MANUAL DE 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 MIRABAUD INVESTIMENTOS LTDA. (“Gestora”) adotou em sua estrutura as atividades de “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 Compliance (“Manual de Compliance”) foi elaborado para atender especificamente às atividades desempenhadas pela Gestora, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de Compliance é aplicável a todos os sócios, diretores, funcionários, empregados, estagiários e demais colaboradores da Gestora (em conjunto os “Colaboradores” e, individualmente e indistintamente, o “Colaborador”).

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

Este Manual de Compliance está de acordo com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários (“CVM”).

2. PROCEDIMENTOS

2.1 Designação de um Diretor Responsável por Compliance

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

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

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

O Diretor de Compliance tem como principais atribuições e responsabilidades o suporte a todas as áreas da Gestora no que concerne a esclarecimentos de todos os controles e regulamentos internos (compliance), bem como no acompanhamento de conformidade das operações e atividades da Gestora com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível 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:

Implantar o conceito de controles internos através de uma cultura de compliance, visando melhoria nos controles;

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

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”);

Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;
Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

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

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

Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Gestora;
Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Gestora, assim como das pessoas envolvidas no caso.

2.2 Comitê Executivo:

Estas Regras estabelecem as seguintes funções e responsabilidades para tomada de decisão em Comitê Executivo:

a. Comitê Executivo

O Comitê Executivo estabelece a política de negócios e a tolerância ao risco de lavagem de dinheiro e determina o apetite ao risco de lavagem de dinheiro. Nesse contexto, o Comitê aprova este Manual. O Conselho de Administração revisa anualmente a política de gestão de risco de lavagem de dinheiro, com base na análise de risco fornecida pelo Diretor de Compliance e de acordo com o Regulamento Organizacional. O Comitê é informado das mudanças no risco de lavagem de dinheiro a cada ano pelo Diretor de Compliance.

O Comitê Executivo decide, ainda, se aprova novos relacionamentos PEP (Pessoa Politicamente Exposta) ou de AR (Alto Risco) e decide a cada ano se deve continuar os relacionamentos PEP/AR existentes abertos por mais de doze meses.

O Comitê Executivo deve:

• ser informado dos relatórios de divulgação enviados à autoridade (COAF);
• ser informado todos os anos dos riscos de branqueamento de capitais reportados nas avaliações de risco jurídico e reputacional;
• validar a continuidade das relações comerciais para todos os PEPs nas revisões anuais;
• validar as relações comerciais de maior risco, as transações de maior risco em geral e outras mudanças significativas nos riscos jurídicos e de reputação, em particular se ativos significativos ou pessoas politicamente expostas forem afetados;
• ser informado de qualquer desvio das disposições legais e regulamentares propostas por uma entidade que seja considerada menos rigorosa do que as estabelecidas nas regras de PLD/FTP do Grupo;
• validar a criação de categorias de risco adicionais.
• acompanhar o processo de avaliação e esclarecimento de maiores riscos, bem como o processo de reporte de relações contempladas (incluindo prospects), relações existentes ou casos de operações sujeitas a maior risco não esclarecidas no prazo designado;

• monitorar a implementação destas Regras e quaisquer adaptações;
• decidir sobre quaisquer outros assuntos relacionados com a prevenção do branqueamento de capitais e financiamento do terrorismo ou com temas de Compliance, e desde que não exista comitê específico para tanto.

2.3 Revisão periódica e preparação de relatório

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

O Diretor de Compliance deve encaminhar aos diretores da Gestora, até o último dia do mês de março 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.

2.4 Treinamento

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

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

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

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

2.5 Apresentação do Manual de Compliance e suas modificações

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

2.6 Atividades Externas

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

2.7 Supervisão e responsabilidades

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

2.8 Sanções

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

3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

Nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021 (“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 informática e pela área de compliance.

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

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

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

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

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

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

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor em nuvem da Gestora. Nesse servidor, as informações são segregadas por área, sendo armazenadas com backup.

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 Instrução CVM nº 358, de 03 de janeiro de 2002 (“Instrução CVM 358”).

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 Gestora possui em seu objeto social as atividades de gestão de recursos de terceiros e a consultoria de valores mobiliário, sendo que , a área de gestão de recursos e a área de consultoria de valores mobiliários serão fisicamente segregada entre si e das demais áreas que venha existir com a Gestora, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas, para garantir que não exista circulação de informações que possam gerar conflito de interesses (“chinese wall”).

As áreas que não sejam segregadas da Gestora deverão ser destinadas à áreas administrativas, como recursos humanos, financeiro, tecnologia de informação etc. Áreas comuns da Gestora como refeitórios, copas e demais espaços deverão ser utilizados para seu destino próprio e não será permitido a divulgação de informações das áreas que devem ser segregadas e não poderão ser utilizadas para reuniões.

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 de gestão de recursos de terceiros e de consultoria de valores mobiliários 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 consultoria de valores mobiliários, nem com os demais Colaboradores, sendo que haverá impressora e fax destinados exclusivamente à utilização da área de administração de recursos e consultoria de valores mobiliários.

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.

Segregação em relação às demais empresas nas quais os sócios e/ou diretores da Gestora tenham participação societária ou constem do conglomerado societário da Gestora.

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 consultoria de valores mobiliários, bem como evitar qualquer compartilhamento de informação, a Gestora determina que os sócios que possuam participação societária em outras empresas atuantes no mercado financeiro e de capitais não poderão ter atuação funcional em tal empresa, devendo figurar apenas como sócios de capital.

Além disso, as empresas das quais componham a estrutura societária da Gestora ou sejam parte do mesmo conglomerado deverão ser fisicamente segregadas das áreas de gestão de recursos de terceiros e consultoria de valores mobiliários, bem como não compartilhar arquivos e sistemas com os daqueles utilizados pela Gestora.

5.3 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:

Definição de responsabilidades dentro da Gestora;

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

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;

Contínua avaliação dos diversos riscos associados às atividades da empresa; e

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 a Instrução CVM nº 400, de 29 de dezembro de 2003 (“Instrução CVM 400”), a Instrução CVM nº 476, de 16 de janeiro de 2009 (“Instrução CVM 476”), a Instrução CVM nº 555, de 17 de dezembro de 2014 (“Instrução CVM 555”), o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, e diretrizes escritas emanadas da ANBIMA. O Diretor de Compliance deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de Compliance é que qualquer material de marketing deve ser utilizado.

