SOD CAPITAL LTDA.

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

FEVEREIRO/2025

ÍNDICE

INTRODUÇÃO

1.1. Sumário

Este Manual de Regras, Procedimentos e Controles Internos ("Manual"), elaborado em conformidade com o disposto (i) no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, (ii) na Resolução da Comissão de Valores Mobiliários ("CVM") n.º 21, de 25 de fevereiro de 2021 ("Resolução CVM n.º 21"), (iii) no Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais - ANBIMA de Ética ("Código ANBIMA de Ética"), (iv) no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), bem como nas Diretrizes e Deliberações do Código de Ética da ANBIMA e demais orientações da CVM aplicáveis aos gestores de recursos de terceiros, tem por objetivo estabelecer regras, normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a **SOD CAPITAL LTDA.** ("Gestora"), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Na busca incessante da satisfação dos clientes, a Gestora atua com total transparência, respeito às leis, normas e aos demais participantes do mercado financeiro e de capitais.

Assim sendo, o presente Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando o atendimento de padrões éticos cada vez mais elevados. Este documento reflete a identidade cultural e os compromissos que a Gestora assume nos mercados em que atua.

A Gestora e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, gênero, deficiência física ou qualquer outra forma de preconceito que possa existir.

A Gestora mantém versões atualizadas do presente Manual em seu website.

1.2. Aplicabilidade do Manual

O presente Manual aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na Gestora, possam ter ou vir a ter acesso às informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.3. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Recebimento e Compromisso"), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Gestora foram apontadas no **Anexo III** do presente Manual.

1.4. Termo de Recebimento e Compromisso

Todo Colaborador, ao receber este Manual, firmará o Termo de Recebimento e Compromisso. Por meio desse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual e com as normas, princípios, conceitos e valores aqui contidos; comprometendo-se a zelar pela aplicação das normas de *compliance* e princípios nele expostos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da Gestora, deverá ser levado para apreciação do Diretor de Compliance, Risco e PLD, conforme abaixo definido, de acordo com os procedimentos estabelecidos neste Manual. Competirá ao Diretor de Compliance, Risco e PLD aplicar as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar o Diretor de Compliance, Risco e PLD sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Gestora, bem como zelar pela reputação da empresa. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, Risco e PLD, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

1. Introdução

1.1 Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor estatutário da Gestora indicado como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretor de Compliance, Risco e PLD"), nos termos da Resolução CVM n.º 21.

São obrigações do Diretor de Compliance, Risco e PLD:

(i) acompanhar as políticas descritas neste Manual;

(ii) levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade da Gestora para apreciação dos administradores da Gestora;

(iii) atender prontamente todos os Colaboradores;

(iv) identificar possíveis condutas contrárias a este Manual;

(v) centralizar informações e revisões periódicas dos processos de *compliance*, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;

(vi) assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a CVM e outros organismos congêneres;

(vii) elaborar relatório **anual** listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Combate e Prevenção à Lavagem de Dinheiro da Gestora;

(viii) encaminhar aos órgãos de administração da Gestora, até o **último dia útil do mês de abril** de cada ano, relatório referente ao ano civil imediatamente anterior

à data de entrega, contendo: ***(a)*** as conclusões dos exames efetuados; ***(b)*** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e ***(c)*** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM na sede da Gestora;

(ix) definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;

(x) promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;

(xi) apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de compliance previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

(xii) garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;

(xiii) solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;

(xiv) aplicar as eventuais sanções aos Colaboradores; e

(xv) analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- investimentos pessoais;

- transações financeiras com clientes fora do âmbito da Gestora;

- recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;

- análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;

- análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou

- participações em alguma atividade política.

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Gestora, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual, deverá informar o Diretor de Compliance, Risco e PLD, para que sejam tomadas as providências cabíveis.

O Diretor de Compliance, Risco e PLD poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de compliance e de risco, com as atribuições a serem definidas caso a caso, a depender da necessidade da Gestora em razão de seu crescimento e de acordo com a senioridade do Colaborador.

