Política Institucional		
Área Gestora ***Compliance* e Gestão de Riscos**	Código	Versão **04**
Assunto **Manual de Controles Internos (*Compliance*)**	Data Criação **10/03/2025**	Data Publicação **10/03/2025**
Abrangência **Limitada à CPV CAPITAL GESTÃO DE RECURSOS 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 **CPV CAPITAL GESTÃO DE RECURSOS 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").

O presente documento 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 está de acordo com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA"), bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM").

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

O relatório referido no parágrafo acima deverá ficar disponível para a CVM na sede da Gestora.

2.3. 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.

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.

2.4. 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 previstono Anexo II ("Termo de Adesão").

2.5. 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 III.

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

2.6. 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. O Diretor de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

2.7. 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 E TRATAMENTO DA INFORMAÇÃO

Nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21"), a Gestora adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador 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

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.

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. 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*.

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 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, usando uma trituradora, de maneira a evitar sua recuperação.

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.

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente

autorizados 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.

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 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

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.

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.

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

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

A utilização e divulgação de qualquer bem 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.

4. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING

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

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

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

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

4.1. Insider Trading e "Dicas"

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

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada

como benefício para a compra e venda de títulos ou valores mobiliários.

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

A prática de qualquer ato em violação deste Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Resolução CVM nº 44, de 24 de agosto de 2021 ("Resolução CVM 44").

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

5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

5.1. Segregação física

A área de gestão de recursos da Gestora será fisicamente segregada das demais, sendo o acesso restrito aos Colaboradores integrantes da área, para garantir que não exista circulação de informações que possam gerar conflito de interesses ("*chinese wall*").

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

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

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

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

5.2. Segregação eletrônica

Adicionalmente, a Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores.

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.

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

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e *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.

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.

6. DIVULGAÇÃO DE MATERIAL DE *MARKETING*

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

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas 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).

Quaisquer materiais de *marketing* devem ser previamente submetidos ao Diretor de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo sem limitação o Código ANBIMA, e diretrizes escritas emanadas da ANBIMA. O Diretor de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de *Compliance* é que qualquer material de *marketing* deve ser utilizado.

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

Qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

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

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

(iii) ser identificado como material de divulgação;

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

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

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

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

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

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

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

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

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

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

(v) destacar o público-alvo do fundo e as restrições quanto à captação, de forma a ressaltar

eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de investidores em geral.

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

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

7. APROVAÇÃO DE CORRETORAS E *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 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. A Gestora somente utilizará as corretoras mais bem classificadas.

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

7.1. Política de Soft Dollar

Quaisquer acordos envolvendo *soft dollars* devem ser previamente aprovados pelo Diretor de *Compliance*. *Soft dollars* podem ser definidos como quaisquer benefícios oferecidos por uma corretora a uma gestora que direcione ordens para a corretora, que podem incluir, sem limitação, *researches* e acesso a sistemas de informações de mercado como o *Bloomberg*.

Acordos de *soft dollar* somente poderão ser aceitos pelo Diretor de *Compliance* se quaisquer benefícios oferecidos (i) possam ser utilizados diretamente para melhorias da tomada de decisão de investimento pela Gestora; (ii) sejam razoáveis em relação ao valor das comissões pagas; e (iii) não afetem a independência da Gestora.

A prática de *soft dollar* é aceita única e exclusivamente para as atividades diretamente

relacionadas à gestão dos recursos dos Clientes.

Os acordos de *soft dollars* não criam nenhuma obrigação para a Gestora operar exclusivamente junto às corretoras que concedem os benefícios.

Atualmente, a Gestora não possui qualquer acordo de *soft dollar.*

8. POLÍTICA DE *KNOW YOUR CLIENT* (KYC), CONHEÇA SEU EMPREGADO (KYE), CONHEÇA SEUS PRESTADORES DE SERVIÇO (KYSP) E PREVENÇÃO À LAVAGEM DE DINHEIRO

8.1. ASPECTOS PRELIMINARES

A CPV Capital Gestão de Recursos Ltda ("CPV" ou "Gestora", conforme aplicável), tem estrito compromisso para com a integridade do sistema financeiro, buscando prevenir quaisquer práticas que a firam. Nesse sentido, é tido como fundamental o respeito para com todas as leis, regulamentações, princípios e diretrizes relacionados à Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo ("PLDFT"). A presente política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo ("PLDFT"), vigente na CPV, compreende uma gama de atividades e procedimentos internos objetivando identificar a licitude dos negócios realizados pelos seus colaboradores, fornecedores e prestadores de serviços.

