MANUAL DE CONFORMIDADE (*COMPLIANCE*) E CONTROLES INTERNOS

DA

RURAL ASSET GESTORA DE RECURSOS LTDA.
CNPJ 65.948.666/0001-11

ATUALIZADO EM ABRIL DE 2026

MANUAL DE CONFORMIDADE (COMPLIANCE)
E CONTROLES INTERNOS

O presente documento refere-se ao Manual de Conformidade (*Compliance*) e Controles Internos ("Manual") da Rural Asset Gestora de Recursos Ltda., sociedade empresária limitada, inscrita no CNPJ sob o nº 65.948.666/0001-11, com sede na cidade e Estado de São Paulo, à Rua Casa do Ator, n° 1.117, Edifício The Taj, 7° andar, conjunto 74, Vila Olímpia, CEP 04546-004 ("Gestora").

1 Introdução

O presente Manual estabelece as diretrizes e regras que devem ser observadas por todos os "Colaboradores" da Gestora, assim denominados os: (i) sócios; (ii) funcionários; e (iii) quaisquer pessoas que possuam cargos, funções ou posições na Gestora, e tem por objetivo estabelecer os procedimentos, regras de *Compliance* e controles internos da Gestora, inclusive sobre a segurança da informação e segregação de atividades, atendendo aos requisitos estipulados pela Comissão de Valores Mobiliários ("CVM"), bem como pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA").

A Gestora atuará, exclusivamente, na gestão de recursos de terceiros, exclusivamente por meio de fundos de investimento constituídos no Brasil ou no exterior geridos pela Gestora ("Fundos").

A Gestora não realiza atividades de administração fiduciária, consultoria de valores mobiliários, nem tampouco de distribuição de cotas de fundos.

Através de seu programa de *Compliance*, a Gestora busca instituir, e manter sempre atualizados e efetivos, os controles internos consistentes com a complexidade de suas atividades, garantindo a conformidade (*Compliance*) com a legislação e regulamentação vigentes aplicáveis.

Em linha com a sua política interna, a Gestora espera que cada um de seus Colaboradores realizem o seu trabalho de forma ética, legal e honesta, sempre respeitando o dever fiduciário devido aos investidores, potenciais investidores e demais participantes do mercado.

Determinadas políticas integrantes deste Manual também serão aplicáveis a familiares diretos, fundos ou clubes de investimentos e/ou sociedades direta ou indiretamente controladas ou geridas discricionariamente por Colaboradores, conforme definido nas próprias políticas deste Manual.

2 ESTRUTURA ORGANIZACIONAL

2.1. Alta Administração da Gestora

A Alta Administração, conforme conceito dado pela Resolução CVM 50, é o órgão decisório máximo da Gestora, responsável pelos assuntos estratégicos da Gestora, pela supervisão da gestão dos Fundos e pelo cumprimento de regras, políticas, procedimentos e controles da Gestora, comprometendo-se com a efetividade e adequação do presente Manual e demais políticas, manuais, procedimentos e controles internos da Gestora.

A Alta Administração da Gestora é composta por pessoas naturais que reúnem a *expertise* e a capacidade técnica para exercer suas respectivas funções, responsável pela eleição dos membros do Comitê de Risco e Compliance e do Diretor de PLD/FTP (abaixo definido), sendo que este último incorpora, também, as funções de Diretor de Risco e Compliance, bem como é o responsável por determinar as diretrizes aplicáveis à prevenção da LDFT na Gestora.

A Alta Administração é formada pelos Srs. (i) **FERNANDO RODRIGUES DE OLIVEIRA,** Diretor Presidente (CEO) da Gestora; (ii) **ANDRÉ BIAGINI DE AMORIM,** Diretor de Vice-presidente da Gestora; e (iii) **JOSÉ AMÉRICO BASSO AMARAL**, sócio da Gestora.

2.2. Diretor de Risco e Compliance

O diretor encarregado pelas políticas, regras, procedimentos e controles da empresa deverá conduzir suas atividades de forma independente, não podendo exercer quaisquer funções relacionadas à gestão dos Fundos.

O diretor indicado pela Gestora para ocupar, cumulativamente, o cargo de diretor de compliance e risco e de diretor de prevenção a lavagem de dinheiro e ao financiamento ao terrorismo e membro do Comitê de Risco e Compliance, é o Sr. **RAFAEL KYI HARADA** ("Diretor de Risco e Compliance")

