Monefica Gestão de Recursos e Consultoria Financeira LTDA

Regras, Procedimentos e Descrição dos Controles Internos (Manual de Compliance)

Florianópolis, 28/03/2022

Quadro de Versões e Revisões

Responsável	Data	Resumo das Alterações
Nathalia Laffin	28/03/2022	Criação das Regras, Procedimentos e Descrição dos Controles Internos (Manual de Compliance)
Nathalia Laffin	30/07/2022	Alteração da Política para inclusão das solicitações feita em Ofício da Anbima nº 01/012765/2022
Nathalia Laffin	30/08/2022	Alteração da Política para inclusão das solicitações feita em Ofício da Anbima nº 02/012765/2022

Sumário

1. Objetivos Gerais

O presente Manual de Compliance (“Manual”) da Monefica Gestora e Consultoria Financeira (“Monefica”) tem por objetivo descrever os princípios éticos e conjunto de regramento de como os colaboradores devem atuar na sua atuação profissional.

Visa-se garantir o contínuo atendimento às normas e regulações vigentes no que tange a gestão de valores mobiliários, e atender aos mais altos padrões éticos e profissionais, assegurando que todos os profissionais que desempenham funções dentro da Gestora, atuem sempre com imparcialidade, e que tenham clareza da legislação vigente, inclusive referente a confidencialidade, segregação de atividades, lavagem de dinheiro entre outros.

Tem por objetivo também, deixar aqui descritas as informações quanto à manutenção do programa de treinamento aos profissionais da Gestora.

1.1 Abrangência

Este Manual abrange todos os administradores, colaboradores ou contratados que atuem em nome da Gestora. Estes, deverão respeitar os termos, atestando expressamente o seu conhecimento relativo as regras aqui estabelecidas.

Estes profissionais, mediante a assinatura do Anexo I, atestam que tiveram o treinamento necessário e que irão cumprir com todos os termos a partir do início do seu trabalho na Gestora.

1.2 Armazenamento e Revisões

Este documento deverá ficar saldo em servidor da Monefica e disponibilizado no site da empresa (www.monefica.com.br) em lugar visível e acessível por todos.

O Comitê de Risco e Compliance ficará responsável pela manutenção desse documento atualizado e promoverá as mudanças pertinentes. Em última instância, o Diretor de Risco e Compliance é a pessoa responsável pelos treinamentos e controle da assinatura de todos os colaboradores do Termo de Adesão e Treinamento (Anexo I).

2. Compliance e Controles Internos

A área de Risco e Compliance é a responsável pela elaboração, manutenção, revisões e atualizações periódicas do Programa de Compliance e das políticas internas, além de realizar testes de aderência a fim de se verificar a efetividade dos treinamentos aos colaboradores.

A Monefica durante o exercício de suas atividades deverá garantir, por meio desse manual, bem como treinamentos e supervisões, o permanente atendimento as políticas, normas e regulações, sempre atendendo a legislação, em especial a resolução CVM nº 21/21, bem como demais normas não ali mencionadas, mas que atendem as melhores práticas nacionais e internacionais éticas para gestão de valores mobiliários.

Esta política deve disciplinar a atuação da área de Compliance da Monefica, deliberando as responsabilidades e procedimentos a serem observados durante a atuação profissional dos colaboradores.

2.1 Atribuições

O Diretor de Risco e Compliance é o responsável, em última instância, por implementar as políticas, regras, procedimentos e controles internos da Gestora, garantindo o seu cumprimento.

É também de sua atribuição, coordenar a área de Risco e Compliance, inclusive o Comitê de Risco e Compliance com suas atribuições.