1.2 Comitê de Compliance e Risco

A Gestora possuirá um Comitê de Compliance e Risco, que será composto ordinariamente pelo Diretor de Compliance, Risco e PLD e pelos demais membros da Equipe de Compliance e Risco (abaixo definida) escolhidos pelo Diretor de Compliance, Risco e PLD, podendo também contar com a participação do Diretor de Investimentos da Gestora ("Diretor de Investimentos"), conforme definido em seu contrato social, ou de outros membros da equipe de gestão, a serem convocados de acordo com a pauta prevista da reunião, e deverá e averiguar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos da Gestora, entre outros assuntos relacionados à área conforme descrito abaixo, além dos demais assuntos pertinentes à gestão de risco das carteiras, conforme Política de Gestão de Risco da Gestora.

São atribuições do Comitê de Compliance e Risco da Gestora relacionadas a este Manual:

- analisar eventuais situações pelo Diretor de Compliance, Risco e PLD sobre as

atividades e rotinas de compliance;

- revisar as metodologias e parâmetros de controle existentes; e

- analisar eventuais casos de infringência das regras descritas neste Manual, nas demais políticas e manuais internos da Gestora, das regras contidas na regulamentação em vigor, ou de outros eventos relevantes e definir sobre as sanções a serem aplicadas.

As reuniões do Comitê de Compliance e Risco serão realizadas semestralmente, ou sob demanda, e suas deliberações serão consignadas em atas e/ou registradas por e-mail e arquivadas na sede da Gestora, as quais deverão ser mantidas arquivadas, disponíveis aos órgãos reguladores, por, no mínimo, 5 (cinco) anos.

1.3 Garantia de Independência

Os Colaboradores que desempenharem as atividades de risco e *compliance* formarão a Equipe de Compliance e Risco, sob a coordenação do Diretor de Compliance, Risco e PLD, sendo certo que a Equipe de Compliance e Risco exerce suas atividades de forma completamente independente das outras áreas da Gestora e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

1.4 Dúvidas ou ações contrárias aos princípios e normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da Gestora, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de *compliance* e princípios que orientam as ações da Gestora.

Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, também é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance, Risco e PLD, para obtenção de orientação mais adequada.

Mesmo que haja apenas a suspeita de potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da Gestora, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Gestora e reforçar os seus princípios éticos.

Para os fins do presente Manual, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, Risco e PLD, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da Gestora, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance, Risco e PLD, exclusivamente por meio de e-mail.

1.5 Acompanhamento das Políticas descritas neste Manual

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, que cheguem ao conhecimento do Diretor de Compliance, Risco e PLD, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de Compliance, Risco e PLD utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelo Diretor de Compliance, Risco e PLD, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance, Risco e PLD julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Gestora.

Adicionalmente, será realizado um monitoramento **anual**, a cargo do Diretor de Compliance, Risco e PLD, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, Risco e PLD, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

O Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

A Gestora realizará inspeções com periodicidade **anual**, a cargo do Diretor de

Compliance, Risco e PLD, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, sendo tal inspeção realizada de forma aleatória.

Adicionalmente, o Diretor de Compliance, Risco e PLD deverá ainda verificar **anualmente** os níveis de controles internos e *compliance* junto a todas as áreas da Gestora, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, o Diretor de Compliance, Risco e PLD poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

1.6 Sanções ("*Enforcement*")

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade Diretor de Compliance, Risco e PLD, garantido ao Colaborador, contudo, amplo direito de defesa. Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Gestora, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Gestora, nesse último caso, nos termos do art. 482 da Consolidação das Leis do Trabalho – CLT, sem prejuízos do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

A Gestora não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Gestora venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, pode exercer o direito de regresso em face dos responsáveis.

1.7 Dever de Reportar

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento ao Diretor de Compliance, Risco e PLD. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. Além disso, todos os

comunicados e investigações serão tratados de maneira confidencial, na medida do possível nestas circunstâncias. Contudo, o Colaborador que se omitir de tal obrigação poderá sofrer além de ação disciplinar, demissão por justa causa, conforme regime jurídico.

