**POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS DA M2DF PARTNERS CAPITAL LTDA.**

Data de Início da Vigência: 15 de outubro de 2025

**Política de Compliance e Controles Internos**

## 1. Introdução.

A Política de Compliance e Controles Internos da M2DF Partners Capital Ltda. ("M2DF Partners" ou "Gestora") foi elaborada em conformidade com a Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21/21"), bem como com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e o Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada, e tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam e aplicam-se à conduta de todos os sócios, administradores, diretores, funcionários, prestadores de serviços, estagiários, consultores e todos os demais dedicados à atividade de análise, gestão, operações e risco da Gestora ("Colaboradores" ou, isoladamente, "Colaborador").

No âmbito institucional e empresarial, compliance é o conjunto de procedimentos e práticas adotadas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como para evitar, detectar e tratar quaisquer desvios ou inconformidades que possam ocorrer.

A Gestora possui em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, compartilhados por todos os seus colaboradores. Na busca do seu crescimento e da satisfação dos seus clientes, com total transparência, respeito às leis, normas e aos participantes dos mercados financeiros e de capitais.

Esta Política de Compliance e Controles Internos foi desenvolvida com a finalidade de consolidar regras, princípios e diretrizes contidos nas políticas e nos manuais da Gestora, diminuindo o risco operacional e aumentando a aderência de seus Colaboradores, à regulamentação e às melhores práticas de mercado. O monitoramento do cumprimento das regras desta Política de Compliance deve ser feita pelo Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

## 2. Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

Nos termos do art. 25 da Resolução CVM nº 21/21, o Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo é responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos na referida resolução, na autorregulação da ANBIMA e pela área de Compliance e Risco da Gestora.

São suas obrigações:

**(i)** monitorar e verificar possíveis condutas contrárias a esta política;

**(ii)** verificar, no mínimo anualmente, se os Colaboradores chave, em especial os sócios controladores e os sócios diretores, estão envolvidos em processos administrativos de órgão reguladores e autorreguladores, criminais de qualquer natureza, ou ainda outros processos que possam trazer contingências para a Gestora e que, portanto, sua divulgação pública possa vir a ser necessária, nos termos da Resolução CVM nº 21/21 e da autorregulação da ANBIMA;

**(iii)** verificar se os profissionais da área de gestão estão com sua certificação ou isenção vigentes e manter a base de dados da ANBIMA atualizada;

**(iv)** atender todas as demandas dos Colaboradores da Gestora relativas a *compliance*;

**(v)** desenvolver documentos normativos que atendam as normas das reguladoras e ao bom desenvolvimento interno da Gestora;

**(vi)** implementar programas de treinamento;

**(vii)** efetuar revisões periódicas dos normativos de *compliance*, principalmente quando são realizadas alterações nos normativos vigentes;

**(viii)** assessorar a gestão dos negócios no que se refere à interpretação e impacto da legislação, e analisar, periodicamente, as normatizações emitidas pelos órgãos normativos como a CVM, ANBIMA e outros organismos congêneres e acionar as áreas responsáveis por seu cumprimento;

**(ix)** receber a manifestação do diretor responsável pela administração de carteiras de valores mobiliários a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, devendo o relatório permanecer disponível à CVM na sede da Gestora;

**(x)** incluir clientes em lista restritiva de negociação e estabelecer períodos de bloqueio, conforme avaliação de risco efetuada;

**(xi)** promover a ampla divulgação desta e das demais políticas da Gestora a todos os seus Colaboradores;

**(xii)** analisar todos os casos informados ou levantados sobre o descumprimento dos preceitos éticos e de *compliance* aqui previstos ou nos demais documentos da Gestora e proceder com as devidas medidas corretivas;

**(xiii)** garantir o sigilo de denúncias de delitos ou infrações mesmo quando não solicitadas, exceto nos casos de necessidade de testemunho judicial;

**(xiv)** solicitar, quando necessário para a análise de suas questões, o apoio da auditoria interna ou externa (autorizada pela CVM) ou outros consultores profissionais;