Por intermédio desta política a CPV – seus sócios, diretores, administradores e empregados ("Colaboradores") – torna-se aderente as normas legais, regulatórias e autorregulatórias aplicáveis, com destaque a Quarta Edição do Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, publicado em julho 2022, elaborado pela Associação Brasileira das Entidades de Mercado Financeiro e de Capitais(ANBIMA) ("Guia ANBIMA de PLDFT"), a Lei n.º 9.613/98, do Ofício Circular CVM/SMI-SIN 04/2020, da Resolução CVM Nº 50, De 31 de Agosto de 2021 e qualquer nova versão dos normativos acima mencionados, que venham a ser publicadas.

Para cumprimento de tais diretrizes, a CPV atuará em conjunto com os administradores fiduciários e distribuidores de fundos de investimento com os quais tiver relacionamento comercial, e buscará observar que tais entidades respeitam os padrões de ética e diligência a eles exigidos nas suas respetivas esferas de atuação.

8.2. GOVERNANÇA E RESPONSABILIDADE

O responsável pela implementação destes procedimentos de prevenção à lavagem de dinheiro e financiamento ao terrorismo é o Diretor de Compliance e Risco. O Diretor de Compliance

e Risco tem amplo, irrestrito e tempestivo acesso a qualquer informação relacionada à atuação da CPV, possibilitando, desta forma, que os dados necessários para o exercício de suas atribuições e dos demais colaboradores da área de compliance e risco, especialmente no que tange as práticas de PLDFT.

Nessa seara, o Diretor de Compliance e Risco é responsável por:

- Aprovar, em primeira instância, e revisar políticas, normas e procedimentos para PLDFT;
- Implementar e acompanhar o cumprimento desta Política e as medidas estabelecidas para coibir operações suspeitas; e
- Elaborar e encaminhar à Diretoria o relatório relativo à Avaliação Interna de Riscos de LDFT.

Ainda, é responsabilidade da Área de Compliance e Risco:

- Efetuar a análise e tratamento dos alertas de monitoramento relacionados à PLDFT;
- Submeter à apreciação da Diretora os alertas tratados e classificados como indícios de PLDFT;
- Avaliar de forma prévia, sob a ótica de PLDFT, os novos produtos ou serviços oferecidos pela CPV;
- Assegurar a realização de treinamento institucional relacionado à PLDFT; e
- Assegurar que os contratos com parceiros Custodiantes, Administradores e Prestadores de serviço possuam cláusulas específicas sobre as obrigações relacionadas à PLDFT.

Sem prejuízo, a diretoria da CPV, deverá:

- Aprovar as políticas, normas e procedimentos para o cumprimento do disposto na legislação vigente sobre crimes de Lavagem de Dinheiro e Financiamento ao Terrorismo (“LDFT”);
- Prover recursos para que todos os procedimentos e controles internos relacionados à PLDFT cumpram seus objetivos;
- Avaliar a adequação da avaliação interna de riscos;
- Designar, perante a CVM, uma diretora responsável por PLDFT
- Estar tempestivamente ciente dos riscos de conformidade relacionadas às práticas PLDFT;

• Assegurar que o Diretor de Compliance e Risco tenha independência, conhecimento técnico suficiente para pleno cumprimento dos seus deveres, assim como pleno acesso a todas as informações que julgar necessárias para que a respectiva governança PLDFT possa ser efetuada; e

• Assegurar a efetiva alocação dos recursos humanos e financeiros suficientes para cumprimento dos pontos anteriormente descritos.

8.3. POLÍTICA INSTITUCIONAL, MECANISMO E FERRAMENTAS DE PLDFT

A Lei de Lavagem de Dinheiro e a Resolução CVM Nº 50 impõem uma série de obrigações administrativas aos integrantes do mercado financeiro e de capitais com o objetivo de delegar a eles a realização de atividades e procedimentos fiscalizatórios que visem a identificação de processos de lavagem de dinheiro. Adicionalmente, o Guia PLD-FT da ANBIMA estabelece práticas sobre o tema a serem observadas no âmbito da autorregulação.

Para a CPV, trataremos das seguintes obrigações: (i) obrigações de identificação de cadastro de (a) contrapartes, (b) funcionários (Colaboradores), (c) fornecedores e (d) pessoas politicamente expostas; (iii) obrigações de monitoramento; e (iv) comunicação de operações com indícios de lavagem de dinheiro e de operações de comunicação obrigatória.

A seguir, serão descritas as obrigações que deverão ser observadas por completo por todos os Colaboradores, sob pena das responsabilizações previstas neste Código e nas normas legais, regulatórias e autorregulatórias aplicáveis.