2. Política de Confidencialidade

2.1 Sigilo e Conduta

As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na Gestora, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no **Anexo II** ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no **Anexo IV** deste Manual) e de *compliance* da Gestora.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da Gestora, incluindo:

a) *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

b) informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;

c) operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Gestora;

d) estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

e) informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;

f) informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

g) transações realizadas e que ainda não tenham sido divulgadas publicamente; e

h) outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados.

Sem prejuízo da colaboração da Gestora com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de Compliance, Risco e PLD, para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading*, Dicas ou *Front-running*.

Insider Trading e "Dicas"

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

Front-running significa a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antecipadamente às operações principais, isto é, antes de uma operação de compra ou venda, da qual tem conhecimento, o Colaborador se antecipa e executa a ordem.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a Gestora, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, Risco e PLD, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance, Risco e PLD anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável, incluindo eventual demissão por justa causa.

3. Políticas de Treinamento

3.1 Treinamento e Processo de Reciclagem

A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, especialmente aqueles que tenham acesso às Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Assim que cada Colaborador for contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Gestora e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Neste sentido, a Gestora adota um programa de reciclagem **anual** dos seus Colaboradores, à medida que as normas, princípios, conceitos e valores contidos neste Manual sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

3.2 Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de Compliance, Risco e PLD e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Gestora, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas neste Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo III** deste Manual.

O Diretor de Compliance, Risco e PLD poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.

4 Políticas de Segurança e Segurança Cibernética

As medidas de segurança da informação têm por finalidade preservar o sigilo, a integridade e a disponibilidade das informações da Gestora contra uma série de riscos, como fraude, violação da privacidade e interrupção de serviço e assim minimizar as ameaças aos negócios da Gestora e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Diretor de Compliance, Risco e PLD, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

4.1 Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua

vulnerabilidade;

- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);

- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

4.2 Objetivos da Segurança da Informação

Confidencialidade: Garantir que as Informações Confidenciais (conforme definidas no Manual de Conduta e Ética) tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: Garantir que as informações sejam mantidas íntegras, sem modificações indevidas, seja acidental ou proposital;

Valor: A informação deve ter um valor agregado para a instituição;

Disponibilidade: Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

4.3 Classificação dos Dados

Toda classificação de dados deve ser realizada no momento que a informação for gerada ou, sempre que necessário, em momento posterior. É preciso saber claramente quais são os dados que estão sendo manipulados e o seu propósito, além de garantir a sua proteção.

O nivelamento da classificação aprovado pelo Comitê de Segurança da Informação, se apresenta da seguinte maneira:

- Público - todo o conteúdo de todos os documentos é visualizado por qualquer colaborador da Gestora.

- Restrito - o acesso ao conteúdo é restrito a determinadas áreas ou funções dentro da Gestora.

- Sigiloso - o acesso ao conteúdo é exclusivo às pessoas a quem for atribuída permissão específica.

Grau de sigilo	**Impacto causado pela quebra da confiabilidade**
Público	Sem impacto
Restrito	Dano médio, podendo ocasionar dano colateral não desejado
Sigiloso	Dano grave/severo, podendo causar sérios danos à instituição (afetando a imagem, gerar prejuízo financeiro, impactar nas operações e inviabilizar objetivos estratégicos).

Para a realização da classificação devem ser considerados quatro aspectos importantes, são eles:

- **Integridade** - informação atualizada, completa e mantida por pessoal autorizado.

- **Disponibilidade** - disponibilidade constante e sempre que necessário para pessoal autorizado.
- **Valor** - a informação deve ter um valor agregado para a instituição.
- **Confidencialidade** - acesso exclusivo por pessoal autorizado.

4.4 Ações de Prevenção e Proteção

Após a identificação dos riscos, a Gestora adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta:

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) 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 confidenciais.

O uso de pen drives deve estar bloqueado na gestora devido aos riscos significativos que eles representam para a segurança de dados e a integridade dos sistemas. Como dispositivos portáteis de armazenamento, os pen drives são facilmente suscetíveis à perda, roubo ou uso indevido, o que pode levar ao vazamento de informações confidenciais, como dados de clientes, estratégias financeiras ou informações sensíveis da Gestora.