São responsabilidades do Diretor de Risco e Compliance:

a. Monitorar e testar o programa de Compliance da Gestora, periodicamente, assim como manter registros e evidências destes testes;

b. Manter e atualizar o presente Manual, o Código de Ética, a Política de Compra e Venda de Valores Mobiliários, Investimentos Pessoais, e as demais políticas internas da Gestora;

c. Manter cópia atualizada do presente Manual no website da Gestora e providenciar uma cópia para cada Colaborador, anualmente e sempre que atualizado;

d. Obter ou garantir que seja obtido por terceiro competente o Formulário 'Conheça seu Colaborador' da Gestora;

e. Coordenar os treinamentos internos de Compliance e garantir que estejam atualizados em relação às leis e regulamentações aplicáveis;

f. Coordenar e acompanhar quaisquer fiscalizações regulatórias;

g. Convocar, presidir e coordenar as reuniões do Comitê de Risco e Compliance;

h. Receber e responder, em tempo hábil, todas as perguntas e dúvidas dos Colaboradores em relação ao Compliance;

i. Registrar a aderência de cada Colaborador às políticas internas da Gestora, assim como às leis e regulamentações aplicáveis;

j. Reportar todas e quaisquer ocorrências indevidas à Alta Administração da Gestora e aos órgãos reguladores competentes, quando aplicável;

k. Fazer com que sejam arquivadas as atas de reunião do Comitê de Risco e Compliance e as evidências de análises de Compliance que possam ser relevantes para futuras auditorias e fiscalizações regulatórias;

l. Elaborar o Relatório Anual de Compliance ("Relatório"), nos termos da Resolução CVM 21, de 25/02/2021. O Relatório uma vez elaborado será apresentado à Alta Administração da Gestora com as seguintes considerações:

- conclusões dos exames efetuados;

- possíveis correções sobre eventuais deficiências encontradas, com o respectivo cronograma de resolução para tais deficiências, se este for o caso; e

- manifestação do diretor responsável pela gestão dos Fundos ou, quando for o caso, do diretor responsável pela gestão de risco, a respeito das deficiências encontradas nas verificações e as medidas planejadas de acordo com cronograma específico ou as medidas efetivamente adotadas a fim de solucioná-las.

Observadas as regras aplicáveis, o Diretor de Risco e Compliance poderá delegar determinados deveres e obrigações de compliance para outros Colaboradores, devidamente qualificados e sempre de acordo com a legislação aplicável.

O Diretor de Risco e Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos administradores ou sócios da Gestora.

2.3. Comitê de Risco e Compliance

O Comitê de Risco e Compliance da Gestora é órgão responsável pelo monitoramento e controle de risco (*risk assessment*) da Gestora e é composto por pessoas naturais que reúnem a *expertise* e a capacidade técnica para exercer suas respectivas funções.

O Comitê de Risco e Compliance é formado pelo Diretor de Risco e Compliance, 01 Analista de Compliance, com a atribuição de atuar como backup do Diretor de Risco e Compliance e 01 (um) membro da equipe de gestão. As reuniões do Comitê de Risco e Compliance são presididas pelo Diretor de Risco e Compliance.

O Comitê de *Compliance* deverá se reunir, no mínimo, duas vezes durante cada ano fiscal mediante convocação do Diretor de *Compliance e Risco* e, extraordinariamente, sempre que necessário.

O Comitê de *Compliance* é o órgão responsável por (i) deliberar sobre as políticas e procedimentos da Gestora; (ii) supervisionar sua aderência e implementação; (iii) analisar o impacto e cumprimento das leis e regulamentações vigentes e aplicáveis; (iv) deliberar sobre eventual descumprimento do presente Manual, do Código de Ética e demais políticas e suas consequências; (v) apurar e tomar as medidas relativas ao gerenciamento de risco, definição de cenários de teste de estresse e limites de risco, além das demais situações que não estejam previstas nas políticas internas.

3 CONFLITOS DE INTERESSE E PRESENTES

O presente Manual dispõe sobre a política de conflitos de interesse ("Política de Conflitos de Interesse"), que tem como objetivo administrar, mitigar e, sempre que possível, eliminar todos e quaisquer reais ou potenciais conflitos de interesse advindos das atividades da Gestora e seus Colaboradores.

Conflitos de interesse podem incluir situações na qual um ou mais Colaborador(es) esteja(m) envolvido(s) em atividades ou relacionamentos que, em algum grau, sejam incompatíveis com a presente Política de Conflito de Interesses.

Nessas situações, suas condutas e decisões de investimentos podem conflitar com a sua função na Gestora, ou até mesmo afetar negativamente a sua capacidade de julgamento ou a performance de suas atividades profissionais. O Colaborador deverá, em todas as circunstâncias, exercitar conscientemente o seu julgamento antes de se comprometer a qualquer atividade ou participar em qualquer transação que possa vir a gerar um conflito.

Na condução de negócios e na execução de suas atividades, a Gestora e seus Colaboradores se comprometem a sempre estarem atentos e evitar circunstâncias em que seus interesses pessoais ou de terceiros possam conflitar ou aparentem ir em desencontro aos interesses da Gestora ou de seus clientes.