8.3.1. IDENTIFICAÇÃO E CADASTRO DE CLIENTES

São considerados clientes da Gestora sujeitos a esta Política, os investidores, pessoas naturais ou jurídicas, com os quais a Gestora mantenha relacionamento comercial direto, assim entendidos, conforme aplicável: (i) os investidores de carteiras administradas sob gestão; e (ii) os eventuais cotistas de fundos ou veículos de investimento exclusivos e/ou restritos com os quais a Gestora tenha tido relacionamento prévio à estruturação dos referidos fundos e seja capaz de obter as informações descritas nesta Política (“Clientes Diretos”).

No curso de suas atividades junto aos Clientes Diretos, a Gestora deve observar as seguintes diretrizes:

- Sempre buscar identificar a identidade real de todos os seus clientes, por meio do procedimento KYC (Know your Client);
- Não receber recursos ou realizar atividades com clientes cujos fundos resultam de atividades criminosas;
- Não receber valores incompatíveis com a ocupação profissional e a situação financeira patrimonial declarada pelo cliente;
- Não aceitar investimentos e realizar operações com clientes que se recusem a fornecer as informações necessárias ao cadastramento ou à atualização do cadastro e/ou que não tenham sido aprovados segundo os processos de PLDFT aqui descritos; e
- Colaborar plenamente com as autoridades reguladoras, bem como informá-las de todas as ocorrências de atividades suspeitas identificadas, nos limites das leis e regulamentos aplicáveis.

8.3.2. CADASTRO E FISCALIZAÇÃO DO ATIVO (CONTRAPARTES)

Nas operações ativas (investimentos), o "cliente" deve ser entendido como o emissor do ativo adquirido e/ou a contraparte da operação, sendo a Gestora responsável pelo seu cadastro e monitoramento, se for o caso, devendo observar o quanto disposto no item a seguir, ressalvadas as exceções aqui previstas ("Contrapartes").

Neste contexto, para as carteiras sob gestão, dentro do princípio da razoabilidade e agindo com bom senso, a Gestora deverá se utilizar das seguintes práticas, conforme estabelecido no Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro divulgado pela ANBIMA:

8.3.2.1. Processo de Identificação de Contrapartes

A negociação de ativos financeiros para as carteiras sob gestão da Gestora deve, assim como os Clientes Diretos (passivo), ser igualmente objeto de análise, avaliação e monitoramento para fins

de prevenção e combate à lavagem de dinheiro. A Gestora deve estabelecer processo de identificação de Contraparte adequado às características e especificidades dos negócios. Tal processo visa a prevenir que a Contraparte utilize as carteiras sob gestão para atividades de LDFT.

Os ativos e valores mobiliários elencados a seguir, em função de sua Contraparte e do mercado nos quais são negociados, já passaram por processo de verificação, o que, em princípio, acabaria por eximir a Gestora de diligência adicional em relação ao controle da Contraparte, a saber: (a) ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM; (b) ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM; (c) ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida; (d) ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e (e) ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (i) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (ii) cuja existência tenha sido assegurada por terceiro devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

No entanto, a Gestora sempre diligenciará no processo de identificação da contraparte, caso seja possível tal diligência em razão das circunstâncias e características do ativo a ser investido.

Para os demais ativos e valores mobiliários, como títulos e valores mobiliários objeto de distribuição privada (renda fixa ou ações), direitos creditórios, empreendimentos imobiliários etc., é recomendável que a Gestora, além dos procedimentos de Identificação de Contrapartes, adote também outros procedimentos (como visita de diligência) e controles internos, ou verificar se a contraparte dispõe de mecanismos mínimos para análise para fins de prevenção e combate à lavagem de dinheiro.

8.3.3. FUNCIONÁRIOS (COLABORADORES)

A CPV possui processo "Conheça seu Colaborador" / "Know Your Employee" alinhada às práticas de Compliance da Instituição, buscando contratar colaboradores com perfis que condizem com as expectativas da empresa, principalmente em relação à Política de Ética Conduta e PLD/FT. Nesse sentido, é realizado processo de análise e avaliação detalhada de informações sobre cada candidato, em momento prévio à admissão.

A Instituição ainda oferece aos Colaboradores, constantemente, treinamentos obrigatórios, principalmente relacionados à Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo, com objetivo de manter seus colaboradores treinados e atualizados em relação aos dispositivos desta política.