Essas medidas visam proteger a empresa contra perdas de dados, roubo de informações e ataques de malware provenientes de dispositivos não autorizados. As informações sobre o uso devem ser consultadas na Política de Gestão de Ativos da Gestora.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. 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.

A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Equipe de Compliance e Risco deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Ademais, fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente Informações Confidenciais.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora.

Cada Colaborador é responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, 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 pelos administradores da Gestora.

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

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora.

A visualização de *sites*, *blogs*, *fotologs*, *webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

- Acesso Escalonado do Sistema

O acesso como "administrador" de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance, Risco e PLD e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Gestora necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação

- Senha e Login

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. O uso de autenticação multifator (MFA) deve estar habilitado e configurado como imposto para todos os colaboradores. O MFA dificulta significativamente o acesso não autorizado, mesmo em casos onde a senha tenha sido comprometida. Essa abordagem é eficaz contra ataques como phishing, roubo de credenciais e tentativas de login maliciosas.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

- Uso de Equipamentos e Sistemas

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

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de Compliance, Risco e PLD.

- Acesso Remoto

A Gestora permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e assinatura de termo de compromisso assegurando o cumprimento das diretrizes de segurança impostos pela SOD Capital.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance, Risco e PLD qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

- Controle de Acesso

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelo administrador da Gestora.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o

desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

- *Firewall, Software*, Varreduras e *Backup*

A Gestora utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLD é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Gestora mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras e *Pen Tests*, no mínimo, **anuais** para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora.

A Gestora utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Compliance, Risco e PLD é responsável por patches regulares nos sistemas da Gestora.

A Gestora mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLD. As informações da Gestora são atualmente objeto de backup **diário** com o uso de computação na nuvem.

4.5 Responsabilidades

4.5.1 Diretor de Compliance, Risco e PLD

- Discutir, elaborar e aprovar as políticas, normas e procedimentos gerais relacionados à Segurança da Informação;
- Designar, definir ou alterar as atribuições da função de Segurança da Informação;
- Analisar os riscos identificados e aprovar os controles requeridos para o tratamento de tais riscos.
- Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
- Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
- Gerenciar a realização de Análise Crítica do SGSI;
- Tratar todos os assuntos relacionados à segurança;
- Definir responsabilidades e autoridades relacionadas a ela;
- Definir necessidades para os negócios da Gestora, no aspecto da Segurança;
- Comunicar aos componentes da estrutura organizacional da Gestora quanto à importância de atender aos objetivos e requisitos legais relacionados ao SGSI.
- Garantir o atendimento às políticas de gestão e aos objetivos do SGSI;
- Aprovar as iniciativas para a melhoria contínua do Sistema;

- Prover recursos para a gestão, operação e monitoramento adequado das atividades do SGSI;
- Suportar perante toda a organização as iniciativas da função de Segurança da Informação;
- Garantir a contínua manutenção da Política de Segurança da Informação;
- Garantir a contínua análise e realimentação dos resultados da gestão de riscos ao SGSI.

4.5.2 Departamento de TI

A Área de TI é responsável pela identificação, apresentação, sustentação, escolha, implantação e manutenção dos controles tecnológicos que apoiam a proteção da informação de todos os departamentos dentro da Gestora. A sua atuação é vital para a Segurança da Informação e deve estar alinhada com os objetivos de cada um dos departamentos e com os objetivos do negócio.

4.5.3 Security Officer

- Produzir diretivas de segurança, regras e padrões a serem usados pelos colaboradores. Estes padrões de segurança local devem levar em conta aspectos como, por exemplo:

  - Necessidades dos negócios da Gestora;
  - Regulamentações e leis locais;
  - Padrões de Segurança alinhados pelo Comitê de Segurança de acordo com os requisitos e necessidades de Segurança da Informação da Gestora;

- Desenvolver e promover programas de conscientização de segurança;
- Garantir que todos os gestores estejam cientes de suas próprias responsabilidades relacionadas à Segurança da Informação;
- Certificar-se que o processo de Gestão de Pessoas leva em conta os aspectos de Segurança da Informação ao contratar novos empregados ou em rescisão de contratos de trabalho;
- Revisar periodicamente o nível de segurança de sistemas internos, emitindo avisos após estas revisões. Analisar criticamente, em intervalos periódicos, o progresso dos planos de melhoria resultantes em conjunto com os gestores envolvidos;
- Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
- Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas na solução dos mesmos. Qualquer incidente de segurança mais importante deve resultar em uma análise realizada

sob a autoridade do Security Officer;