Caso um conflito de interesse venha a ser inevitável, caberá ao Diretor de Risco e Compliance (e, na sua ausência, pelos demais membros do Comitê de Risco e Compliance) realizar a análise técnica do conflito de interesse em questão, e, em sequência, tomar as medidas necessárias para reduzir ou mitigar ao máximo os seus riscos.

Caso seja verificado algum possível conflito de interesse relacionado às atividades desenvolvidas pela Gestora, seus Colaboradores e prestadores de serviços, bem como em

relação a prestadores e contrapartes dos Fundos por ela geridos, o Colaborador deverá imediatamente comunicar o potencial conflito ao Diretor de Risco e Compliance que, por sua vez, deverá:

- Entender a situação com as partes envolvidas;
- Entender quais são os interesses em jogo e se é um caso de conflito real ou em potencial; e
- Verificar formas de dirimir o conflito ou, se não for possível, de ao menos mitigá-lo.

Em última instância, o Diretor de Risco e Compliance convocará uma reunião com a Alta Administração da Gestora com a finalidade de deliberar sobre conflitos de interesse.

São exemplos de possíveis conflito de interesses:

- Determinado Colaborador (ou um parente próximo) ser proprietário ou administrador de uma empresa que negocia diretamente com a Gestora;
- Determinado Colaborador possuir função/emprego externo ou possua interesses comerciais que possam interferir com a sua capacidade de executar seu trabalho na Gestora; ou
- Determinado Colaborador (ou um parente próximo) ser acionista com influência significante, diretor, funcionário, consultor ou agente de empresa, organização ou entidade concorrente da Gestora ou que tenha negócios atuais ou prospectivos, como cliente da Gestora, fornecedora ou contratada.

É vedado aos Colaboradores o exercício de atividades externas, remuneradas ou não, que possam caracterizar conflito de interesses com os negócios da Gestora ou utilização indevida de informações, conhecimentos ou quaisquer outros meios que sejam de propriedade da Gestora.

Caso o Colaborador deseje exercer atividades externas, remuneradas ou não, deverá comunicar previamente o Diretor de Risco e Compliance para aprovação, a fim de evitar potenciais conflitos de interesses e a falta de dedicação na atuação junto a Gestora.

3.1. Presentes, Brindes e Entretenimento

Os Colaboradores da Gestora são expressamente proibidos de receber qualquer forma de vantagem (por exemplo, presentes, doações e brindes), seja de clientes, possíveis clientes, fornecedores e quaisquer terceiros que possa influenciar na sua tomada de decisão ou em suas ações dentro da Gestora.

Os Colaboradores, de forma geral, são proibidos de solicitar e são desencorajados a aceitar presentes de clientes, potenciais clientes ou parceiros que não sejam membros de suas famílias.

Os Colaboradores estão expressamente proibidos de oferecer, prometer dar, receber ou promete receber, em nome da Gestora, qualquer objeto de valor a qualquer colaborador de empresa atuante no mercado financeiro e de capitais ou órgãos reguladores, caso haja a

intenção de corrupção pública ou privada.

3.1.1. Exceções

Estão isentos dessas normas os brindes promocionais personalizados com a identificação do fornecedor ou cliente.

Refeições eventuais e brindes de valor razoável podem estar isentos destes dispositivos, devendo, em caso de dúvida, o Colaborador buscar a aprovação do Diretor de Risco e Compliance, previamente.

Para fins de esclarecimento, refeições realizadas durante o curso de uma reunião, seja na sede da Gestora ou em outro lugar, não serão consideradas como presente e sim como despesa de representação.

4 POLÍTICA DE TREINAMENTO

O presente Manual dispõe sobre a política de treinamento de Compliance ("Política de Treinamento de Compliance"), que tem como objetivo estabelecer as condições, a frequência e a importância da realização de treinamentos junto aos Colaboradores da Gestora.

O Diretor de Risco e Compliance da Gestora é encarregado de organizar, ou garantir a organização, de treinamentos, anuais e obrigatórios, de Compliance, observados os seguintes temas:

- Prevenção à Lavagem de Dinheiro;
- Anticorrupção e Confidencialidade;
- Práticas de mercado, produtos disponíveis e regulamentação aplicável; e
- Insider Trading.

Os treinamentos serão disponibilizados aos Colaboradores através de acesso online, palestras presenciais, seminários ou envio de material escrito. Os treinamentos poderão ser elaborados e realizados por Colaboradores devidamente capacitados ou por escritório de advocacia/terceiros qualificados contratados pela Gestora.

O Diretor de Risco e Compliance tem o dever de manter, ou estipular determinado Colaborador ou algum procedimento para manter o registro de todos os treinamentos realizados, bem como seus materiais e relação de Colaboradores que estiveram presentes e concluíram os treinamentos no tempo estipulado. As listas de presença e conclusão de treinamento que serão reportadas ao Comitê de Risco e Compliance. Colaboradores que não concluírem os treinamentos serão advertidos pelo Diretor de Risco e Compliance,

podendo sofrer medidas disciplinares.