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

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

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

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

ser identificado como material de divulgação;

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;

ser apresentado em conjunto com a lâmina, se houver;

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

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

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

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

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

mencionar a data do início de seu funcionamento;

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;

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

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

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

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

Ficam incorporadas por referência, ainda, as disposições do Capítulo VI do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como das

"Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento" da ANBIMA, disponíveis publicamente no website desta instituição.

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 melhores classificadas.

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

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) E PREVENÇÃO À LAVAGEM DE DINHEIRO AO FINANCIAMENTO DE PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

O termo “lavagem de dinheiro” abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. A Gestora e seus Colaboradores devem obedecer todas as regras de prevenção à lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613, de 03 de março de 1998, conforme alterada (“Lei 9.613/98”), e a Instrução CVM nº 50, de 02 de setembro de 2021 (“Instrução CVM 50”), cujos principais termos estão refletidos neste Manual de Compliance.

O Diretor de Compliance será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento de proliferação de armas de destruição em massa (PLD/FTP).

O Diretor de Compliance estabelecerá o devido treinamento dos Colaboradores da Gestora – na forma deste Manual de Compliance – para que estes estejam aptos a reconhecer e a combater a LD/FTP, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

8.1 Supervisão Baseada em Risco

Como principal diretriz do seu programa de PLD/FTP, 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 LD/FTP inerentes às suas atividades por meio da adoção de uma abordagem baseada em risco, para garantir que as medidas de prevenção sejam proporcionais aos riscos identificados.

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

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

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

A Gestora adota procedimentos internos para a seleção e monitoramento de administradores, funcionários, e prestadores de serviços relevantes contratados.

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 LD/FTP.

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

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

Além da supervisão baseada em risco, A Gestora adota os seguintes procedimentos permanentes de controle e vigilância, visando minimizar o risco de ocorrência de LD/FTP nas diversas operações financeiras sob sua responsabilidade, a saber:

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

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

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

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

Avaliação das políticas e práticas de prevenção e combate à LD/FTP adotada por terceiros/parceiros da Gestora;

Verificação da adequação ao perfil da Gestora dos Clientes oriundos dos distribuidores de cotas de fundos de investimento cujas carteiras sejam geridas pela Gestora;

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

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

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

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

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

Não estabelecer relacionamento com pessoas ligadas direta ou indiretamente a crime organizado, a empresas de "fachada", a lavagem de dinheiro, ao financiamento ao terrorismo ou com vínculo a produção ou distribuição de armas e produtos militares;

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

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

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

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

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

A Gestora adota procedimentos que permitem o monitoramento das faixas de preços das cotas de fundos geridos distribuídas, de modo que eventuais operações efetuadas fora dos padrões praticados

no mercado, de acordo com as características do negócio, sejam identificadas, e se for o caso, comunicados aos órgãos competentes.

8.2 Cadastro de clientes e atualização

Na atuação de gestão de carteiras e/ou distribuição de cotas de fundos geridos pelo Mirabaud, aplicar-se-á o procedimento previsto nesta seção.

8.3 Governança:

O sistema de governança e gestão interna de LD/FTP consiste em três linhas de defesa, cada uma das quais está envolvida em seu próprio nível no monitoramento das relações comerciais e transações dentro da entidade. Estas três linhas de defesa são definidas da seguinte forma:

A primeira linha de defesa é representada pelos Gerentes de Relacionamento ("o(s) Gerente(s) de Relacionamento") e os responsáveis pela implementação das atividades operacionais do Mirabaud. Essas pessoas normalmente estão em contato direto com os clientes e têm um bom conhecimento dos riscos de LD/FTP, o que lhes permite detectar potenciais indicadores de risco. As unidades de negócio geradoras de receitas exercem a sua função de controle da atividade diária do Mirabaud através da gestão dos riscos e, em particular, da monitorização direta, orientação e reporte.

A segunda linha de defesa é representada em particular pelo Departamento de Compliance. As tarefas e responsabilidades deste departamento incluem a elaboração de uma análise de risco numa perspectiva de combate ao branqueamento de capitais e financiamento do terrorismo, tendo em conta fatores como a sede ou domicílio do cliente, o segmento de clientes gerido e os produtos e serviços oferecidos. A análise é atualizada regularmente e pelo menos uma vez por ano. Para além das suas atribuições e responsabilidades enquanto função de controlador independente, o Departamento de Compliance apoia e aconselha a direção executiva e os colaboradores do Mirabaud no desenvolvimento, implementação e monitorização de alterações regulatórias e regulamentos internos. O Departamento de Compliance também apoia a gestão executiva na formação e informação dos colaboradores sobre questões relacionadas com o compliance. O envolvimento da segunda linha de defesa aumentará dependendo do nível de risco atribuído a um cliente.

A terceira linha de defesa é representada pela função de auditoria, que avalia de forma independente as duas primeiras linhas de defesa e verifica a eficácia dos controles existentes.

Como primeira linha de defesa, o Gerente de Relacionamento deve ter um entendimento de seus clientes e é responsável por coletar e formalizar as informações necessárias para avaliar o risco de lavagem de dinheiro, por exemplo, quando um novo relacionamento é estabelecido, uma mudança é

feita os elementos que compõem o perfil de relacionamento (como abertura de carteira adicional, adição ou retirada de procuração, mudança de domicílio ou estabelecimento etc.), um relacionamento é revisto, uma operação é caracterizada por maior risco etc.

Como primeira linha de defesa, o Gerente de Relacionamento é responsável pelo seguinte:

- obter os esclarecimentos adicionais necessários para encerrar com a maior brevidade possível os alertas gerados pelo sistema utilizado para identificar as operações de maior risco;
- informar imediatamente o Departamento de Compliance sobre qualquer elemento trazido ao seu conhecimento que possa ter impacto na avaliação do risco de lavagem de dinheiro e risco reputacional.
- realizar revisões periódicas e controlar os riscos das relações comerciais.
- aplicar as instruções e diretrizes fornecidas pelo Departamento de Compliance para fornecer suporte conforme necessário para as revisões anuais do PEP;
- revisar e validar alertas previamente esclarecidos pelo Gerente de Relacionamento, no que diz respeito aos alertas gerados pelo sistema utilizado para identificar transações de maior risco;
- apoiar os Gerentes de Relacionamento na avaliação de relacionamentos e/ou transações comerciais de alto risco.