8.3.3.1. Processo de Pré-Seleção

Durante o processo de contratação, os empregados devem obter informações qualitativas sobre o terceiro interessado em iniciar vínculos legítimos com a Gestora, a fim de permitir um melhor julgamento durante a pré-seleção ("Processo de Pré- seleção"). As informações a serem obtidas devem incluir:

(i) A data de início das atividades;

(ii) Qualificações dos principais sócios/executivos;

(iii) Lista de clientes (passados e atuais) e objeto da contratação;

(iv) Busca na rede mundial de computadores sobre notícias negativas sobre o terceiro; e

(v) Outras informações qualitativas que possam ser relevantes para melhor avaliar o terceiro.

O terceiro deverá estar legalmente constituído, gozar de boa reputação, ter capacidade econômica, financeira e técnica compatível com o objeto do contrato e com a assunção de

responsabilidades contratuais.

Serão solicitadas cópias do cartão de registro no CNPJ e documentos constitutivos e/ou corporativos relevantes ao terceiro. Se necessário, devem ser solicitadas cópias das demonstrações financeiras dos últimos 3 (três) anos e referências bancárias e técnicas do terceiro.

Além disso, os seguintes aspectos devem ser considerados durante o Processo de Pré- seleção:

(i) Estrutura da empresa;

(ii) Boa reputação (no caso de uma pessoa jurídica, a reputação dos sócios e dos principais executivos também deve ser considerada);

(iii) Nível de satisfação de outros clientes, passados e presentes;

(iv) Estrutura para atender o objeto da Contratação;

(v) Capacidade econômica e financeira;

(vi) Código de Ética e Conduta, ou similar;

(vii) Política Anticorrupção, ou similar;

(viii) Política de Combate à Lavagem de Dinheiro, ou similar;

(ix) Qualquer documento, procedimento e/ou formulário relacionado com a integridade e o cumprimento das regras; e

(x) Selo de Associado ou Aderente à ANBIMA, quando aplicável, ou, se não for o caso, as razões para não obter referido selo.

Após a revisão do procedimento de due diligence realizado, o empregado responsável pela contratação classificará o fornecedor de acordo com seu risco potencial, segundo o Anexo IV a este Manual de Compliance.

O início das atividades dos empregados estará vinculado à formalização do contrato, e nenhum pagamento poderá ser feito antes da celebração efetiva do contrato.

Os empregados responsáveis pelo processo de seleção de fornecedores manterão registros atualizados dos fornecedores, eliminando aqueles sobre os quais haja qualquer dúvida relativa a má conduta, comportamento antiético, comportamento ilícito ou que possam ter uma má reputação no mercado.

8.3.3.2. Não Aplicabilidade do Processo de Pré-Seleção

A Gestora poderá deixar de aplicar os procedimentos ora estabelecidos (ou parte deles), a seu critério exclusivo, quando o terceiro não estiver relacionado ao negócio principal do gestor de recursos e tiver uma clara capacidade econômica, financeira e/ou técnica para satisfazer o objeto da contratação e para cumprir suas responsabilidades e arranjos contratuais.

8.3.4. MONITORAMENTO DA ATIVIDADE REALIZADA POR TERCEIROS

O monitoramento das atividades realizadas por terceiros para a Gestora, assim como os próprios terceiros, é de responsabilidade da área que solicitou a contratação. O monitoramento deve ser contínuo durante a vigência da contratação, e o terceiro avaliado proporcionalmente ao serviço prestado, com ênfase em eventuais disparidades de tempo, qualidade e quantidade esperada.

Além disso, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a Gestora, e os respectivos relatórios devem ser enviados para a Equipe de Compliance.

8.3.4.1. GESTÃO DE CONTRATAÇÃO DE TERCEIROS

A Gestora somente selecionará prestadores de serviços terceirizados após a devida diligência e geralmente escolherá aqueles que são conhecidos e estabelecidos dentro de seus segmentos.

Ao contratar um prestador de serviço terceirizado com acesso a dados confidenciais, a Gestora incluirá cláusulas de confidencialidade no respectivo contrato de prestação de serviços.

8.3.4.2. FORNECEDORES / PRESTADORES DE SERVIÇO

A CPV realizará procedimentos de identificação e aceitação de prestadores de serviços e fornecedores para o estabelecimento de relações de parceria comercial. A avaliação prévia da CPV terá como objetivo prevenir a realização de negócios com parceiros inidôneos ou suspeitos de envolvimento em atividade ilícitas, bem como assegurar que tais parceiros também apresentem PLDFT consistentes e adequadas.