Todo novo Colaborador, ao iniciar suas atividades na Gestora, deve ter acesso a todos os manuais/políticas internos e a todos os procedimentos vinculados às suas funções, aderindo expressamente a estes. O novo Colaborador também passará pelas reuniões de onboarding conduzidas pelo Diretor de Risco e Compliance. As reuniões tem como objetivo apresentar as diferentes áreas da Gestora e compreensão das políticas e diretrizes internas da Gestora.

5 POLÍTICA DE CONFIDENCIALIDADE

O presente Manual dispõe, também, sobre a política de confidencialidade ("Política de Confidencialidade"), que tem como objetivo estabelecer os termos da confidencialidade das informações da Gestora e de seus Fundos.

A confidencialidade é um dos princípios norteadores das atividades desenvolvidas dentro do mercado financeiro e de capitais. O princípio da confidencialidade deverá reger e será aplicável a todas e quaisquer informações (i) não públicas da Gestora, (ii) obtidas pela Gestora no curso de suas atividades, e (iii) recebidas de clientes, ex-clientes ou potenciais clientes ("Informações Confidenciais").

Inclui-se na definição de Informações Confidenciais todas as comunicações orais e escritas, informais ou não, independentemente do meio enviado, seja presencialmente, por carta, impressão, correio eletrônico, assim como a informações geradas no computador ou aplicativo de comunicação.

Os Colaboradores da Gestora deverão proteger a confidencialidade das Informações Confidenciais que não sejam de domínio público, informações essas que tenham obtido ou criado em função das atividades que desempenham ou desempenharam junto à Gestora.

Nenhum Colaborador poderá revelar qualquer Informação Confidencial ou informação proprietária referentes à Gestora, seus Colaboradores, clientes/investidores ou parceiros, a terceiros que não estejam autorizados a recebê-las ou sobre as quais não tenham necessidade de tomar conhecimento. A única exceção é a revelação autorizada pelo cliente/investidor ou parceiro, ou requerida por lei ou autoridade competente, como por exemplo, os órgãos fiscalizadores de supervisão, em processo legal cabível.

5.1. Proteção das Informações.

A Gestora e os seus Colaboradores reconhecem a sua obrigação de resguardar as informações sigilosas e pessoais que porventura receba ou se refiram aos seus clientes/investidores, de forma segura e confidencial.

É um compromisso da Gestora manter seguras as informações e usá-las de modo adequado, que preza pela confiança de seus clientes e Colaboradores.

Os Colaboradores também devem garantir que as informações recebidas sejam utilizadas

apenas para as finalidades para as quais foram colhidas, salvo se outro tipo de utilização for permitido por lei ou normas internas.

Informações pessoais confidenciais deverão ter o seu acesso controlado, de forma a proteger contra acessos não autorizados. As informações confidenciais, de acesso restrito, somente poderão ser compartilhadas: (i) dentro da Gestora e quando seja imperiosa para a boa condução de seus negócios; (ii) com afiliadas da Gestora e outras empresas, quando necessário para atender o cliente; e (iii) com os reguladores e/ou quando exigido por lei, norma, regulamentos ou ordem judicial emitida por um tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo; desde que, no entanto, o Comitê de Risco e Compliance seja consultado previamente para aprovação.

Quaisquer outras exceções para o compartilhamento de Informações Confidenciais, com pessoas não autorizadas, deverão ser revisadas e previamente aprovadas pelo Comitê de Risco e Compliance.

Informações sobre a Gestora e seus Fundos deverão ser disponibilizadas apenas se tiverem um propósito legítimo. O compartilhamento de informações deve ser restrito e deverá ser feito com o entendimento de que as mesmas são confidenciais e devem ser utilizadas exclusivamente para o objeto restrito para o qual foram recebidas ou concedidas.

A Informação Confidencial só pode ser usada para fins profissionais e sob nenhuma hipótese deve ser utilizada para obtenção de quaisquer vantagens pessoais. É estritamente proibida a divulgação de informação para terceiros não envolvidos ou não autorizados a recebê-la.

O serviço de e-mail da Gestora é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, o firewall de software é ativado em cada computador individual na rede de escritório. Com seus procedimentos de backup externo e acesso remoto a e-mails, a mesma pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório. O backup externo é realizado pelo serviço Google Workspace.

6 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O presente Manual dispõe sobre a política de segurança da informação ("Política de Segurança da Informação"), que estabelece a forma a ser observada por todos os Colaboradores da Gestora que, em virtude de seus cargos, funções ou posições na empresa, tenham acesso a informações relevantes, com a finalidade de assegurar a segurança dessas informações, inclusive aquelas armazenadas ou disponibilizadas nos equipamentos cedidos pela Gestora para o exercício de suas funções, sendo de sua responsabilidade a sua conservação, integridade e garantia de sua confidencialidade.