- Representar a empresa, interna e externamente, nos assuntos relacionados ao SGSI;
- Gerenciar os processos do SGSI, na busca da melhoria contínua e alinhamento com a Diretoria;
- Realizar a coleta de dados e informações para a realização da Análise Crítica pelo Comitê de Segurança;
- Dar retorno dos resultados das análises críticas feitas pela direção, aos envolvidos visando providências;
- Acompanhar o sistema de ações corretivas e preventivas do SGSI;
- Garantir a contínua manutenção e atualização dos indicadores de desempenho dos processos do SGSI, estimulando melhorias e mudanças de metas;
- Definir e implantar um plano anual de melhorias de segurança;
- Certificar-se de que a Política de Segurança da Informação da Gestora está implantada;
- Elaborar um mapa de recursos de segurança e mantê-lo atualizado;
- Efetuar o levantamento e análise dos riscos e mantê-lo atualizado;
- Assegurar que os padrões e os procedimentos de segurança definidos sejam respeitados e certificar-se também de que as medidas definidas sejam eficientes e estejam de acordo com as exigências, sem perder o foco dos indicadores estabelecidos;
- Definir e atualizar os indicadores de segurança da informação, que devem contemplar os riscos a que os sistemas de informação estão expostos.

4.5.4 Gestores

- Responsabilidade funcional sobre as suas áreas de operação;
- Responsabilidade de manter atualizada a definição dos ativos de informação e notificar em qualquer alteração no inventário de ativos de sua área;
- Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto à proteção da Segurança da Informação;
- Informar/comunicar ao SGSI todos os fatos relacionados a riscos e incidentes relacionados às áreas de operação sob sua responsabilidade;
- Contribuir para implantação dos objetivos do SGSI e efetuar as medições necessárias por processos;
- Implantar as oportunidades de melhoria;
- Planejar a adoção de procedimentos do SGSI e monitorar sua eficácia;
- Garantir a contínua eficácia dos controles implantados para atender os requisitos

do SGSI.

4.5.5 Colaboradores

- Responsabilidade de notificar qualquer alteração no inventário de ativos de sua área;
- Conhecer e seguir os procedimentos pertencentes ao SGSI;
- Recomendar melhorias no SGSI para melhoria do processo geral de Segurança da Informação;
- Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da Gestora. No caso de terceirizados e prestadores de serviço reportar diretamente para o Departamento de Segurança da Informação;
- Todos os colaboradores têm a responsabilidade de proteger as informações a que tiverem acesso.

4.6 Monitoramento e Testes

O Diretor de Compliance, Risco e PLD (ou pessoa por ele incumbida) adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **semestral**:

(i) monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;

(ii) monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Gestora para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Gestora; e

(iii) verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Compliance, Risco e PLD poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

4.7 Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance, Risco e PLD prontamente. O Diretor de Compliance, Risco e PLD determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance, Risco e PLD determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Diretor de Compliance, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

(i) avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais

de fundo de investimento sob gestão da Gestora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

(vii) determinação do responsável (ou seja, a Gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

- Incidente Caracterizado

Se for caracterizado um incidente, o Diretor de Compliance, Risco e PLD, juntamente com os Administradores da Gestora deverão tomar as medidas imediatas, que poderão abranger se:
(i) Deverá será registrado um boletim de ocorrência ou queixa crime, informar à alguma autoridade e/ou instituição contratante;
(ii) será necessário envolver consultor ou advogado externo;
(iii) haverá comunicação interna ou externa, em especial a cliente que tenha sido afetado; e
(iv) houve prejuízo para a Gestora ou terceiro específico.

Além disso, deverão definir os passos a serem tomados sob o aspecto de *cybersecurity*, tais como:
(i) certificar a aplicação das redundâncias automáticas de TI.