8.4. PESSOA POLITICAMENTE EXPOSTA – PPE

Para fins de controle de ilícitos de "lavagem de dinheiro" e financiamento ao terrorismo, a Gestora empreenderá esforços específicos na análise das operações com que possuam como contraparte uma pessoa considerada como politicamente expostas ("PPE"), nos termos definidos na regulamentação aplicável. Com efeito, a participação de PPE em qualquer operação no mercado financeiro é entendida como um ponto de alta sensibilidade pelas entidades de regulação e autorregulação dos mercados financeiro e de capitais.

Temos que a conduta do gestor de recursos deve ser pautada em um procedimento interno objetivo que tenha como escopo uma análise cautelosa e de gestão contínua de monitoramento de risco acerca: (i) das informações de cadastro da PPE; (ii) dos documentos pessoais da PPE, seus parentes, cônjuge, sócios e seus estreitos colaboradores; (iii) dos documentos sociais das empresas e dos veículos de investimento que a PEP tenha influência relevante; e (iv) dos contratos, termos e demais documentos relativos aos ativos que o gestor de recursos pretenda adquirir para a carteira do fundo.

Portanto, a Gestora realizará uma análise com base em seu procedimento interno, com a adicional atenção da peculiaridade da operação, em verificações que serão realizadas caso a caso.

Adicionalmente, no que cabe aos ativos e operações com participação de PPE, a Gestora deverá receber as informações acerca da relação da PPE com a eventual operação ou ativo específico e com as partes envolvidas na emissão, distribuição, comercialização e circulação do ativo. Nestes casos, os principais pontos de preocupação da análise serão focados nas empresas emissoras e garantidoras do ativo, seus sócios e demais partes relacionadas.

8.4.1. OBRIGAÇÕES DE MONITORAMENTO

A Gestora deve adotar procedimentos com vistas a controlar e monitorar a faixa de preços dos ativos negociados para as carteiras sob sua gestão, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas e, se for o caso, comunicadas aos órgãos competentes.

No intuito de identificar situações que possam levantar indícios de lavagem de dinheiro, as operações devem ser monitoradas observando:

• os preços dos ativos e valores mobiliários negociados, levando em consideração o seu grau de liquidez e organização do mercado específico em que são negociados;

• As contrapartes envolvidas, levando em consideração compatibilidade da operação com a sua situação patrimonial, e comportamento em relação ao volume, frequência e modalidade.

No caso de ativos que não possuam mercado ativo, o valor deve ser suportado por laudo de avaliação elaborado pela Gestora, por terceiro independente e especializado e/ou por quem o regulamento do respectivo fundo indicar.

Eventuais casos identificados como potencialmente suspeitos deverão ser levados para a análise do Diretor de Compliance e Risco para que este avalie a decisão e, se for o caso, comunicar à Unidade de Inteligência Financeira do Ministério da Economia.

8.4.2. EXCLUSÕES AO MONITORAMENTO

Em função da sua contraparte e do mercado no qual são negociados, os ativos e valores mobiliários abaixo já passaram por processo de PLDFT, de tal forma que não existe responsabilidade sob o gestor de recursos em realizar diligências adicionais em relação ao controle de contraparte:

- Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;
- Ofertas públicas de esforços restritos dispensadas de registro de acordo com as normas emitidas pela CVM;
- Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistemas de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;
- Ativos e valores mobiliários cuja contraparte seja instituição financeira ou comparada;
- Ativos e valores mobiliários de mesma natureza econômica daqueles listados acima, quando negociados no exterior, desde que: (a) sejam admitidos à negociação em bolsa de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

8.5. AVALIAÇÃO INTERNA DE 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 deverá classificar em baixo, médio e alto risco de LDFT, observada as métricas

abaixo descritas, todos os (i) produtos oferecidos; (ii) serviços prestados; (iii) respectivos ambientes de negociação e registro em que atue; e (iv) principais prestadores de serviços:

8.5.1. AVALIAÇÃO DOS PRODUTOS, SERVIÇOS, AMBIENTES DE NEGOCIAÇÃO E PRINCIPAIS PRESTADORES DE SERVIÇOS

Levando em conta os seguintes elementos:

- As atividades da Gestora são altamente reguladas e supervisionadas pela Comissão de Valores Mobiliários e pela ANBIMA; e
- Os fundos sob gestão contam com administradores fiduciários e distribuidores devidamente registrados e supervisionados pela CVM e ANBIMA.

A Gestora classifica como baixo o risco de LDFT associado aos produtos, serviços, ambientes de negociação e principais prestadores de serviços.