Suas principais responsabilidades são:

i) Estabelecer princípios éticos e regras de conduta, no mínimo, contemplando a legislação sobre o tema contido na Resolução CVM n. 21, o Código de Administração de Recursos de Terceiros – ANBIMA, a Resolução CVM n. 50 e a Lei Geral de Proteção de Dados.

ii) Efetuar as alterações neste Manual sempre que necessário o seu aperfeiçoamento ou adequação às novas legislações;

iii) divulgar esse Manual e demais políticas internas da Gestora, por meio eletrônico ao público em geral, além dos treinamentos para colaboradores;

iv) Fiscalizar o cumprimento deste Manual e demais políticas dentre os colaboradores no dia a dia das operações da Gestora;

v) Receber os pedidos de autorização, dúvidas relativas a Compliance ou esclarecimentos que porventura possam surgir entre os colaboradores e deliberar a respeito das providências;

vi) Receber denúncias sobre ocorrências suspeitas ou atitudes que possam estar em desacordo com este Manual e demais políticas, executar as diligências necessárias e encaminhar os resultados para os órgãos competentes, caso seja necessário, além das atitudes internas;

vii) Realizar avaliações periódicas a fim de testar a eficiência dos processos internos e controles de gerenciamento de riscos, revisando estes caso se mostrem inadequados;

viii) Acompanhar a legislação e normas emitidas por entidades reguladores ou não, como CVM e Anbima, informando as áreas e departamentos que devem se adequar;

ix) fazer cumprir as obrigações relativas ao combate aos crimes de lavagem de dinheiro e financiamento de terrorismo;

x) Aplicar as sanções e punições aos colaboradores quando cometidas irregularidades.

Quando entender necessário, o Diretor de Risco e Compliance poderá levar assuntos de sua competência para deliberação do Comitê de Risco e Compliance, em reuniões ordinárias ou extraordinárias.

3. Contratação de Prestadores de Serviços e Colaboradores

A Monefica entende que para resguardar sua reputação, é imprescindível que tenha o zelo de contratar colaboradores e prestadores de serviços que possuam reputação ilibada, bem como qualificação e as certificações que sejam necessárias para a execução de suas atividades.

Com esse objetivo, a área de Compliance deve estabelecer os procedimentos que nortearão a aprovação de colaboradores e prestadores de serviços.

Logo, a área de Compliance deverá trabalhar em conjunto com a área de recrutamento e seleção de pessoas a fim de se verificar situações de desenquadramento.

3.1 Uso de distribuidores terceirizados

O objetivo da contratação de serviços de terceiros, tem como principal razão deixar a Gestora focada na parte de gestão de valores mobiliários.

Sendo assim, poderá ser utilizado distribuidores terceirizados para captação de recursos, em acordo com o administrador, utilizando critérios como reputação, histórico de atuação, qualidade do trabalho desenvolvido, entre outros. Para isso, poderá ser renunciada parte da receita com a taxa de administração e/ou taxa de performance.

4. Política de Segurança da Informação

A presente política de Segurança da Informação visa determinar os procedimentos a serem seguidos pela Gestora a fim de garantir a segurança, tanto da informação quanto cibernética da empresa e estabelecer as medidas a serem tomadas para evitar riscos que possam deixar vulneráveis a terceiros ou que possam prejudicar a execução de suas atividades.

A área de Risco e Compliance procurou identificar os eventos com maior probabilidade de ocorrência , bem como as informações mais sensíveis e confidenciais, com o objetivo de mitigar riscos a suas atividades ou vazamento dos dados.

Nesse sentido, nenhuma informação confidencial deve ser compartilhada para colaboradores que não demandem dela para exercício de suas atividades, nem permitindo que se tenha acesso a ela.

Toda informação relativa a empresa, sócios, colaboradores ou clientes, obtidas em decorrência do desempenho das atividades da empresa, não deve ser compartilhada sob nenhuma hipótese, salvo se expresso formalmente pelo agente detentor das informações, ou excepcionalmente se autorizado pelo Diretor de Risco e Compliance.