- Determinação da Gravidade do Incidente

O Diretor de Compliance, Risco e PLD analisará e determinará a gravidade do incidente, considerando, dentre outros elementos, (a) os tipos de dados pessoais envolvidos, (b) a sensibilidade da informação comprometida, (c) as medidas de segurança em vigor (*e.g.* criptografia), (d) o que efetivamente aconteceu com os dados pessoais objeto do incidente, (e) existência ou não de uso não autorizado dos dados pessoais comprometidos, (f) impacto real ou potencial do incidente para os titulares dos dados pessoais, (g) número de titulares afetados ou potencialmente afetados e (h) prejuízos efetivos ou potenciais aos titulares dos dados pessoais comprometidos. Feito isto, se entenderem que o incidente pode acarretar risco ou dano relevante aos titulares dos dados pessoais, deverão, imediatamente:

(i) Estabelecer as medidas que serão tomadas para mitigar ou reverter os efeitos negativos do incidente, tanto em relação à Sociedade quanto em relação aos titulares dos dados pessoais comprometidos no incidente;

(ii) Caso a Sociedade seja a Controladora (toma as decisões referentes ao tratamento dos dados pessoais comprometidos no incidente):

- comunicar a Autoridade Nacional de Proteção de Dados, disponibilizando as informações legalmente exigidas, quais sejam, (a) descrição da natureza dos dados pessoais afetados, (b) informações sobre os titulares envolvidos, (c) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciais , (d) riscos relacionados ao incidente, (e) motivos da demora, no caso de a comunicação não ter sido imediata e, (f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

- comunicar os titulares dos dados pessoais comprometidos no incidente, preferencialmente por meio capaz de registrar o envio dessa comunicação.

(iii) Caso a Sociedade seja a Operadora (realiza o tratamento dos dados pessoais comprometidos no incidente em nome de um Controlador):

- verificar as obrigações contratuais relativas a incidentes de segurança que eventualmente assumiu perante o Controlador;

- na ausência de disposição ou orientação contratual especifica, comunicar o Controlador, em prazo razoável e não superior a 3 (três) dias, contados de quando a Sociedade tomou conhecimento do incidente, enviando, no mínimo, as seguintes informações, (a) descrição da natureza dos dados pessoais afetados, (b) informações sobre os titulares envolvidos, (c) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, (d) riscos relacionados ao incidente e, (e) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

(iv) Avaliar a conveniência de divulgar, nos meios de comunicação, uma nota de esclarecimentos sobre o incidente, incluindo, em especial, uma descrição das medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos negativos do incidente, principalmente se tal incidente já tiver sido reportado na mídia.

(v) Avaliar o cabimento de outras comunicações para entidades, organizações e terceiros que podem eventualmente ser impactados pelo incidente em razão dos dados que foram – ou posam ter sido – comprometidos (e.g. bancos).

- Providências Finais

Após o adequado gerenciamento do incidente e a devida mitigação de seus respectivos efeitos, o Diretor de Compliance, Risco e PLD, no prazo máximo de 15 (quinze) dias corridos, contados a partir da data de conhecimento do incidente:

(i) Analisar se será necessário implementar algum mecanismo, dispositivo ou tecnologia de segurança para evitar que novos incidentes similares voltem a ocorrer e, em caso positivo, providenciar tal implantação;

(ii) Analisar se será necessário corrigir alguma vulnerabilidade da estrutura de segurança da informação da Sociedade para evitar que novos incidentes similares voltem a ocorrer e, em caso positivo, providenciar tal correção;

(iii) Consolidar o valor total que a Sociedade despendeu no gerenciamento do incidente e dos respectivos efeitos;

(iv) Analisar se um valor maior deve ser aprovado para gerenciamento de eventuais novos incidentes e seus efeitos e, em caso positivo, providenciar as aprovações necessárias;

(v) Analisar se as políticas internas, incluindo este Plano, foram eficazes, identificando e realizando possíveis aprimoramentos, com o apoio do Jurídico, e;

4.8 Arquivamento de Informações

De acordo com o disposto neste Manual, os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com a Resolução CVM n.º 21.