8.5.2. AVALIAÇÃO DOS CLIENTES DIRETOS

A classificação dos Clientes Diretos por grau de risco tem como objetivo destinar maior atenção aos Clientes Diretos que demonstrem maior probabilidade de apresentar envolvimento com LDFT.

Os Clientes são determinados pelos seguintes graus de risco:

- "Alto Risco" - Clientes Diretos que apresentem pelo menos uma das seguintes características:

(a) Reputação maculada: assim entendidos os acusados e condenados em processo administrativo sancionador por parte da CVM ou em processo de apuração de irregularidade por parte da ANBIMA nos últimos 3 (três) anos, considerados graves pelo Comitê de Risco e Compliance;

(b) Pessoa Politicamente Exposta bem como seus parentes até 1º grau, cônjuge ou

companheiro, sócios, estreitos colaboradores ou sociedades que possuam PPE em seu quadro de colaboradores e/ou societário;

(c) Clientes que se recusem a fornecer as informações necessárias ou apresentem informações cadastrais com consideráveis inconsistências, incluindo, mas não se limitando aos que recebem valores incompatíveis com a ocupação profissional e a situação financeira patrimonial declarada, bem como aqueles que realizam operações que evidenciem mudança repentina e injustificada relativamente às modalidades operacionais, volume ou frequência de negócios usualmente utilizados;

(d) Clientes que apresentem investimentos relevante em ativos ou participações como sócio ou administrador de empresa e outras estruturas de investimento constituídas ou com sede em jurisdição offshore que: (i) seja classificada por organismos internacionais, em especial o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo – GAFI, como não cooperante ou com deficiências estratégicas, em relação à prevenção e ao combate à lavagem de dinheiro e ao financiamento do terrorismo; (ii) faça parte de lista de sanções ou restrições emanadas pelo CSNU; e (iii) não possua órgão regulador do mercado de capitais, em especial, que tenha celebrado com a CVM acordo de cooperação mútua que permita o intercâmbio de informações financeiras de investidores, ou seja signatário do memorando multilateral de entendimento da Organização Internacional das Comissões de Valores – OICV/IOSCO; e

(e) organização sem fins lucrativos, nos termos da legislação específica.

Anualmente a Gestora realizará a atualização cadastral destes Clientes Diretos. A Equipe de Compliance destinará especial atenção para aqueles Clientes Diretos classificados como de Alto Risco, devendo monitorar continuamente e de maneira diferenciada a relação de negócio e as propostas de início de relacionamento.

- “Médio Risco” - Clientes Diretos que sejam:

(a) investidores com grandes fortunas geridas por área de instituições financeiras voltadas

para clientes com este perfil.

A cada 24 (vinte e quatro) meses a Gestora realizará a atualização cadastral destes Clientes Diretos.

- "Baixo Risco" - Clientes Diretos não listados acima.

A cada 36 (trinta e seis) meses a Gestora realizará a atualização cadastral destes Clientes Diretos.

A Gestora deverá realizar reavaliações na ocorrência de qualquer fato novo que possa alterar a classificação acima.

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.

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.

8.6. COMUNICAÇÃO AO ÓRGÃO REGULADOR

A Gestora deverá comunicar à Unidade de Inteligência Financeira do Ministério da Economia, no prazo de 24 (vinte e quatro) horas a contar da conclusão da análise que caracterizou a atipicidade da operação, respectiva proposta, ou mesmo situação atípica detectada, qualquer ato suspeito, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela a qual se refira a informação.

Cada reporte deverá ser trabalhado individualmente e fundamentado da maneira mais detalhada possível, sendo que dele deverão constar, sempre que aplicável, as seguintes informações:

- Data de início de relacionamento da Gestora com a pessoa autora ou envolvida na operação ou situação;
- A explicação fundamentada dos sinais de alerta identificados;
- A descrição e o detalhamento das características das operações realizadas;
- A apresentação das informações obtidas por meio das diligências previstas nesta Política, inclusive informando tratar-se, ou não, de PPE ou entidade sem fins lucrativos, e que detalhem o comportamento da entidade ou pessoa comunicada; e
- A conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada para a Unidade de Inteligência Financeira, contendo minimamente as informações definidas nos itens acima.

A Gestora e todos as pessoas físicas a ela vinculadas registradas junto à CVM, devem comunicar à CVM, anualmente, até o último dia útil do mês de abril, por meio dos mecanismos estabelecidos no convênio celebrado entre a CVM e a Unidade de Inteligência Financeira, a não ocorrência no ano civil anterior, de situações, operações ou propostas de operações passíveis de serem comunicadas (declaração negativa). Será de responsabilidade do Diretor de Compliance as comunicações relativas à Gestora descritas acima.