Como segunda linha de defesa, o Departamento de Compliance é responsável pelas seguintes tarefas, em particular:

- análise de casos com riscos potenciais de LD/FTP;
- realização de verificações adicionais de PEP e relações de maior risco no início dessas relações, nomeadamente com base em esclarecimentos obtidos pela primeira linha de defesa;
- identificar relacionamentos existentes que precisam ser categorizados como PEP ou relacionamentos de maior risco com base em informações obtidas pelos Gestores e/ou alertas gerados por sistemas de triagem e/ou outras fontes consideradas confiáveis. Após análise e verificação dos esclarecimentos adicionais obtidos pela primeira linha de defesa, o Departamento de Compliance submete as reclassificações, com o seu parecer, ao Comitê Executivo;
- emitir diretrizes para revisões periódicas de todas as relações comerciais.

Durante essas revisões periódicas, o papel do Departamento de Compliance é limitado a:

- Verificar se a 1ª linha de defesa gerenciou adequadamente os riscos com base nas orientações fornecidas;
- fornecer sua expertise em casos particulares que exigem habilidades especiais, para os casos de maior risco ou mesmo para relacionamentos de maior risco;

- revisar como parte de revisões de relacionamentos caracterizados por níveis de risco padrão, verificando a qualidade da revisão realizada por amostragem pela primeira linha de defesa;
- verificar as relações de maior risco efetuada pela primeira linha de defesa, antes da sua submissão ao Comitê Executivo;
- preparar a revisão anual do PEP e ser o departamento competente para analisar as informações coletadas pelo Gestor com base nas diretrizes emitidas, a fim de emitir um parecer informado sobre a continuidade do relacionamento comercial, a ser submetido ao Comitê Executivo;
- reunir os resultados da revisão anual de todos os relacionamentos PEP para as entidades do Grupo;
- analisar os esclarecimentos adicionais sobre operações de maior risco obtidos por amostragem pela primeira linha de defesa.
- analisar qualquer relação ou transação que suscite motivos razoáveis de suspeita ou indícios que alimentem a suspeita de que os bens provêm de um crime, criando o dever ou o direito de comunicar essa situação à autoridade competente contra o branqueamento de capitais (COAF). O Departamento de Compliance determina se o relacionamento ou transação deve ser reportado aplicando o processo detalhado neste Regulamento;
- elaborar um relatório anual dirigido aos sócios sobre a avaliação do risco de compliance e as atividades do Departamento de Compliance;
- treinar funcionários sobre as disposições destas Regras e sobre as leis e regulamentos locais que se aplicam além destas Regras.

8.4 Diretrizes do Programa de KYC

O processo de aceitação, aprovação, e classificação em graus de riscos dos clientes, bem como o monitoramento de transações, devem ser compatíveis com o perfil determinado para cada cliente. Além disso, deve se levar em consideração o risco de utilização dos produtos e serviços oferecidos pela Gestora. Assim, a fim de se adaptar à legislação e regulamentação vigente, a Gestora desenvolveu o seguinte conjunto de regras e procedimentos:

(xv) Sempre que possível, conhecer pessoalmente o cliente, caso não for possível, conhecer o cliente por meio de informações e documentos confiáveis, de fonte independente;

(ii) Realizar visitas periódicas ao cliente em sua empresa ou residência, sempre que a Gestora julgar necessário, caso existam indícios de má conduta ou descumprimento ao presente Manual de Compliance;

(iii) Verificar informações sobre o cliente disponíveis em jornais e na internet, se for o caso;

(iv) Conhecer a fonte de renda e a origem do patrimônio do cliente, bem como o país onde a renda é auferida, a profissão e atividades exercidas para comprovação da renda ou faturamento;

(v) Avaliar se a finalidade da conta e o nível de atividade proposto estão de acordo com o perfil financeiro geral do cliente;

(vi) Conhecer a origem e destino dos recursos movimentados pelo cliente e a fonte de renda;

(vii) No caso de PPE, conhecer o cargo atual ou anteriormente exercido e sua duração;

(viii) Conhecer o nível de acesso da PPE a fundos estatais;

(ix) Avaliar a transparência e a complexidade da estrutura e da posse da conta de cada cliente;

(x) Avaliar se a finalidade da conta e o nível de atividade estão de acordo com o perfil do cliente;

(xi) Se o cliente for pessoa jurídica, condicionar o início do relacionamento comercial à apresentação de informações sobre as pessoas naturais que se caracterizam como beneficiários finais de forma satisfatória, a critério da Gestora, bem como de seus controladores indiretos e sempre levando em conta o disposto na regulamentação aplicável;

(xii) Se o cliente for estrangeiro, conhecer o regime político e socioeconômico do país de origem, seu nível de corrupção, controle de drogas, se constituídos sob a forma de trusts e sociedades com títulos ao portador. Contribuem para elevar o risco dos investidores não residentes: 1. Dificuldade na identificação do próprio investidor e da origem dos recursos, de acordo com a estrutura utilizada; 2. Dificuldade de visita in loco; 3. Utilização de estruturas que envolvam jurisdições diversas que impossibilitem ou dificultem o acesso a informações;

(xiii) Se o cliente estrangeiro for constituído sob a forma de trust ou veículo assemelhado, serão: 1. Pessoa que instituiu o trust ou veículo assemelhado (settlor); 2. O supervisor do veículo de investimento, se houver (protector); 3. O administrador ou gestor do veículo de investimento (curador ou trustee); e 4. O beneficiário do trust, seja uma ou mais pessoas naturais ou jurídicas.

(xiv) Possibilidade de veto a relacionamentos devido ao risco envolvido, considerando aquilo que foi exposto nas alíneas anteriores; e

(xv) Identificação, análise, decisão e reporte das situações atípicas.

As informações obtidas como resultado das diligências representadas nos itens anteriores, bem como informações relevantes, deverão ser documentadas em formulários ou registros eletrônicos adequados, e serão mantidos em arquivo por pelo menos 5 (cinco) anos após o fim de cada relacionamento comercial.