**(xv)** monitorar e manter atualizados os controles e políticas de gestão de risco e *compliance* da Gestora em seu website (https://m2df.com/), conforme Art. 16 da Resolução CVM nº 21/21, bem como aquelas cuja publicidade seja exigida pela ANBIMA;

**(xvi)** definir e preservar os princípios éticos a serem observados por todos os Colaboradores da Gestora constantes nesta política e no Código de Ética, zelando pela manutenção do dever fiduciário perante os clientes e investidores;

**(xvii)** definir e aplicar eventuais sanções ao não cumprimento das normas aqui definidas;

**(xviii)** realizar a gestão de controles internos, conforme estabelecido no Art. 25 da Resolução CVM nº 21/21;

**(xix)** realizar a gestão da política de prevenção à lavagem de dinheiro e não financiamento do terrorismo, implementando a política própria e seus procedimentos de forma a prevenir a ocorrência de situações atípicas e permitindo sua imediata identificação e comunicação ao COAF, conforme aplicável.

O Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo deve analisar situações de "conflitos de interesse" pessoais e profissionais, prevendo e implementando procedimentos para sua mitigação, bem como zelando pela observância das vedações normativas previstas no Art. 20 da Resolução CVM nº 21/21.

São alguns exemplos de conflitos em situações que envolvam:

**(i)** investimentos pessoais;

**(ii)** transações financeiras com clientes fora do âmbito da Gestora;

**(iii)** conflitos de interesses entre a atividade de gestão de recursos da Gestora e quaisquer outras que venham a ser por ela desempenhadas no futuro;

**(iv)** recebimento de favores/presentes de administradores e/ou sócios de empresas investidas, fornecedores ou clientes;

**(v)** análise financeira ou operação com empresas cujo Colaborador possua alguma relação pessoal;

**(vi)** operações com empresas que o Colaborador possua investimento próprio; e

**(vii)** participações em atividade política.

Cabe ressaltar que o Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo possui total autonomia no exercício de suas atividades, não sendo, de qualquer forma, subordinado à área de gestão.

## 3. Certificação Profissional.

O Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo comunicará aos Colaboradores com 3 (três) meses de antecedência a aproximação do vencimento das suas respectivas certificações, e da consequente obrigatoriedade de suas atualizações. Colaboradores cuja certificação venha a vencer durante o exercício das suas atividades deverão enviar ao Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo justificativa para tal e plano de adequação, podendo a não regularização da certificação levar ao afastamento do Colaborador.

O Diretor de Gestão de Recursos, bem como os demais Colaboradores que integrem a área de gestão e tenham poder de decisão de investimentos, deverão manter a Certificação de Gestores ANBIMA ("CGA") ativa ou obter sua isenção, nos termos das Regras e Procedimentos de Certificação da ANBIMA, o que também será monitorado pelo Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

## 4. Formulário de Referência.

O Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo deve enviar o Formulário de Referência, por meio de sistema eletrônico da CVM, até o dia 31 de março de cada ano, devendo assegurar que as informações ali contidas são verdadeiras, completas e não induzam o investidor a erro, bem como encontram-se em linguagem simples, clara, objetiva e concisa.

O Formulário de Referência deverá constar no website da Gestora (https://m2df.com/), em sua versão mais atualizada enviada à CVM. Adicionalmente, será revisto integralmente, no mínimo, anualmente, e sempre que ocorrerem alterações significativas na Gestora, sua estrutura e atividades.

Não obstante, caberá ao Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo elaborar, manter e atualizar outros formulários

regulatórios, inclusive, mas não se limitando àqueles solicitados pela ANBIMA, conforme sistema interno mantido pelo Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo, e nos termos das regulamentações aplicável às operações da Gestora.

## 5. Plano de Continuidade de Negócios.

A Gestora possui plano e recursos tecnológicos preparados para permitir a continuidade dos negócios e a consequente preservação do patrimônio dos seus clientes, na ocorrência de circunstâncias de força maior e/ou que fujam à sua capacidade de intervenção.