A informação é um bem essencial para a operação das atividades da Gestora e, portanto, como qualquer outro bem de propriedade da empresa, deve ser usada com diligência, ética

e profissionalismo, assim como deve ser protegida (independentemente de sua forma de armazenamento ou transmissão) por todos os Colaboradores.

A Gestora classifica suas informações de acordo com o grau de confidencialidade e criticidade para seus negócios. Todas as informações precisam estar protegidas durante seu ciclo de vida, conforme aplicável: geração, manuseio, armazenamento, transporte e descarte.

a. **Informações Públicas**: são aquelas destinadas ao público em geral, que podem ser de caráter informativo. Exemplos: informações disponíveis no website da Gestora; comunicados e apresentações institucionais e dos Fundos, destinadas aos clientes/investidores e parceiros, informações genéricas sobre os Fundos e companhias investidas (desde que não sejam consideradas como informações internas e/ou confidenciais);

b. **Informações Internas**: são aquelas destinadas ao uso dos Colaboradores da Gestora, que só devem circular e ser compartilhadas internamente a quem tem necessidade de ter acesso (*need to know basis*). A divulgação externa não intencional não causaria danos à Gestora, aos investidores ou Colaboradores. Exemplos: atas de comitês internos; relatórios internos; cartas e notificações de órgãos reguladores e autorreguladores cujo conteúdo não seja crítico para os negócios da Gestora.

c. **Informações Confidenciais**: correspondem a mais alta classificação de segurança para as informações que transitam na Gestora. Refere-se a informações cuja divulgação não autorizada poderia potencialmente causar danos substanciais, constrangimentos ou penalidades à Gestora, seus investidores, Colaboradores, companhias investidas ou mesmo companhias alvo dos Fundos geridos e que estão inteiramente sujeitas à Política de Confidencialidade prevista acima. Exemplos: informação antecipada e não autorizada de operações, tais como fusões e aquisições; novos produtos e/ou serviços; informações protegidas por sigilo legal; informações sigilosas relativas aos Fundos, companhias investidas e/ou seus negócios; informações societárias e/ou de remuneração dos Colaboradores; etc.

Além disso, a Gestora implementa um ***programa de segurança cibernética*** que inclui:

I. Identificação/avaliação de riscos (risk assessment). A Gestora realiza uma avaliação de riscos regular e abrangente para identificar os riscos internos e externos. Esta avaliação inclui a identificação de todos os ativos relevantes da Gestora, sejam equipamentos, sistemas, processos ou dados, usados para seu correto funcionamento. Além disso, a Gestora avalia as vulnerabilidades dos ativos em questão, identificando as possíveis ameaças e o grau de exposição dos ativos a elas. Vários cenários são considerados nessa avaliação, incluindo os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, que devem ser monitorados:

a) Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;

c) Pharming;
d) Phishing scam;
e) Vishing;
f) Smishing;
g) Acesso pessoal;
h) Ataques de DDoS e botnets; e
i) Invasões (advanced persistent threats).

II. Monitoramento e testes. A Gestora implementa um programa de monitoramento e testes para detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico. Isso inclui a criação de mecanismos de monitoramento de todas as ações de proteção implementadas, a manutenção de inventários atualizados de hardware e software, a realização de testes de invasão externa e phishing, e a análise regular dos logs e as trilhas de auditoria criados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Para garantir as regras mencionadas nesta Política, a Gestora deverá (a) Para os riscos associados,c onduzir treinamentos e campanhas periódicas, bem como testes de Phishing e outros, (b) Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;(c) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; (d) Testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, ao menos anualmente.

III. Criação do plano de resposta. A Gestora mantém um plano de resposta a incidentes de segurança cibernética, que inclui a comunicação interna e externa necessária em caso de incidente. Este plano é revisado e atualizado regularmente para garantir que permaneça eficaz e relevante para as necessidades da Gestora. O plano de ação conta com mecanismos que asseguram a comunicação imediata para todos os colaboradores relevantes com relação a incidentes que possam gerar riscos à empresa, e prevê o acionamento dos colaboradores-chaves e contatos externos relevantes, inclusive de reguladores, considerando critérios e prazos vigentes, quando aplicável:

- Procedimento em caso de incidente.

  Uma vez que o Diretor de Risco e Compliance tenha sido acionado devido a um potencial incidente, este deverá atuar em conjunto com a área de TI para solução imediata do problema.

• Avaliação Inicial.
Na etapa inicial, aspectos e decisões fundamentais deverão ser analisadas e tomadas após o incidente. Deverá ser realizada uma análise do que aconteceu, compreendendo motivos e consequências imediatas, bem como a gravidade da situação, devendo ser decidido a formalização ou não do incidente.