8.7. POLÍTICAS DE TREINAMENTO

A CPV fornecerá treinamento digital ou presencial de PLDFT abordando informações técnicas

dos fundos e as regras descritas neste documento.

O treinamento será realizado anualmente, sendo obrigatório a todos os Colaboradores e aos prestadores de serviço das áreas da CPV.

Após cada treinamento, será circulada lista de presença para controle dos presentes, sendo certo que as listas de presença permanecerão arquivadas pelo Diretor de Compliance e Risco da Gestora por, pelo menos, 5 (cinco) anos.

Quando do ingresso de um novo Colaborador, o Diretor de Compliance e Risco aplicará o devido treinamento previsto no Manual de Compliance, que inclui temas relacionados aos desta política.

8.8. CUMPRIMENTO DE SANÇÕES IMPOSTAS POR RESOLUÇÃO DO CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS

As corretoras e o administrador fiduciário deverão monitorar, direta e permanentemente, as determinações de indisponibilidade, bem como eventuais informações a serem observadas para o seu adequado atendimento, inclusive o eventual levantamento total ou parcial de tais determinações em relação ao cliente sancionado ou ativos, visando ao cumprimento imediato do quanto determinado, acompanhando para tanto, sem prejuízo da adoção de outras providências de monitoramento, as informações divulgadas na página do CSNU na rede mundial de computadores.

A CPV deverá, ainda:

- informar, sem demora, ao Ministério da Justiça e Segurança Pública (MJSP) e à CVM, a existência de pessoas e ativos sujeitos às determinações de indisponibilidade a que deixaram de dar o imediato cumprimento, justificando as razões para tanto;
- comunicar imediatamente a indisponibilidade de ativos e as tentativas de sua transferência relacionadas aos clientes diretos sancionados ao MJSP, à CVM e à Unidade de Inteligência Financeira;

- manter sob verificação a existência ou o surgimento, em seu âmbito, de ativos alcançados pelas determinações de indisponibilidade, para efeito de pôr tais ativos imediatamente, tão logo detectados, sob o regime de indisponibilidade; e
- proceder o imediato levantamento da indisponibilidade de ativos, na hipótese de exclusão dos clientes diretos eventualmente sancionados das listas do CSNU ou de seus comitês de sanções.

8.9. COMUNICAÇÕES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas; 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, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que 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.

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 peça Resolução CVM 21, o qual contém, sem limitação, informações sobre os fundos geridos, valores sob gestão e tipos de investidores; (iii) revisão periódica de seus manuais, códigos e políticas, os quais devem ser disponibilizados no website da Gestora; e (iv) informações exigidas pela legislação e regulamentação que trata da prevenção à lavagem de dinheiro.

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

10. PROCEDIMENTOS OPERACIONAIS

A Gestora atua em conformidade com os padrões e valores éticos elevados, principalmente observando e respeitando as normas expedidas pelos órgãos reguladores e suas Políticas Internas. Na condução de suas operações, a Gestora deverá:

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

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

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

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

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

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

10.1. Registro de operações

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

10.2. Liquidação das Operações

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

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 acionado toda vez que, por qualquer motivo, o acesso às

dependências da Gestora fique inviabilizado.

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

12. SEGURANÇA CIBERNÉTICA

A Gestora adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

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

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 ruma 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.

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*).

12.3. 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

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.

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; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

12.5. 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 análise e decisão do Diretor de *Compliance*.

ANEXO I - Modelo de Relatório Anual de *Compliance*

São Paulo,_____de janeiro de_____.

Aos Diretores,

Ref.: Relatório Anual de *Compliance*

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos **CPV CAPITAL GESTÃO DE RECURSOS LTDA** ("Gestora"), nos termos do Manual de Controles Internos *(compliance)* da Gestora ("Manual de *Compliance*"), e da Resolução CVM 21, de 25 de fevereiro de 2021, da Comissão de Valores Mobiliários ("Resolução CVM 21"), e na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de *Compliance* e da Resolução CVM 21 ("Diretor de *Compliance*"), informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20_.

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

I. Conclusão dos exames efetuados:

II. Recomendações e cronogramas de saneamento:

III. Manifestação sobre verificações anteriores:

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____

Diretor de *Compliance* e Risco

ANEXO II - Termo de Adesão

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

1. Estou ciente da existência do "Manual de Controles Internos *(compliance)*" da **CPV CAPITAL GESTÃO DE RECURSOS 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" ("Políticas Internas"), que recebi, li e tenho em meu poder.