O plano tem o objetivo de:

**(i)** conhecer e minimizar os danos no período pós-contingência;
**(ii)** minimizar as perdas para si, seus clientes, seus sócios e colaboradores, advindos da interrupção de suas atividades;
**(iii)** normalizar o mais rápido possível as atividades de gestão.

Os passos para a execução são:

**(i)** identificação das atividades essenciais à consecução da atividade de gestão profissional de recursos de terceiros.
**(ii)** identificação da interrupção do funcionamento dos recursos;
**(iii)** comunicação imediata ao Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo;
**(iv)** comunicação aos Colaboradores com orientação sobre postura e providências cabíveis;
**(v)** ativação do plano e acesso às informações para continuidade das operações. Todos os sistemas contratados para auxiliar no processo de análise e gestão são passíveis de serem acessados de qualquer localidade.

Recursos Computacionais

Para se defender de eventuais falhas dos recursos computacionais, entendidos aqui como os computadores e sistemas de armazenagem de dados, a Gestora possui, para fins de contingência e continuidade dos negócios: computadores portáteis ("notebooks"), telefones celulares integrados com os serviços "na nuvem" da *Microsoft* e *no breaks* no caso de falta de luz.

Sede da Gestora

Em circunstâncias que tornem as instalações da Gestora inacessíveis, ou que haja necessidade de evacuação delas, o Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo deverá efetuar o deslocamento do exercício das suas atividades para algum local considerado seguro. Isto é, que possibilite a utilização da estrutura "na nuvem" de forma adequada, por meio da utilização dos notebooks e celulares próprios da Gestora, para continuidade das operações em regime móvel.

Energia Elétrica

Para fins de mitigação do impacto de falhas no fornecimento externo de energia elétrica, a Gestora possui sistemas de baterias conhecidos como "*no breaks*".. Após o acionamento dos "*no breaks*" o Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo deverá monitorar a previsão de retorno do fornecimento normal de energia elétrica, autonomia restante das baterias, e, caso entenda necessário, efetuar o deslocamento do exercício das atividades para algum local considerado seguro. Isto é, que possibilite a utilização da estrutura "na nuvem" de forma adequada, por meio da utilização dos notebooks e celulares próprios da Gestora, para continuidade das operações em regime móvel

Testes de Contingência

**(i)** testes dos *no breaks*, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
**(ii)** acesso aos dados armazenados; e
**(iii)** outros testes necessários à continuidade das atividades.

## 6. Sistema de Gerenciamento.

A Gestora utiliza soluções do Windows Office 365 para gestão de *compliance* e risco. Tal sistema disponibiliza uma matriz de atividades regulatórias (com responsabilidades e obrigações de cada área) contendo alertas para realização dos controles internos e testes de aderência para cumprimento das normas de regulação e autorregulação aplicáveis à Gestora, os quais serão realizados mensalmente pela própria equipe.

Por fim, o Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo, com auxílio dos seus assessores legais contratados, deverá conduzir uma revisão anual completa de todo programa de *compliance*, que inclui esta política, a agenda regulatória, o programa de treinamento, inclusive da própria área de Compliance e Risco, revisões de formulários e testes de aderência, detalhados em sistema interno, devendo elaborar relatório de conclusões de controles internos de que trata o Art. 25 da Resolução CVM nº 21/21.

A Gestora fornece treinamentos iniciais e contínuos aos Colaboradores. Todos os Colaboradores participarão anualmente do treino organizado pelo Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo], para capacitação sobre as normas e políticas da Gestora, assim como as atualizações sobre a regulamentação brasileira pertinente à atividade, incluindo a prevenção a lavagem de dinheiro e combate ao terrorismo.

## 7. Segurança da Informação.

As medidas de segurança da informação têm por finalidade a proteção contra ameaças, de modo a garantir a continuidade dos negócios e minimizar riscos. Tais medidas devem ser observadas por todos os Colaboradores.

