu poder.

2. Tenho ciência do inteiro teor 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 pela Gestora, e comprometo-me a comunicar, imediatamente, aos diretores da Gestora 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 nas Políticas Internas da Gestora, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.

4. O não-cumprimento 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 pela Gestora 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 da Gestora, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Gestora, 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 nas Políticas Internas da Gestora não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pela Gestora, 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 a Gestora 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 II
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 **CAPSIGMA INVESTMENT PARTNERS LTDA.** ("Gestora"), e que não interfere com suas atividades na Gestora, não compete ou conflita com quaisquer interesses da Gestora. O Colaborador declara e garante, ainda, que irá comunicar ao diretor de *compliance* da Gestora 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

_____
Diretor de *Compliance*

ANEXO III - Informações Periódicas Exigidas pela Regulamentação

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 o último dia útil de abril de cada ano, com base nas informações do ano civil imediatamente anterior	*Comitê Executivo*	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)
Confirmar que os profissionais da equipe de gestão de investimento são certificados 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	Até o último dia útil de abril de cada ano, com base no ano imediatamente anterior	COAF	SISCOAF

Informações	**Prazo**	**Destinatário**	**Forma de Arquivamento**
9.613/98, tendo por base o ano imediatamente anterior.			
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
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
Revisão anual de Compliance	Anualmente até 31 de março	Comitê Executivo/Diretoria	Físico ou eletrônico
Formulário ADV	Anualmente até 31 de março	SEC	Via IARD
Formulário 13F - Reporte das posições em ações listadas nos EUA se o total superar US$ 100 milhões	Trimestral, até 45 dias após o fim do trimestre	SEC	Sistema EDGAR

Informações	**Prazo**	**Destinatário**	**Forma de Arquivamento**
Formulário 13D - Arquivamento obrigatório ao adquirir mais de 5% de ações com direito a voto de uma companhia aberta, com intenção de influenciar o controle	Até 10 dias após a aquisição	SEC	Sistema EDGAR
Formulário 13G - Alternativa passiva ao 13D para detenção de mais de 5% sem intenção de controle	Inicial, anual e conforme alterações	SEC	Sistema EDGAR
Formulário 13H - "Large Trader" – entidade que negocia ≥ 2 milhões de ações ou US$ 20 milhões em um dia, ou ≥ 20 milhões de ações ou US$ 200 milhões em um mês no mercado dos EUA	Inicial ao atingir o limite; Anualmente até 14 de fevereiro; atualizações conforme necessário	SEC	Sistema EDGAR

* * *

Controle de versão

Data	Versão	Aprovado por
28/03/2023	01	Diretor de Compliance