• Incidente Caracterizado
Se for caracterizado um incidente, devem ser tomar as medidas imediatas, que poderão abranger (i) se será registrado um boletim de ocorrência ou queixa crime, (ii) se há necessidade de informar à CVM, ANBIMA ou mais alguma autoridade, (iii) se é necessário envolver consultor ou advogado externo; (iv) se haverá comunicação interna ou externa, em especial a Investidor que eventualmente tenha sido afetado; e (v) se houve prejuízo para a Gestora, algum veículo de investimento ou investidor específico. Além disso, caso seja necessário, deverão ser definidos os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

• Recuperação
Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados, caso necessário. Será realizado um acompanhamento, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados. Colaboradores externos relevantes deverão ser mantidos atualizados, caso seja necessário.

• Retomada
Por fim, essa fase é a de transição ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. Ademais, após eventual evento de contingência, o Diretor de Risco e Compliance deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

• Testes de Contingência
Os Testes de Contingência serão realizados com periodicidade mínima anual ou em virtude das mudanças ocorridas na Gestora que assim o justifiquem, de modo a permitir que a Gestora esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

O objetivo do teste incluirá a avaliação se o Plano desenvolvido é capaz de suportar,

de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Gestora e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se o Plano pode ser ativado tempestivamente.

Os testes abrangerão os seguintes eventos, apenas de forma amostral, a saber:

- Testes dos nobreaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
- Acesso aos sistemas e aos e-mails remotamente, de endereço externo;
- Acesso aos dados armazenados externamente; e
- Outros necessários à continuidade das atividades.
- O resultado de cada teste será registrado no documento de Teste de Contingência.

IV. Governança. A Gestora mantém o programa de segurança cibernética continuamente atualizado garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida. O Comitê de Risco e Compliance tem como uma de suas funções tratar de segurança cibernética dentro da Gestora, a revisão periódica do programa de segurança cibernética, a promoção e disseminação da cultura de segurança com a criação de canais de comunicação internos eficientes, e a definição e manutenção de indicadores de desempenho (*key performance indicators*).

Caso algum Colaborador identifique a conservação inadequada, utilização indevida de qualquer ativo (físico ou eletrônico) ou sistemas, deverá comunicar a ocorrência ao Diretor de Risco e Compliance.

O Diretor de Risco e Compliance será o responsável pela revisão da política cibernética e suas revisões, bem como para tratar e responder questões de segurança cibernética dentro da Gestora.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Diretor de Risco e Compliance, devendo ser observado o procedimento previsto nesta Política em caso de vazamento de informação confidencial.

O Diretor de Risco e Compliance irá se consultar com setor de tecnologia de informação, tendo como objetivo a supervisão e monitoramento das regras de Segurança Cibernética, conforme aqui previsto.

Um plano de contingência e a continuidade dos sistemas e processos operacionais críticos deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a

necessidade de planos de contingência, serão previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

A Gestora exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Caso algum Colaborador identifique a conservação inadequada, utilização indevida de qualquer ativo (físico ou eletrônico) ou sistemas, deverá comunicar a ocorrência ao Diretor de Risco e Compliance.

6.1. Descrições e Características

Todos os computadores utilizados pelos Colaboradores deverão ser entregues com senhas individuais e de modo a permitir a identificação do seu usuário recente. A administração de acesso à informação centralizada é submetida ao departamento de Compliance com o devido controle de contas e senhas.

Os computadores, também, são configurados com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, inclusive mas não se limitando a segregação das funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Todos os arquivos armazenados nos servidores utilizados na Gestora são objeto de backup diário, protegidas por *firewall* de última geração e sistema antivírus atual.

Os backups são feitos de forma automática diariamente com sistema proprietário da Gestora, bem como por ferramenta de armazenamento em nuvem Google Cloud. A Gestora possui serviço de backup e *restore* de arquivos, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

A Gestora mantém por 5 anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados. Nesse sentido, através dos logs realizados, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas.

Todas as declarações de imprensa (envolvendo ou não a Gestora) deverão ser previamente aprovadas pelo Diretor de Risco e Compliance que, a qualquer tempo e sem aviso prévio, poderá verificar o conteúdo das ligações telefônicas gravadas, dos arquivos disponíveis no diretório interno e dos e-mails enviados e recebidos, sem que isto configure quebra de sigilo,

para fins de monitoramento do fiel cumprimento das normas de Compliance e normativos legais pertinentes à gestão de fundos de investimento.

O descarte de Informações Confidenciais armazenadas em forma digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos em meio físico que não necessitem ser arquivados e que contenham Informações Confidenciais deverá ser realizado imediatamente após seu uso de forma a evitar sua recuperação ou leitura.

Quando for o caso, para impedir a comunicação entre determinados Colaboradores ou áreas, as áreas de Compliance e tecnologia, em conjunto, poderão implementar barreiras de informações para preservar a confidencialidade de determinadas Informações Confidenciais e impedir sua comunicação entre áreas da Gestora. Os Colaboradores não devem comunicar Informações Confidenciais sujeitas a barreiras de informação a outras áreas, sem aprovação prévia do Diretor de Risco e Compliance.