Realizados os procedimentos previstos neste Manual de Compliance será atribuída classificação de risco para o cliente segmentada por grau entre (i) baixo; e (ii) alto.

Nos termos da Instrução CVM 50, o cadastro dos Clientes da Gestora deve abranger, no mínimo, as informações e documentos indicados abaixo:

Pessoa física: nome completo, data de nascimento, naturalidade, nacionalidade, estado civil, nome da mãe, número do documento de identificação e órgão expedidor, número de inscrição no Cadastro de Pessoas Físicas ("CPF"), nome e respectivo número do CPF do cônjuge ou companheiro, se for caso, endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP), número de telefone, endereço eletrônico para correspondência, ocupação profissional, nome da entidade para qual trabalha com a respectiva inscrição no Cadastro Nacional de Pessoas Jurídicas ("CNPJ"), informações atualizadas sobre os rendimentos e a situação patrimonial, informação sobre o perfil do cliente, conforme regulamentação específica, se cliente opera por conta de terceiros (no caso de carteiras administradas), se o cliente autoriza ou não a transmissão de ordem por procurador (nesse caso, será necessário o endereço completo dos procuradores, bem como o registro se eles são considerados PPE), qualificação dos procuradores e descrição dos seus poderes, datas das atualizações do cadastro e assinatura do cliente. Além disso, é necessário cópia dos seguintes documentos: documento de identidade e comprovante de residência ou domicílio; e, caso o cliente atue por meio de procurador, cópias da procuração e documento de identidade do procurador (com CPF).

Pessoa jurídica: denominação ou nome empresarial, nomes e CPF dos controladores diretos ou nome empresarial e inscrição no CNPJ dos controladores diretos com a indicação se eles são PPE, nome e CPF dos administradores, se for o caso, nome e CPF dos procuradores, inscrição no CNPJ, endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP), número de telefone, endereço eletrônico para correspondências, informações atualizadas sobre o faturamento médio mensal dos últimos 12 (doze) meses e a respectiva situação patrimonial, informações sobre o perfil do cliente, conforme regulamentação específica, se o cliente opera por conta de terceiros (no caso de carteiras administradas), se o cliente autoriza ou não a transmissão de ordens por representante ou procurador, qualificação dos representantes ou procuradores e a descrição dos seus poderes, datas das atualizações do cadastro e assinatura do cliente. Também serão necessárias cópias dos seguintes documentos: cartão do CNPJ, documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente, e atos societários que indiquem os administradores da pessoa jurídica, se for o caso; e, caso o cliente atue por meio de procurador, cópias da procuração e documento de identidade do procurador (com CPF).

Em todos os casos, o cadastro dos clientes deverá observar aquilo disposto no Anexo B da Instrução CVM 50. Ainda, a Gestora adotará procedimentos para identificação da pessoa natural caracterizada como beneficiário final, nos termos da legislação e regulamentação vigentes.

As alterações ao endereço constante do cadastro dependem de ordem do Cliente, escrita ou por meio eletrônico, e comprovante do correspondente endereço.

Do cadastro deve constar declaração, datada e assinada pelo Cliente ou, se for o caso, por procurador legalmente constituído, de que (conforme aplicável):

são verdadeiras as informações fornecidas para o preenchimento do cadastro;

o Cliente se compromete a informar, no prazo de 10 (dez) dias, quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, inclusive eventual revogação de mandato, caso exista procurador;

o Cliente é pessoa vinculada ao intermediário, se for o caso;

o Cliente não está impedido de operar no mercado de valores mobiliários;

suas ordens devem ser transmitidas por escrito, por sistemas eletrônicos de conexões automatizadas ou telefone e outros sistemas de transmissão de voz; e

o Cliente autoriza os intermediários, caso existam débitos pendentes em seu nome, a liquidar os contratos, direitos e ativos adquiridos por sua conta e ordem, bem como a executar bens e direitos dados em garantia de suas operações ou que estejam em poder do intermediário, aplicando o produto da venda no pagamento dos débitos pendentes, independentemente de notificação judicial ou extrajudicial.

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

Após a análise e verificação, pela área de 26ompliance, dos documentos e informações fornecidos pelo Cliente, o Diretor de Compliance decidirá pela aprovação ou, caso seja identificado um caso de PPE ou AR, envio do cadastro do cliente para análise do Comitê Executivo. O fornecimento da totalidade dos documentos e informações solicitados não é garantia da aprovação do cadastro do Cliente, podendo a Gestora recusar o cadastramento de Clientes a seu exclusivo critério.

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

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

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

8.5 Procedimentos relacionados às contrapartes

A Gestora é responsável por tomar todas as medidas necessárias, segundo a legislação e regulamentação aplicável, incluindo, mas não limitado a, Lei 9.613/98, Instrução CVM 50 e Ofício-Circular nº 5/2015/SIN/CVM, as regras de cadastro, know your client - KYC ("conheça seu cliente"), know your employee – KYE ("conheça seu funcionário") e know your partner – KYP ("conheça seu parceiro") presentes neste Manual de Compliance e as melhores práticas adotadas pelas entidades autorreguladoras do mercado, para estabelecer e documentar a verdadeira e completa identidade, situação financeira e o histórico de cada contraparte nas operações realizadas pelos fundos de investimento.

Nesse sentido, além dos clientes de suas carteiras, a Gestora busca analisar e monitorar, para fins de cumprimento às normas de prevenção à lavagem de dinheiro, as contrapartes com quem venha negociar os ativos que pretende adquirir, novas tecnologias, serviços ou produtos que pretenda adquirir visando uma eficaz prevenção de quaisquer atividades inidôneas em seus ativos sob gestão.

Como complementação ao processo de KYC, o Departamento de Compliance realiza procedimento de background check por meio de ferramentas de pesquisas automatizadas para verificação de ocorrências e fatos relevantes em nome de clientes, prospects e pessoas relacionadas, incluindo as seguintes ferramentas (sem prejuízo da utilização de outras): World Check, Lexis Nexis e Google.