4.1 Segurança Cibernética

É cada vez mais recorrente a utilização de ataques eletrônicos para fins de obtenção de informações confidenciais das empresas, dos seus colaboradores e de clientes. Por se tratarem de dados sigilosos, ligados a questões financeiras, é especial o interesse dentro da Gestora de proteger esses dados, salvaguardando os direitos individuais dos agentes colaboradores e clientes.

Entende-se como principais possibilidades de ataques cibernéticos a utilização das seguintes ações:

- Phishing: email ou mensagem eletrônica, normalmente simulando ser uma pessoa ou empresa confiável, captando informações pessoais da empresa ou indivíduo através de um link ou na própria mensagem;
- Pharming: direcionamento para site fraudulento, sem o conhecimento da vítima;
- Malware: softwares e programas desenvolvidos para corromper e compartilhar dados de um computador ou rede;
- Cavalo de Tróia: aparece dentro de um arquivo ou software infectado, que abre a porta para invadirem o computador ou rede;
- Vírus: software que causa danos a máquinas, redes, softwares ou banco de dados;
- Vishing: ligação onde se simula ser uma empresa ou indivíduo confiável e conhecido da vítima para obter informações confidenciais;
- Invasões (advanced persistent threats): ataques sofisticados que buscam achar fragilidades dentro de um sistema ou ambiente tecnológico para conseguir invadi-lo.

A empresa utiliza controles de acesso físico e lógico aos seus sistemas de informação. Esses controles visam garantir a identificação, autenticação e que os sistemas ou ativos da Monefica só sejam acessados por pessoas com autorização através de login e senha pessoal.

Nesse sentido, todos os colaboradores da empresa devem seguir estritamente as rotinas de redefinição de senha periodicamente, com os pré-requisitos estabelecidos de constituição, para acesso aos sistemas internos. Os eventos de login e locais acessados, são registrados e podem ser checados posteriormente. Qualquer inconsistência no acesso é acusada em servidor. Caso haja o desligamento do colaborador, ou de forma preventiva, se avalie o bloqueio do acesso, imediatamente este pode ser desativado para qualquer acesso aos sistemas da Monefica.

São adotadas as seguintes medidas, de caráter preventivo, para os riscos cibernéticos identificados:

- Backup periódico do sistema;
- Instalação e manutenção de firewall e antivírus;
- Análise de prestadores de serviço e due diligence;
- Cláusula de confidencialidade entre os colaboradores.

O monitoramento dos controles existentes contará com a participação de empresas subcontratadas especializadas em segurança cibernética, e será supervisionada

pela Administração da empresa. Estes devem ser realizados anualmente, junto aos testes de contingência a fim de permitir que a Gestora esteja apta a manter suas atividades e mitigar riscos operacionais.

Os servidores e dados da empresa são armazenados criptografados em arquivos na nuvem junto a empresa Google. Os dados são criptografados e seu acesso é restrito e controlado pelo Diretor de Risco e Compliance. Além disso, esses dados são armazenados em discos rígidos físicos, feito backup mensal dos dados (backup do backup).

4.2 Confidencialidade e Proteção de Informação

É definido como informação confidencial, toda e qualquer informação técnica, operacional, financeira, econômica, bem como demais informações comerciais, know-how, cópias, diagramas, amostras, modelos, programas de computador, informações relativas a estratégias de investimento e research, informações financeiras de clientes ou fundos geridos, planos de ação, relação de clientes, contrapartes, fornecedores, prestadores de serviços ou informações de qualquer natureza relativa a Gestora Monefica, seus sócios e clientes bem como quaisquer informações registros, cópias, físicos ou eletrônicos obtidos direta ou indiretamente em razão de sua atividade na empresa, mesmo que tais informações e dados não estejam aqui relacionados.