4.9 Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gestora, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora, salvo se autorizado expressamente pela Gestora e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à Gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Gestora, o Colaborador deverá assinar declaração nos termos do **Anexo IV** ao presente Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e

arquivos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

4.10 Treinamento

O Diretor de Compliance, Risco e PLD organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme descrito no item 5 acima).

4.11 Revisão da Política

O Diretor de Compliance, Risco e PLD realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética a cada **24 (vinte e quatro) meses**, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

5 Política de Sustentabilidade

A Gestora deve sempre buscar adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, incluindo, mas não se limitando a: (a) utilização de papel reciclável para impressão de documentos; (b) utilização de refil de cartuchos e toners para impressão; (c) separação do material reciclável para fins de coleta seletiva de lixo; (d) utilização de lâmpadas de baixo consumo energético; e (e) incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Colaboradores, como transportes coletivos, caronas ou bicicletas.

Além disso, a Gestora incentiva seus Colaboradores a adotar postura semelhante no dia a dia de suas atividades, por exemplo: (a) evitar imprimir e-mails e arquivos eletrônicos, exceto se necessário; (b) optar por utilizar canecas ou copos reutilizáveis; (c) desligar os computadores todos os dias ao final do expediente; (d) apagar as luzes das salas ao sair; e (e) desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

6 Política de Anticorrupção

6.1 Introdução

A Gestora está sujeita às leis e normas anticorrupção, especialmente à Lei nº 12.846/13 e ao Decreto nº 8.420/15 (“Normas de Anticorrupção”) e suas congêneres estaduais e municipais, mas também a outras, tais como a Lei de Improbidade Administrativa e a Lei de Licitações.

Qualquer violação desta Política Anticorrupção e das normas de combate à corrupção pode resultar em penalidades civis e administrativas severas para a Gestora e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade civil e criminal dos indivíduos envolvidos.

6.2 Abrangência das Normas de Anticorrupção

O sistema normativo anticorrupção construído em torno da Lei nº 12.846/13 As Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito à Lei nº 12.846/13 e suas congêneres estaduais e municipais s Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo,

bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados “agentes públicos” para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

Definição

Nos termos das Normas Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

I prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

III comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar licitação pública ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

V dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

São também relevantes as definições de improbidade administrativa veiculadas na Lei 8.429/92, em especial os atos que importem enriquecimento ilícito ou dano ao erário. Essa lei estabelece rol bastante mais extenso de condutas, que se aplicam primariamente aos agentes públicos, mas também ao particular que induza sua prática ou concorra para tanto.

6.3 Normas de Conduta

É terminantemente proibido dar, prometer, negociar ou oferecer qualquer valor, ou presente ou vantagem, inclusive de entretenimento ou hospitalidade, a agente público, em razão de sua condição funcional, mesmo antes de assumi-la, sem autorização prévia do Diretor de Compliance, Risco e PLD, que deverá receber plena informação sobre o contexto das tratativas.

Os Colaboradores deverão se atentar, ainda, para o fato de que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de vantagem suborno seja recusada pelo agente público.

É admitido a quaisquer Colaboradores receber agentes públicos em eventos sociais, desde que o convite e o evento não constituam, em si, vantagem.

Os colaboradores devem comunicar formalmente ao Diretor de Compliance, Risco e PLD qualquer reunião com agente público. Esta comunicação deve ocorrer antes do evento, sempre que possível, e deve incluir informações detalhadas sobre o propósito da reunião, os participantes, e qualquer documentação relevante. Em situações em que a comunicação prévia não for possível, o colaborador deve reportar o evento ao Diretor de Compliance, Risco e PLD imediatamente após sua realização.

Os Colaboradores deverão questionar a legitimidade de quaisquer solicitações de pagamentos vantagem formuladas por solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar, os Colaboradores deveram adotar as seguintes condutas:

i manter postura de cordialidade e procurar preservar o bom relacionamento institucional;
ii explicitar que não se comprometem com o atendimento da solicitação;
iii informar que submeterão a solicitação à área de compliance da Gestora;
iv alertar o Compliance sobre qualquer reunião com o Poder Público;
v informar o Diretor de Compliance, Risco e PLD;
vi se assim orientados, informar o agente público da decisão do Compliance, fazendo-o na presença de ao menos mais um Colaborador.