8.6 Pessoas politicamente expostas

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

O Anexo A da Instrução CVM 50 dista aqueles indivíduos que são considerados PPE, sendo possível genericamente designá-los como aqueles que "desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo, sendo consideradas como pessoas expostas politicamente os os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União; os ocupantes de cargo, no Poder Executivo da União, de: a) Ministro de Estado ou equiparado; b) Natureza Especial ou

equivalente; c) Presidente, Vice-Presidente e Diretor, ou equivalentes, de entidades da administração pública indireta; e d) Direção e Assessoramento Superior - DAS de nível 6 ou equivalente; os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal; os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal; os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União; os Presidentes e Tesoureiros nacionais, ou equivalentes, de partidos políticos; os Governadores e Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os Presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os Presidentes de Tribunais de Justiça, Militares, de Contas ou equivalentes de Estado e do Distrito Federal; os Prefeitos, os Vereadores, os Secretários Municipais, os Presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas de Municípios ou equivalentes. E também aquelas que, no exterior, sejam: chefes de estado ou de governo; políticos de escalões superiores; ocupantes de cargos governamentais de escalões superiores; oficiais generais e membros de escalões superiores do poder judiciário; executivos de escalões superiores de empresas públicas; dirigentes de partidos políticos; os dirigentes de escalões superiores de entidades de direito internacional público ou privado.

A Circular do BACEN nº 3.978, de 23 de janeiro de 2020, e alterações posteriores, dispõe sobre os procedimentos a serem observados pelos agentes financeiros para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PPE, os quais devem ser estruturados de forma a possibilitar a caracterização de pessoas consideradas PPE e identificar a origem dos fundos envolvidos nas transações dos Clientes assim identificados.

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

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

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

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

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

8.7 Regras adicionais para PPEs

O Mirabaud tem como política ser restritivo na aceitação de relações comerciais com PPEs. Nesta base, os riscos associados a uma relação PPE são avaliados através de um sistema de pontuação que tem em conta o país onde o PPE opera, o grau de proximidade com os líderes do país em causa, o setor de atividade, a reputação do PEP, e se a posição é atual. A estrutura de análise é fornecida no Anexo V a título de ilustração, cabendo ao Departamento de Compliance assegurar a sua adaptação e atualização.

Essa avaliação é realizada pelo Gerente de Relacionamento no início do relacionamento e a cada revisão anual:

- se a pontuação for superior a 3, o relacionamento PPE não deve ser aberto ou continuado, a menos que sejam realizados procedimentos adicionais de esclarecimento (por exemplo, obtenção de relatório de um provedor especializado). Quando for utilizado um prestador de serviços externo, o Departamento de Compliance é responsável por selecionar, instruir e monitorar esse prestador. O relatório é atualizado, em princípio, a cada três anos, desde que a pontuação permaneça acima de 3;

- se a pontuação for 3 ou inferior, a relação PEP é considerada um risco aceitável e pode ser aberta ou continuada.

8.8 Regras específicas onde uma estrutura complexa está envolvida

Uma estrutura é classificada como complexa quando atende aos seguintes critérios (ver Anexo VI):

- existem pelo menos três pessoas jurídicas posicionadas entre o titular da conta e o beneficiário efetivo;
- o Relacionamento possui um Link para Clientes domiciliados em pelo menos três jurisdições diferentes. Nesse caso, é o Relacionamento que é considerado de maior risco.

Para identificar se a estrutura é complexa, o Gerente de Relacionamento coleta as seguintes informações e documentos:

- para Clientes que sejam «sociedades domiciliadas»: documentos comprovativos da titularidade do beneficiário efetivo (por exemplo, extrato do registo de acionistas);
- para Clientes que sejam 'empresas sujeitas à obrigação de divulgação de entidades que exerçam o controle': um extrato do registro oficial.

A complexidade da estrutura deve ser mais bem analisada pelo Gerente de Relacionamento para que o Departamento de Compliance possa avaliar se ela se justifica. De fato, as razões para usar tais estruturas devem ser esclarecidas e compreendidas tanto pela primeira quanto pela segunda linha de defesa.

Além disso, quando a estrutura possui acionistas indicados, o Gerente de Relacionamento deve obter documentação sobre a relação contratual subjacente.

Caso o contratante seja uma empresa domiciliada, o Gerente de Relacionamento deve documentar os motivos pelos quais o Relacionamento utiliza essa construção.

8.9 Desclassificação de PPE e status de alto risco

Cinco anos após o abandono do estatuto que justifica a classificação como PPE a eventual desclassificação da relação é analisada pelo Departamento de Compliance durante a revisão anual e é elaborado um parecer pelo Departamento de Compliance ao Comitê Executivo, que acabará por confirmar a desclassificação.

Quando uma relação de alto risco não se qualifica como tal, uma revisão de desclassificação é realizada da mesma forma que a revisão periódica de contas de alto risco. Um parecer de desclassificação é enviado pelo Departamento de Compliance ao Comitê Executivo, que valida essa desclassificação.

8.10 Regras Adicionais de AR

Os critérios para determinar as operações de maior risco são detalhados no Anexo VI.

Ao identificar uma operação que apresente indícios de lavagem de dinheiro na acepção da regulamentação aplicável, o Departamento de Compliance avalia se, dependendo das circunstâncias, essa operação deve ser considerada uma operação de maior risco.

O Gerente de Relacionamento tem a responsabilidade primária de monitorar as transações realizadas para os Clientes e Carteiras sob seu controle.

Quando o Gerente de Relacionamento identifica uma transação de maior risco ou que possa indicar lavagem de dinheiro, ele informa imediatamente o Departamento de Compliance. Essas transações também podem ser identificadas por qualquer departamento ou pelo Departamento de Compliance por meio do sistema informatizado.

Independentemente da forma como estas operações tenham sido identificadas, são consideradas operações de maior risco e, portanto, sujeitas a esclarecimentos adicionais.

Para esclarecer as transações de maior risco, o Gerente de Relacionamento preenche uma nota de contato especificando a finalidade econômica da transação, bem como seu histórico econômico, a contraparte (atividade comercial/profissional e relacionamento com o cliente) e a cadeia de propriedade/entidades exercendo o controle se for uma empresa pertencente ao cliente. O Gerente de Relacionamento também examina se a transação pretendida parece plausível e suficientemente fundamentada com base no conhecimento do cliente e no contexto econômico apresentado.