Todos os colaboradores devem assinar o Termo de Compromisso presente no Anexo I em que atestam:

- Manter sigilo de todas as informações confidenciais, privilegiadas, comprometendo-se a não utilizar ou reproduzir a terceiros ou colaboradores que não seja estritamente necessário para realização do seu trabalho.
- Caso o colaborador seja obrigado a divulgar informação confidencial por determinação judicial, deve comunicar a área de Risco e Compliance sobre a existência de tal determinação previamente a divulgação, limitando-se estritamente a divulgação nos limites do que foi requisitado;
- Para os objetivos dessa política, caberá ao colaborador o ônus de provar o caráter não confidencial da informação que eventualmente vazada;
- O controle de acesso a informações confidenciais de clientes se dará através da restrição do acesso as pastas, armazenadas na nuvem, que estarão contidas tais informações. Este acesso é único e individual, e que poderá ser restringido, a fim de limitar o acesso de cada colaborador a informações pelo Diretor de Risco e Compliance;
- A obrigatoriedade dos colaboradores em observar as regras aqui contidas se mantém mesmo após o desligamento deste da empresa, sujeitando a

responsabilização por eventuais vazamento de informações confidenciais nas espera cível e penal;
- Todas as informações confidenciais em posse do Colaborador, em caso de desligamento, devem ser devolvidas imediatamente a empresa;

Todos os prestadores de serviços terceirizados, que forem contratados e tiverem acesso a informações confidenciais, deverão assinar contrato com previsão de cláusula de confidencialidade com relação às informações que tiverem acesso no decorrer de suas atividades e mesmo após findo o contrato.

5. Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios da Monefica visa estabelecer os procedimentos a serem adotados em caso de contingências que possam afetar as operações e negócios.

Neste plano estão contidas as ações a serem tomadas pela equipe, designando suas funções e responsabilidades com o objetivo de mitigar os possíveis impactos negativos e que possa ser possível retomar com menor impacto e de forma tempestiva as atividades.

5.1 Principais Diretrizes

Para garantir a sua efetiva implementação, a Gestora busca mapear e saber reparar de maneira tempestiva os principais pontos de vulnerabilidade de suas instalações e sistemas, tomando medidas que visem minimizar os danos no período pós contingência, mitigar ao máximo os danos para seus clientes, sócios e colaboradores causados pela interrupção das atividades e que busquem retormar de maneira mais rápida possível a normalidade.

Nesse sentido, todos os colaboradores da Gestora deverão conhecer os procedimentos de backup e salvaguarda das informações da empresa e clientes, bem como as melhores práticas de saúde e segurança no ambiente de trabalho.

A identificação por parte de colaboradores de situações que possam por em risco a continuidade dos negócios da Gestora, devem ser informadas de imediato ao Diretor de Risco e Compliance para avaliar e tomar providências. Caso seja algo

que não possa ser postergado, o próprio colaborador deve tomar as primeiras ações a fim de impedir maiores danos.

A direção de Risco e Compliance ao receber tal comunicação relativo a evento de contingência deverá:

i) Identificar o incidência e determinar a urgência de resposta;

ii) Comunicar todos os colaboradores da empresa;

iii) Conferência dos equipamentos e sistemas sob ameaça;

iv) Tomar as atitudes necessárias para correção do problema, comunicando os responsáveis pela solução do mesmo;

v) Avaliar as medidas adotadas e redefinir os protocolos caso seja necessário.

Após a realização do protocolo pelo diretor de Risco e Compliance, e verificando que não será possível a utilização do escritório físico por razões diversas, os colaboradores poderão trabalhar à distância, de suas casas, acessando os servidores e sistemas através da internet.

Caso perdure a inviabilidade de utilização do escritório por mais de 5 dias, deve ser mantida uma reunião virtual com todos os colaboradores, diariamente, a fim de verificar acessos, dificuldades e sugestão de melhores práticas a fim de evitar que se prejudiquem as atividades profissionais da Gestora.