Causam situações de risco à segurança da informação:

**(i)** acessar a sites não relacionados às atividades da Gestora;
**(ii)** utilizar mídias ("*pen-drives*", CDs, entre outras) para armazenamento de arquivos/dados digitais, com exceção das disponibilizadas pela Gestora;
**(iii)** acessar ou salvar informações sensíveis e informações confidenciais em pastas virtuais de acesso público;
**(iv)** salvar arquivos pessoais na rede de computadores institucional;
**(v)** utilizar mídias para transporte de informações não criptografadas; e
**(vi)** dividir senhas.

<u>Processo de Segurança da Informação e Cibernética Adotados Pela Gestora</u>

Estes serão os processos adotados pela Gestora:

**(i)** análises, controle e proteção de acessos indevidos ou ameaças que possam comprometer o negócio e/ou produto da Gestora. Para tanto, os acessos devem ser, quando possível, restritos por meio de autenticação de dois fatores da *Microsoft*,

**(ii)** adotar mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados;

**(iii)** adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades mediante sistema de armazenamento em nuvens da Microsoft One Drive;

**(iv)** adotar mecanismos para prevenir que vírus e outros tipos de *software* e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores e sistemas ou exponham a Gestora a vulnerabilidades. Para tanto, os *softwares* de segurança, como o antivírus, devem estar presentes em todos os computadores de seus Colaboradores;

**(v)** condução do plano de continuidade mencionado anteriormente; e

**(vi)** treinamentos para apresentar, explicar e esclarecer a rotina de segurança para novos Colaboradores.

Processo de Segurança da Informação e Cibernética Adotados Pela Gestora (Software de Gestão de Recursos e Armazenamento em Nuvem)

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a Gestora adota políticas e procedimentos para os processos elencados a seguir.

Gestão de Acesso

Devem ser realizadas análises, controles e proteção de acessos indevidos ou ameaças que possam comprometer o negócio e/ou produto da Gestora. Para tanto, os acessos devem ser utilizados por meio logins e senhas individuais cadastrados para todos os Colaboradores e autenticação de dois fatores da *Microsoft*. Os sistemas da Gestora devem ser utilizados tão somente para a finalidade devidamente autorizada. A Gestora deve assegurar proteção dos mesmos durante todo o seu ciclo de vida, a fim de garantir que os princípios da confidencialidade, integridade e disponibilidade sejam cumpridos integralmente.

Autenticação

A Gestora adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de acessos e funções.

Segmentação

A Gestora deve adotar mecanismos internos para a segmentação de rede (ex.: VPC), base de dados e acesso de modo a proteger seus dados de ataques cibernéticos. Para a necessidade de criação de novas regras de acesso lógico a equipe de Cibersegurança deve ser envolvida de imediato.

Controle de Acesso

A Gestora deve adotar controles de acesso em toda sua infraestrutura de sistemas para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas. Desta forma, deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados, consistentes e cofre de senha e gerenciado pela equipe responsável.

Gestão de Risco

A Gestora possui processo para análise de vulnerabilidades, ameaças e impactos sobre suas instâncias computacionais para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

Backup

A Gestora deve adotar uma rotina de *backup* e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

Proteção contra vírus, arquivos e softwares maliciosos

A Gestora deve adotar mecanismos para prevenir que vírus e outros tipos de *software* e condutas maliciosas (e.g., phishing, spam etc.) se propaguem nos computadores e sistemas ou exponham a Gestora a vulnerabilidades. Para tanto, os *softwares* de segurança, como o antivírus, devem estar presentes em todos os computadores de seus colaboradores.

Testes de varredura para detecção de vulnerabilidades

A Gestora se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e instâncias para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

**Anexo I**

Termo de Recebimento e Compromisso

Por meio deste instrumento eu, [●], inscrito no CPF/MF sob o nº [●], DECLARO para os devidos fins:

- ter recebido, na presente data, a Política de Compliance e Controles Internos atualizada da M2DF Partners Capital Ltda. ("Gestora");
- ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes na referida política;
- estar ciente de que a Política de Compliance e Controles Internos como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e
- estar ciente do meu compromisso de comunicar ao Diretor de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas na referida política.

[local], [data].

_____

**[COLABORADOR]**