Documentos comprovativos devem ser anexados à nota de contato, dependendo da natureza da transação. O Departamento de Compliance realiza uma segunda análise sobre uma amostra de transações.

O Departamento de Compliance avalia se os esclarecimentos da primeira linha de defesa são satisfatórios no caso específico que está analisando:

- Em caso afirmativo, fecha o alerta.
- Caso contrário, o Departamento de Compliance entra em contato por e-mail com o Gerente de Relacionamento, informando-o sobre os pontos pendentes e indicando as informações e possíveis documentos a serem obtidos para o fechamento do alerta.

O Departamento de Compliance analisa os esclarecimentos adicionais obtidos por amostragem pela primeira linha de defesa.

Se as informações necessárias não puderem ser obtidas após o processo de esclarecimento adicional, o Departamento de Compliance decidirá que:

- o alerta pode ser fechado como está;
- um prazo adicional deve ser alocado;
- a transação deve ser submetida ao Comitê Executivo.

8.11 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:

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;

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;

operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;
operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

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

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

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

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;
operações liquidadas em espécie, se e quando permitido;

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

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

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;

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

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

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

situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas; e

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

A Gestora deverá dispensar especial atenção às operações em que participem as seguintes categorias de Clientes:

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

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

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.

8.12 Processo

É responsabilidade do Gerente de Relacionamento identificar se um relacionamento apresenta uma ou mais características de um relacionamento de maior risco e determinar se deve ser classificado como tal.

A classificação como PPE ou relacionamento de maior risco é verificada pelo Departamento de Compliance. Nos casos em que a relação se refira a um PPE ou apresente riscos superiores, o Departamento de Compliance envia todo o processo e respetivo parecer ao Comitê Executivo. O processo de tomada de decisão em relação à classificação do relacionamento e aceitação dessa classificação é documentado.

Quando um relacionamento existente é identificado recentemente como um relacionamento de alto risco ou como um relacionamento PPE, o Departamento de Compliance informa imediatamente ao Gerente de Relacionamento e os pergunta, na medida em que o arquivo ainda não esteja

suficientemente documentado, para complementar as informações relevantes por meio de novos perfis ou procedimentos de esclarecimento adicionais. Esse departamento apresentará seu parecer sobre se a relação deve ser comunicada ao órgão competente.

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

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

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:

observar o princípio da probidade na condução de suas atividades;

prezar pela capacitação para o desempenho das atividades;

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

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

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

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:

Malwares: softwares desenvolvidos para corromper computadores e redes:
Vírus: software que causa danos à máquina, rede, outros softwares e bancos de dados;
Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

Spyware: software malicioso para coletar e monitorar o uso de informações; e
Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoas e número de cartão de crédito:
Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
Phishing: links transmitidos por e-mails, simulando se ruma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; 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.

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

Invasões (advanced 37ersistente 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:

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;

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;

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;

12.3 Rotinas de backup;

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

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;

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

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

12.4 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.

12.5 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.

12.6 Reciclagem e revisão

A Gestora manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

O Diretor de Compliance, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme 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 **MIRABAUD INVESTIMENTOS LTDA.** ("Gestora"), nos termos do Manual de *Compliance* da Gestora ("Manual de *Compliance*"), e do Artigo 25 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*

* * *

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 *Compliance)*" da MIRABAUD INVESTIMENTOS **LTDA.** ("Manual de *Compliance*" e "Gestora", respectivamente) e de todas as políticas internas da Gestora, inclusive o "Código de Conduta", a "Política de Investimento Pessoal" e a "Política de Gestão de Risco" ("Políticas Internas"), que recebi, li e tenho em meu poder.
2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas 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 Conduta e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos 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 **MIRABAUD INVESTIMENTOS 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 - Informações Periódicas Exigidas pela Regulamentação

Informações	Prazo	Destinatário	Forma de Arquivamento
Enviar à CVM o Anexo E da Resolução CVM 21 devidamente preenchido, contendo informações sobre os Veículos de Investimento sob gestão, profissionais, estrutura administrativa e operacional etc.	Até o dia 31 de março de cada ano, com base nas posições de 31 de dezembro do ano anterior	CVM	Internet (por meio do site da CVM)
O Diretor de *Compliance* deverá encaminhar relatório dos controles internos, regras e procedimentos estabelecidos neste Manual de *Compliance* (e.g. testes de segurança nos sistemas, medidas para manter as informações confidenciais, programas de treinamento).	Até 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 serem comunicadas nos termos da Lei 9.613/98, tendo por base o ano imediatamente anterior.	Até 31 de janeiro de cada ano, com base no ano imediatamente anterior	COAF	SISCOAF
Voto adotado nas assembleias de acionistas dos veículos de investimento.	5 dias subsequentes à assinatura	Administrador	Forma e horários previamente estabelecidos pelo Administrador
Em cada momento em que o conjunto de veículos de investimento gerenciado	Imediatamente após a ocorrência do evento	Companhia listada que	Carta ou qualquer outro modo

Informações	Prazo	Destinatário	Forma de Arquivamento
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.		emitiu os valores mobiliários	definido pela administração do(s) fundo(s) de investimento
Suspeita de lavagem de dinheiro ou atividades de financiamento de terrorismo, conforme definido na Lei 9.613/98.	24 horas após a ocorrência do evento	COAF	SISCOAF
Registrar a versão mais completa e atualizada da Política de Voto junto à ANBIMA.	No momento da adesão e sempre que atualizada	ANBIMA	Via Sistema SSM da ANBIMA
Registrar a versão mais completa e atualizada do Manual de Gerenciamento de Liquidez junto à ANBIMA.	No momento da adesão e no prazo de 15 (quinze) dias sempre que houver atualização	ANBIMA	Via Sistema SSM da ANBIMA

* * *

ANEXO V

CRITÉRIOS PARA RELACIONAMENTOS DE ALTO RISCO

CRITÉRIOS PARA IDENTIFICAÇÃO DE RELACIONAMENTO DE ALTO RISCO

Considera-se como de maior risco um Cliente que tenha relação com um titular de conta, uma entidade que exerça o controle societário, um beneficiário final ou um vínculo beneficiário por procuração que se enquadre um dos seguintes critérios:

• o titular da conta, beneficiário final ou entidade que exerce o controle ou beneficiário por procuração é um PPE;