A Gestora deverá Proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado.

7 PROCEDIMENTO DE TESTES PERIÓDICOS

O Diretor de Risco e Compliance deverá realizar, ou garantir que serão conduzidos testes de Compliance ao longo do ano fiscal, com o condão de identificar e mitigar eventuais riscos aos quais a Gestora possa estar exposta e a assegurar a conformidade com a legislação, regulamentação, políticas e procedimentos internos da Gestora, além de realizar um teste periódico específico de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

O Diretor de Risco e Compliance deverá emitir um relatório para cada teste de Compliance realizado, contendo as recomendações a respeito de eventuais deficiências identificadas, assim como o estabelecimento de cronograma de saneamento, quando aplicável. Os relatórios deverão ser reproduzidos no Relatório.

O Relatório deverá observar e conter os seguintes elementos:

1) Análise e verificação dos requisitos de reputação ilibada dos Diretores e dos controladores da Gestora; Análise e verificação de eventuais ajustes realizados em políticas e documentos da Gestora, originados de: (i) mudanças regulatórias; (ii) exigências das autoridades reguladoras; (iii) como consequência de mudanças internas, decisões gerenciais, ou de apontamentos recebidos no âmbito de processos de *due diligence*;

2) Análise e verificação do descumprimento dos Códigos e demais políticas internas da Gestora por parte dos Colaboradores, restando claro que deverá ser relatado como foi equacionado a referida ocorrência de desvios profissionais mais graves, se estes resultaram em sanções e/ou consequências (financeiras, comerciais, de imagem) à Gestora

e ao Colaborador em questão, devendo-se destacar as medidas tomadas para sua prevenção futura;

3) Confirmação que o programa de treinamento dos Colaboradores, previamente estabelecido, foi devidamente cumprido, conforme indicado no item 4 do presente Manual;

4) Confirmação que a Política de Conflitos de Interesse está sendo cumprida de forma eficaz, conforme indicado no item 3 do presente Manual;

5) Confirmação que a Política de Confidencialidade é eficaz, bem como da existência de testes periódicos de segurança dos sistemas;

6) Confirmação que a Política de Gestão de Risco (determinado em manual próprio) foi cumprida, e se está adequada às normas e regulamentos;

7) Relato de eventuais desvios e desenquadramentos ocorridos no cumprimento do mandato pelo respectivo administrador dos Fundos, e quais medidas foram adotadas;

8) Indicação de que a atuação de terceiros contratados para a prestação de serviços está adequada, inclusive quanto à sua qualificação. Caso cabível, deve-se apontar eventuais rupturas de contratos que tenham sido motivadas por situações que eventualmente representavam riscos aos fundos de investimento da Gestora e aos investidores/clientes da empresa; e

9) Apresentação de estatísticas dos eventos ocorridos ao longo do ano, seu diagnóstico e aprimoramentos, no que diz respeito aos riscos operacionais.

A Gestora possui uma sistemática de processos internos para inclusão de todas as rotinas e procedimentos relacionados ao cumprimento do quanto disposto na regulamentação em vigor e em sua Política de Gestão de Risco.

Todas as rotinas e procedimentos da área de Gestão de Risco deverão variar de acordo com o tipo de risco envolvido, considerando a operação objeto do controle. A área de risco atuará de forma preventiva e constante para alertar, informar e solicitar providencias ao gestor em frentea eventuais desenquadramentos de limites normativos e daqueles estabelecidos internamente pela Gestora.

8 PROCEDIMENTO INTERNO DE REPORTE DE VIOLAÇÕES À CVM

O presente Manual dispõe sobre o procedimento interno de reporte de violações à CVM ("Procedimento"), que estabelece normas e procedimentos, a serem utilizados por todos os Colaboradores que tenham acesso a informações relevantes sobre a Gestora ou sobre suas estratégias de investimento com a finalidade de assegurar a comunicação à CVM de quaisquer violações às regulamentações emitidas por esta autarquia.

Os Colaboradores deverão comunicar imediatamente ao Diretor de Risco e Compliance a identificação ou suspeita de quaisquer violações.

No caso de violações relativas à legislação expedida pela CVM, o Diretor de Risco e Compliance, deverá analisar o cadastro, as operações ou transações pertinentes, e, decorrido todos os prazos para regularização de eventual situação de não conformidade ou após todas as análises a suspeita se confirmar, deverá apresentar um relatório sobre o caso, com recomendação de comunicação ou não ao Conselho de Controle de Atividades Financeiras ("COAF") - que é a unidade de inteligência financeira do Brasil, ao Comitê de Risco e Compliance que deliberará sobre a comunicação ao COAF.