Com o objetivo de voltar de forma mais tempestiva possível a normalidade após evento de contingência, a empresa poderá:

i) Manter os procedimentos e operações, inclusive administrativas, durante a contingência, em espaço compartilhado de coworking;
ii) Substituição de equipamentos e sistemas danificados através de fornecedores já conhecidos;
iii) Acessar crédito bancário para despesas de contingência emergencial para compra de equipamentos ou contratação de terceiros provisoriamente para suporte;

Ademais, cabe ressaltar que os administradores fiduciários bem como custodiantes, contam com procedimentos próprios de contingência e que suportariam a continuidade dos negócios.

6. Segregação de Atividades

Como já discorrido no presente Manual, a Monefica tem como objeto de atuação a gestão de carteira de valores mobiliários de terceiros, via gestão de fundos de investimento ou sob carteiras administradas de pessoas físicas ou jurídicas, mantendo uma estrutura de pequeno porte e desenvolvendo atividades que não possam ser conflitantes entre si.

Relativo às áreas da empresa, estas apesar de ocuparem o mesmo espaço físico, até para facilitar a comunicação e desenvolvimento das atividades, tem acessos e sistemas de armazenamento diferentes conforme descrito no item 6.1 abaixo. O objetivo é que o colaborador tenha acesso somente aos documentos necessários à execução de suas funções.

Relativo a operações futuras, caso a Monefica venha a desenvolver atividade no mercado de capitais fora da parte de gestão de carteiras de valores mobiliário, essa atividade deverá ser segregada, física e em sistemas, das atividades atualmente realizadas, salvo no que for expressamente permitido pela legislação e desde que haja protocolos para segregação das atividades, a fim de manter a independência de ambas

6.1 Segregação de Instalações de Tecnologia

A Monefica dispõe de segregação de parte das instalações de tecnologia a fim de garantir a independência e evitar acesso a informações, especialmente referente a Área de Risco e Compliance, como resultados de Atas de Reuniões e votações, a fim de garantir a livre tomada de decisões.

Nesse sentido, os sistemas de armazenamento de arquivos na nuvem (Google) são segregados das demais pastas da empresa, tendo acesso exclusivo para a área de Risco e Compliance. O controle do acesso dessa pasta é de responsabilidade do Diretor de Risco e Compliance, que possui acesso a todas as pastas da empresa. Sendo assim, a área de Administração de Valores Mobiliários não possui acesso aos dados da área de Gestão de Risco e Compliance e também não possui qualquer espécie de ingerência sobre os trabalhos realizados por esta última.

7. Política de Treinamento

Esta Política de Treinamento da Monefica tem por objetivo definir os treinamentos obrigatórios a serem aplicados a todos os colaboradores, administradores e empregados em geral, especialmente aqueles com acesso a informação

confidencial e que participem do processo de decisão de investimentos, bem como os treinamentos eletivos, não obrigatórios.

A empresa incentiva a participação em treinamentos e obtenção de títulos e certificações na área em que atua, e promove a disseminação das melhores práticas entre todos da empresa.

7.1 Treinamentos Obrigatórios

Todos os administradores, colaboradores ou empregados, que desempenhem atividade dentro da gestora, devem participar do treinamento quando do início das atividades profissionais, atestando que foi instruído quando as políticas e práticas internas.

Tal participação no treinamento obrigatório, deverá ser registrado pelo colaborador dentro do Termo de Adesão ao Manual de Compliance da Monefica, onde consta especificamente sua participação no treinamento a que se refere esta política.

Entende-se que não há distinção quanto ao treinamento entre as partes, especialmente no que se refere aqueles que possuam acesso a informações confidenciais, dado que todos os colaboradores, em maior ou menor grau, deverão ter acesso a alguma informação de caráter confidencial. Logo, todos devem passar por treinamento relativo a essa questão.

Dentre as questões a serem abordadas incluem-se:

i) Política de Segurança da informação, tratando das regras de confidencialidade, processos e penalidade pelo descumprimento;

ii) Procedimentos de continuidade de negócio em caso de eventual contingência que não permita a utilização do espaço físico ou sistemas da empresa;

iii) Princípios éticos e regras de conduta;

iv) Negociação de investimentos pessoais;

Poderá ser feito em conjunto, o treinamento de PLD e FT caso assim prefira o Diretor de Risco e Compliance. Entretanto, conforme descrito no Manual específico do tema, deve-se atentar para a assinatura específica do termo de PLD e FT, não constituindo a assinatura do Anexo I deste Manual de Compliance como comprovação.