• as relações comerciais com intermediários financeiros suíços e estrangeiros para os quais o Banco realiza operações de correspondente bancário devem, em todos os casos, ser consideradas de maior risco, com exceção das entidades do Grupo Mirabaud. Em princípio, o Banco não atua como banco correspondente de outras instituições bancárias, exceto entidades do Grupo Mirabaud, e se abstém de qualquer relação comercial com bancos de fachada;

• a sede, domicílio ou local de negócios da parte contratante, a entidade que exerce o controle ou o beneficiário final dos ativos está localizado em um país que o GAFI considere ser um país de alto risco ou não cooperativo, incluindo países para que exige uma maior diligência. O local de constituição das sociedades domiciliárias não deve ser considerado como algo natural, mas sim com base no risco real apresentado pelo relacionamento. Da mesma forma, a nacionalidade do contratante ou do beneficiário efetivo dos ativos em um desses países deve ser considerada caso a caso no cálculo do risco;

• a sede, domicílio ou local de negócios da parte contratante ou do beneficiário efetivo dos ativos está localizado em um país sob sanções (de acordo com as listas das Nações Unidas, a Secretaria de Estado Suíço para Assuntos Econômicos (SECO), o Escritório de Controle de Ativos Estrangeiros dos EUA (OFAC), Reino Unido e União Européia). Da mesma forma, a nacionalidade do cocontratante ou do beneficiário efetivo dos ativos em um desses países deve ser considerada caso a caso no cálculo do risco;

o Relacionamento está envolvido ou esteve envolvido em atividades comerciais nos seguintes setores (ver definições no Anexo VI):

• o Cliente é uma Conta Comercial;

• o Cliente representa um risco maior em relação a infrações fiscais;

• a estrutura da relação é considerada complexa;

• o Mirabaud não se encontrou com o titular da conta ou beneficiário efetivo.

• o Departamento de Compliance estimou que um Relacionamento pode ser considerado de maior risco sem que as condições previstas neste regulamento sejam atendidas e que o Comitê Executivo confirmou esta avaliação;

Critérios cumulativos

Considera-se como de maior risco, o Cliente cuja Relação com titular de conta, entidade que exerça o controle, beneficiário final ou procurador vinculado satisfaça pelo menos dois dos seguintes critérios:

o Relacionado exerce uma atividade econômica principal ou tem seu domicílio ou sede em um país definido como risco cumulativo na lista de países.

• o Relacionamento está envolvido ou tem sua atividade econômica em um setor definido como tendo um critério de risco cumulativo no Anexo VI;

* * *

Áreas de atividade profissional caracterizadas por maior risco e definições

Áreas de Atividade	Tipo de Critério	Comentários
Armas e equipamentos militares	Critério Simples	Armas e/ou equipamento militar: Relacionamento do cliente com qualquer indivíduo ou grupo de pessoas ou pessoas jurídicas que estejam direta ou indiretamente envolvidas em: - qualquer actividade relacionada com a concepção, produção ou comércio (nomeadamente intermediação) de equipamento militar ou outras armas ou armamentos; - qualquer serviço prestado no setor de segurança ou defesa; - o financiamento direto ou indireto desses materiais e atividades.
Casinos, apostas desportivas, jogos de azar	Critério Simples	N/A
Atividades sujeitas a concessão pública	Critério Simples	Compra/venda de produtos e serviços de contrapartes governamentais que representem pelo menos 25% das receitas, incluindo obras públicas e construção de infraestruturas públicas (estradas, pontes, etc.)
Construção de imóveis	Critério Cumulativo	Construção de edifícios comerciais e edifícios residenciais privados
Corretora de imóveis	Critério Cumulativo	N/A
Pedras preciosas e metais preciosos (mineração e comércio)	Critério simples	Mineração, comércio de diamantes e outras pedras e metais preciosos

Advogados	Critério Cumulativo	N/A
Transportadora maritima	Critério Simples	Propriedade e exploração de navios mercantes, corretagem e desmanche de navios
Vendas, corretagem e intermediação no campo da arte (plástica ou visual)	Critério Simples	Somente em caso de atividade professional
Recursos naturais e matérias-primas (mineração e comércio)	Critério Simples	Extração/comercialização de produtos físicos/exploração (exceto agricultura, silvicultura ou pesca)
Instituições religiosas/de líderes/políticas, incluindo seus líderes	Critério Cumulativo	N/A
Criptoativos	Critério Simples	Atividades associadas à emissão, negociação ou depósito de criptoativos e como principal fonte de riqueza ou fundos depositados
Profissional do Esporte	Critério Cumulativo	Em particular, jogadores profissionais de alto nível, seus agentes, árbitros profissionais, treinadores ou dirigentes de seleções nacionais
Indústrias Farmacêuticas, Biotecnologia e MedTech	Critério Cumulativo	Empresas e gestores (exceto varejo)
Casa de câmbio	Critério Simples	N/A

MIRABAUD

Tabela para avaliar o nível de risco para relacionamentos PEP

1. . Classificação do país com classificação inferior a 40 pela Transparência Internacional 2021	☐ sim ☐ não País: Avaliação:
2. Relatórios públicos internacionais sobre corrupção/escândalos no país/governo ou família governante (imprensa internacional, relatórios de ONGs, etc.)	☐ sim ☐ não
3. Proximidade ao governo ou família governante (ministro ou membro de gabinete ministerial, gerente de empresa pública nacional (> 50%), próximo a essa pessoa ou membro da família)	☐ sim ☐ não Descrição:
4. Um ou mais campos de atividade sensíveis do PEP (monopólio público, gerente de alto nível em empresa pública (> 50%), associado ou empregado de família governante)	☐ sim ☐ não Descrição:
5. PEP supostamente envolvido em corrupção/escândalos de acordo com relatórios públicos	☐ sim ☐ não
6. PEP há mais de cinco anos (aumento da consolidação de influência e rede potencializando o risco) ou é PEP há mais de cinco anos e deixou o cargo há menos de dois anos ou exerce atividade vinculada a tais funções públicas anteriores. 7.	☐ sim ☐ não Descrição:
Risco de Conformidade e Reputação	**Se mais de três 'sim' forem marcados, o risco de conformidade e reputação requer medidas adicionais** **/ seis 'sim' marcados**

Classificação de países em risco

O Departamento de Compliance elabora e atualiza a lista de países pelo menos uma vez por ano, levando em consideração seu GAFI, Transparência Internacional, sanções e classificações fiscais, bem como o conhecimento específico do Banco de determinados mercados em que atua. Esta lista é validada anualmente pelo Comitê Executivo.