2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas 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 no Manual de *Compliance* da Gestora, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.

4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos 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 no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada 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 III - Solicitação para Desempenho de Atividade Externa

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

_____
_____

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

3. Descreva suas responsabilidades decorrentes da Atividade Externa:

_____

_____.

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

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

_____.

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da **CPV CAPITAL GESTÃO DE RECURSOS 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 IV - Metodologia de Avaliação do Risco e Monitoramento Individualizado

Com vistas ao cumprimento do Código ANBIMA, após a análise do terceiro, a Área de Compliance classificará o terceiro com o potencial de (i) Baixo Risco; (ii) Médio Risco; ou (iii) Alto Risco, conforme segue:

1. <u>Metodologia e Avaliação</u>

1.1. **<u>Baixo Risco</u>**: a Gestora pode deixar de aplicar os procedimentos de pré-seleção estabelecidos neste Manual de Compliance a seu exclusivo critério quando também se verificar que o terceiro, cumulativamente: (i) possui destacada capacidade econômica e financeira e/ou técnica para satisfazer o propósito do contrato; (ii) possui capacidade para cumprir as responsabilidades contratuais estabelecidas; (iii) possui reputação ilibada; e (iv) é membro/associado da ANBIMA, quando aplicável.

1.2. **<u>Médio Risco:</u>** a Gestora adotará os procedimentos estabelecidos nesta Política, e documentos adicionais poderão ser solicitados conforme o caso. Serão classificados como de Médio Risco terceiros que não possam ser classificados como de Baixo Risco, mas que não tenham sua atividade relacionada com a atividade fim da Gestora.

1.3. **<u>Alto Risco:</u>** Terceiros com Potencial Alto Risco: a Gestora sujeitará o terceiro à mais completa investigação, de acordo com os procedimentos adotados nesta Política e outros documentos e certificados necessários de terceiros. Será classificado como de Alto Risco o terceiro que não se enquadrar nas hipóteses anteriores. Uma vez classificado como um terceiro de Alto Risco, a decisão final sobre a contratação desse terceiro caberá ao Comitê de Compliance da Gestora,

juntamente com um relatório derivado de sua análise da documentação recebida pelo terceiro durante o Processo de Pré-seleção.

2. Monitoramento

Terceiros serão supervisionados e reavaliados de acordo com sua classificação por grau de risco e segundo os artigos 23 e 24 do Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros, como segue:

(i) **Baixo Risco**: Uma vez a cada 36 (trinta e seis) meses;

(ii) **Médio Risco**: Uma vez a cada 24 (vinte e quatro) meses; e

(iii) **Alto Risco**: Uma vez a cada 12 (doze meses)

Histórico das Atualizações		
Data	**Versão**	**Responsável**
Julho de 2022	1ª	Diretor de Compliance e Risco
Abril de 2023	2ª	Diretor de Compliance e Risco
Abril de 2024	3ª	Diretor de Compliance e Risco
Março de 2025	4ª	Diretor de Compliance e Risco

ANEXO V - Informações Periódicas Exigidas pela Regulamentação

Informações	**Prazo**	**Destinatário**	**Forma de Arquivamento**
Enviar à CVM o Formulário de Referência devidamente preenchido, contendo informações sobre os Veículos de Investimento sob gestão, profissionais, estrutura administrativa e operacional etc.	Até o dia 31 de março de cada ano, com base nas posições de 31 de dezembro do ano anterior	CVM	Internet (por meio do site da CVM)
O Diretor de *Compliance* deverá encaminhar relatório dos controles internos, regras e procedimentos estabelecidos neste Manual de *Compliance* (e.g. testes de segurança nos sistemas, medidas para manter as informações confidenciais, programas de treinamento).	Até 31 de janeiro de cada ano, com base nas informações do ano civil imediatamente anterior	*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 certificadas pela ANBIMA e que as informações de NAV e valor das cotas dos fundos de investimento foram enviadas.	Até 31 de março, com base nas informações de 31 de dezembro do ano anterior	ANBIMA	Site da ANBIMA
Reportar ao COAF e CVM, se for o caso, a não ocorrência de propostas, transações ou operações passíveis de	Até o último dia útil de abril de cada ano, com base no ano imediatamente anterior	COAF	SISCOAF

Informações	**Prazo**	**Destinatário**	**Forma de Arquivamento**
serem comunicadas nos termos da Lei 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 o s 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	No momento da adesão e sempre	ANBIMA	Via Sistema SSM da ANBIMA

de Voto junto à ANBIMA.	que atualizada		
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

* * *