A convicção de ilicitude não é condição para que o Comitê de Risco e Compliance determine que se proceda a comunicação de uma operação suspeita ao COAF, sendo apenas necessário que o Comitê de Risco e Compliance consiga firmar uma consistente e fundamentada convicção de sua atipicidade.

Após a devida deliberação do Comitê de Risco, caberá ao Diretor de Risco e Compliance realizar a comunicação ao COAF, dentro do prazo regulatório, das transações ou propostas de transação que constituam ou possam constituir sérios indícios de infração.

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

a. data de início e natureza do relacionamento com a Gestora;

b. explicação fundamentada dos sinais de alerta identificados; descrição e o detalhamento das características das operações realizadas;

c. apresentação das informações obtidas por meio das diligências previstas Resolução CVM nº 50 de 31 de agosto de 2021, que qualifiquem os envolvidos, inclusive informando tratar-se, ou não, de PPE, e que detalhem o comportamento da pessoa comunicada; e

d. conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada ao COAF.

Os registros das conclusões de suas análises acerca de operações ou propostas que fundamentaram a decisão de efetuar, ou não, as comunicações de que trata esta seção devem ser mantidas pelo prazo de 5 (cinco) anos, ou por prazo superior que venha a ser expressamente determinado pela CVM, em caso de processo administrativo.

Caso a Gestora não preste comunicação ao COAF no decorrer de um determinado ano civil, deverá informar à CVM, até o último dia útil do mês de janeiro do ano imediatamente subsequente, por meio de sistema eletrônico disponível no site da CVM, a não ocorrência de transações ou propostas de transações passíveis de comunicação no

referido ano civil findo.

9 SEGREGAÇÃO DE ATIVIDADES

Inicialmente, cumpre esclarecer que a Gestora atua exclusivamente como gestora de fundos de investimento, com foco em fundos de investimento de participações, na categoria de gestão de recursos, não prestando, portanto, quaisquer outros serviços no mercado de capitais.

Em razão disso, não é suscitada qualquer hipótese de conflito no nível da Gestora. Não obstante, a Gestora manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

A segregação de atividades é um requisito essencial para que seja dado o efetivo cumprimento às suas estratégias de administração de recursos de terceiros.

O Diretor de Risco e Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos Diretores ou demais sócios da Gestora.

A Área de Compliance atua de forma autônoma e independente, se reportando ao Diretor de Risco e Compliance.

A Gestora adota um conjunto de procedimentos estabelecidos pelo Diretor de Risco e Compliance, com o objetivo de proibir e impedir o fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou Colaboradores, da instituição que não estejam diretamente envolvidos na atividade de administração de recursos de terceiros.

A Gestora realizará os melhores esforços para que a segregação das informações e suas atividades sejam sempre preservadas. Com o intuito de assegurar a completa segregação, os seguintes procedimentos operacionais serão adotados:

I. Instalação física própria com limitação de acesso de terceiros;

II. A segregação informacional absoluta e inviolável da Gestora e qualquer sociedade que os Colaboradores tenham relacionamento;

III. A preservação de informações confidenciais por todos os seus Colaboradores, proibindo a transferência de tais informações a pessoas não habilitadas ou que possam vir a utilizá- las indevidamente, em processo de decisão de investimento, próprio ou de terceiros;

IV. A implantação e manutenção de programa de treinamento de Colaboradores que tenham acesso a informações confidenciais e/ou participem de processo de decisão de

investimento; e

v. O acesso restrito a arquivos, bem como à adoção de controles que restrinjam e permitam identificar as pessoas que tenham acesso às informações confidenciais.

Dessa forma, a Gestora acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, buscando servir adequadamente seus clientes e cumprir com suas obrigações.

10 CONSIDERAÇÕES FINAIS

Este Manual não substitui a obrigação que cada Colaborador tem de usar o bom senso, discernimento e de, sempre que necessário, em caso de dúvidas, contatar o Diretor de Risco e Compliance diretamente ou através do e-mail compliance@ruralasset.com.br .

Quaisquer solicitações de exceções às regras descritas neste Manual devem ser encaminhadas ao Diretor de Risco e Compliance, que verificará a solicitação e determinará a necessidade (ou não) de encaminhá-la ao Comitê de Risco e Compliance. O Comitê de Risco e Compliance por sua vez possui amplos poderes para aprovar exceções a este Manual, desde que a razão, natureza, prazo, e outras informações importantes sobre a decisão sejam devidamente formalizadas, sempre respeitando as leis e regulamentações aplicáveis.

Mediante a contratação/início do relacionamento profissional, e anualmente, todos os Colaboradores deverão aderir a este Manual através do preenchimento e assinatura do Formulário 'Conheça seu Colaborador' que será disponibilizado pelo Diretor de Risco e Compliance.

A versão atualizada do Manual deverá ser aprovada pelo Comitê de Risco e Compliance e, subsequentemente, divulgada a todos os Colaboradores e no website da Gestora www.ruralasset.com.br

* * * * *