A classificação dos países é baseada em três cores:

• Laranja: risco único
• Amarelo: risco cumulativo
• Verde: sem risco

* * *

MIRABAUD

ANEXO VI

Lista de países - (Lista em Inglês)	Sumário de Risco
Afghanistan	U
Aland Islands	S
Albania	U
Algeria	C
American Samoa	C
Andorra	S
Angola	C
Anguilla	S
Antarctica	S
Antigua and Barbuda	S
Argentina	C
Armenia	U
Aruba	C
Australia	S
Austria	S
Azerbaijan	U
Bahamas	S
Bahrain	S
Bangladesh	C
Barbados	U
Belarus	U
Belgium	S
Belize	S
Benin	C
Bermuda	C
Bhutan	C
Bolivia	C
Bonaire St Eustatius	S
Bosnia and Herzegovina	U
Botswana	S
Bouvet Island	S
Brazil	S
British Indian Ocean Territory	C
British Virgin Islands	S
Brunei Darussalam	S
Bulgaria	C
Burkina Faso	U
Burundi	U
Cabo Verde	C
Cambodia	U
Cameroon	C

Canada	S
Cayman Islands	U
Central African Republic	U
Chad	C
Channel Islands	S
Chile	S
China	U
Christmas Island	S
Cocos (Keeling) Islands	S
Colombia	C
Comoros	C
Congo	C
Cook Islands	S
Costa Rica	S
Côte D'Ivoire	U
Croatia	S
Cuba	U
Curacao	S
Cyprus	S
Czech Republic	S
Democratic Republic of the Congo	U
Denmark	S
Djibouti	C
Dominica	S
Dominican Republic	C
Ecuador	C
Egypt	C
El Salvador	C
Equatorial Guinea	C
Eritrea	C
Estonia	S
Ethiopia	U
Falkland Islands (Malvinas)	S
Faroe Islands	S
Fiji	C
Finland	S
France	S
French Guiana	S
French Polynesia	S
French Southern Territories	C
Gabon	C
Gambia	C
Georgia	S
Germany	S

Ghana	S
Gibraltar	S
Greece	S
Greenland	S
Grenada	S
Guadeloupe	S
Guam	C
Guatemala	C
Guinea	U
Guinea Bissau	U
Guyana	C
Haiti	U
Heard Island and Mcdonald Islands	S
Holy State (Vatican City State)	S
Honduras	C
Hong Kong	U
Hungary	S
Iceland	S
India	C
Indonesia	C
Iran	U
Iraq	U
Ireland	S
Isle of Man	S
Israel	S
Italy	S
Jamaica	U
Japan	S
Jordan	U
Kazakhstan	C
Kenya	C
Kiribati	C
Korea, North	U
Korea, South	S
Kosovo	C
Kuwait	S
Kyrgyzstan	C
Laos	C
Latvia	S
Lebanon	U
Lesotho	C
Liberia	C
Libya	U
Liechtenstein	S

Lithuania	S
Luxembourg	S
Macao	U
Macedonia	C
Madagascar	C
Malawi	C
Malaysia	S
Maldives	C
Mali	U
Malta	U
Marshall Islands	S
Martinique	S
Mauritania	C
Mauritius	S
Mayotte	S
Mexico	C
Micronesia, Fed. Sts.	C
Moldova	U
Monaco	S
Mongolia	C
Montenegro	S
Montserrat	C
Morocco	U
Mozambique	C
Myanmar	U
Namibia	S
Nauru	C
Nepal	C
Netherlands	S
Netherlands Antilles	C
New Caledonia	C
New Zealand	S
Nicaragua	U
Niger	C
Nigeria	C
Niue	C
Norfolk Island	S
Northern Mariana Islands	S
Norway	S
Oman	S
Pakistan	U
Palau	C
Palestine	C
Panama	U

Papua New Guinea	C
Paraguay	C
Peru	C
Philippines	U
Pitcairn	C
Poland	S
Portugal	S
Puerto Rico	C
Qatar	S
Reunion	S
Romania	C
Russia	U
Rwanda	C
Saint Helena	S
Saint Lucia	S
Saint Pierre and Miquelon	S
Saint Vincent and the Grenadines	S
Saint-Barthelemy	S
Samoa	C
Samoa (US)	C
San Marino	S
Sao Tome and Principe	S
Saudi Arabia	S
Senegal	U
Serbia	C
Seychelles	S
Sierra Leone	C
Singapore	S
Sint Maarten (Dutch part)	C
Slovakia	S
Slovenia	S
Solomon Islands	S
Somalia	U
South Africa	S
South Georgia and the South Sandwic	C
South Sudan	U
Spain	S
Sri Lanka	C
St. Kitts and Nevis	C
St. Martin (French part)	S
Sudan	U
Suriname	C
Svalbard and Jan Mayen Islands	C
Swaziland	C

Sweden	S
Switzerland	S
Syria	U
Taiwan	C
Tajikistan	C
Tanzania	C
Thailand	C
Timor-Leste	C
Togo	C
Tokelau	C
Tonga	C
Trinidad and Tobago	S
Tunisia	U
Turkey	C
Turkmenistan	C
Turks and Caicos Islands	S

Continua ...

Tuvalu	C
Uganda	U
Ukraine	U
United Arab Emirates	C
United Kingdom	S
United States Minor Outlying Islands	S
United States of America	S
Uruguay	S
Uzbekistan	C
Vanuatu	C
Venezuela	U
Vietnam	C
Virgin Islands (U.S.)	S
Wallis and Futuna Islands	S
West Bank and Gaza	C
Western Sahara	C
Yemen	U
Zambia	C
Zimbabwe	U

Risk code:	
Unique risk criteria	U
Cumulative risk criteria	C
Standard risk criteria	S

Offshore entities	
Cayman Islands	Incorporation of a domiciliary company in those jurisdiction is not considered a risk factor
Malta	
Panama	

* * *