Além do treinamento obrigatório de iniciação das atividades profissionais, o treinamento deve ser promovido com periodicidade máxima anual, com todos os colaboradores, empregados e administradores com as atualizações promovidas durante os 12 meses anteriores.

7.2 Treinamentos eletivos e incentivados

A Monefica procura incentivar seus profissionais a crescerem e se desenvolverem através de cursos relacionados a área de interesse e que atuam dentro do mercado financeiro.

Nesse sentido a empresa oferece suporte financeiro para as seguintes atividades:

- Participação em cursos, seminários e afins, dentro da área de atuação do colaborador e desde que aprovados pela administração;
- Apoio para obtenção de certificações Anbima;
- Apoio para obtenção de certificações profissionais, tais quais: CGA - Anbima, CNPI - Apimec e CFP da Planejar.

Caso o profissional tenha interesse em participar, deverá enviar email para o seu superior direto na empresa, apresentando as especificidades do curso, evento ou certificação em questão, bem como porque isso seria útil para ele e para a empresa.

Para aqueles que forem aprovados, a empresa poderá solicitar que faça uma apresentação do tema para os demais colaboradores, a fim de disseminar o conhecimento na empresa.

7.3 Responsabilidades

A área de Gestão de Riscos e Compliance é a responsável pelo treinamento e monitoramento de todos os profissionais que possam ter acesso a informações confidenciais, reservadas ou privilegiadas, bem como ministrar o treinamento e manter em arquivo os termos de participação de todos os administradores, colaboradores e empregados.

8. Disposições Finais

O desrespeito as normas constituídas neste Manual, bem como as demais políticas da empresa, a legislação, regulação, ou autorregulação por parte do colaborador, podem levar, dependendo da sua gravidade, a advertência verbal, escrita ou demissão do quadro da empresa, não eximindo ainda de processos penal, civil ou trabalhista.

Tais casos de violação, serão analisados pela área de Risco e Compliance, e por última instância podem ser levados a área da Administração da empresa. Por fim, pode ser ainda, caso necessário, reportar às autoridades competentes, sendo certo que serão tratadas dentro do mais absoluto sigilo de modo a preservar os interesses da empresa e não gerar riscos de imagem, para ela e para o colaborador.

A área de Compliance deverá manter atualizada esta política e manter todos os documentos e informações exigidas pelo prazo previsto em regulamentação.

Este Manual ficará disponível na rede mundial de computadores, sempre em sua última versão atualizada, sem impedimentos de acesso por login ou senha e podendo ser visitada no site da Gestora em: www.monefica.com.br

Quaisquer denúncias, reclamações ou sugestões que envolvam o desenvolvimento das atividades da Gestora deverão ser encaminhadas para o e-mail compliance@monefica.com.br, sendo garantido o anonimato quando solicitado.

Anexo I

Termo de Adesão ao Manual de Compliance da Monefica

Eu,_____
__, inscrito(a) no CPF/MF sob o n. _____, na qualidade de _____(cargo)
da Monefica, pelo presente instrumento, atesto que recebi, li e entendi o Manual de Compliance da Monefica e confirmo que tenho conhecimento integral de todas as Políticas e procedimentos aqui constantes.

Me comprometo a cumprir integralmente e fazer cumprir a quem me incumbir, no que for aplicável, confirmando minha ciência acerca das sanções aplicáveis a cada um dos casos de violação das Políticas constantes deste Manual.

Declaro também que participei do treinamento inicial, onde foram abordadas todas as políticas e manuais internos, e que todas as dúvidas foram mitigadas.

Florianópolis, __ de _____ de 20__

_____

Assinatura