Nenhum sócio ou colaborador poderá ser punido penalizado ou mal avaliado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

6.4 Proibição de Doações Eleitorais

A Gestora não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos. Em relação às doações individuais dos Colaboradores, a Gestora e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

6.5 Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências (“Audiências”) internas ou externas com agentes públicos, a Gestora será representada por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a Gestora contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Gestora deverão elaborar relatórios de tais Audiências, e apresentá-los ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

1.1. Introdução

A Gestora está sujeita às disposições do Código ANBIMA de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

1.2. Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros, a Gestora identificou, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA ("CGA") no Código ANBIMA de Certificação pertinentes às suas atividades, sendo a CGA aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento.

Nesse sentido, a Gestora definiu que apenas o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Investimentos, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CG.

Em complemento, a Gestora destaca que a CGA é pessoal e intransferível, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance:

Caso o Colaborador esteja exercendo a atividade elegível de CGA na Gestora, conforme acima indicada, e a certificação não esteja vencida a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGA será indeterminado, enquanto perdurar o seu vínculo com a Gestora. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGA na Gestora, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível de CGA.

Desse modo, a Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos no Código ANBIMA de Certificação.

Colaboradores certificados pela CPA-20 deverão, para fins de atualização de sua certificação, participar de programa de treinamento oferecido pela ANBIMA com este

propósito específico, desde que a conclusão do programa de treinamento e aprovação na avaliação final do curso ocorram até a data de vencimento da certificação, observado os prazos mínimos para realização dos cursos disponíveis no site da ANBIMA na internet.

1.3. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, o Diretor de Compliance, Risco e PLD deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, a Gestora deverá inserir o Colaborador no Banco de Dados da Gestora.

O Diretor de Investimentos deverá esclarecer ao Diretor de Compliance, Risco e PLD se os Colaboradores que integrarão os departamentos técnicos terão ou não alçada/poder discricionário de decisão de investimento.

Caso seja identificada a necessidade de certificação, o Diretor de Compliance, Risco e PLD deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

O Diretor de Compliance, Risco e PLD também deverá checar se Colaboradores que estejam se desligando da Gestora estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Gestora.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer **até o último dia útil do mês subsequente à data do evento** que deu causa a atualização, nos termos do art. 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de Compliance, Risco e PLD, conforme disposto abaixo.

1.4. Rotinas de Verificação

Mensalmente, o Diretor de Compliance, Risco e PLD deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código ANBIMA de Certificação.

Ainda, o Diretor de Compliance, Risco e PLD deverá, **mensalmente**, contatar o Diretor de Investimentos que deverá informá-lo se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do art. 17 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Gestora sem a aprovação prévia do Diretor de Investimentos, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pelo Diretor de Compliance, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Investimentos por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, o Diretor de Compliance, Risco e PLD deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, **anualmente** deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

Por fim, serão objeto do treinamento **anual** de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Gestora, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos dos fundos sob gestão, reforçando que somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Gestora, devendo os demais buscar aprovação junto ao Diretor de Investimentos; e (iii) treinamento direcionado aos Colaboradores da Área de Compliance

e Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

1.5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do art. 9º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

Os profissionais já certificados, caso deixem de ser Colaboradores da Gestora, deverão assinar a documentação prevista no Anexo a este Manual denominado "Termo de Afastamento", comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do Anexo aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado **anualmente**, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	Versão	Responsável
Novembro/2021	1ª	Diretor de Compliance, Risco e PLD
Julho/2023	2ª	Diretor de Compliance, Risco e PLD
Agosto/2024	3ª	Diretor de Compliance, Risco e PLD
Fevereiro/2025	4ª e atual	Diretor de Compliance, Risco e PLD

ANEXO I

TERMO DE RECEBIMENTO E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, DECLARO para os devidos fins:

(i) Ter recebido, na presente data, o Manual de Regras, Procedimentos e Controles Internos atualizado ("Manual") da **SOD CAPITAL LTDA.** ("Gestora");

(ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;

(iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e

(iv) Estar ciente do meu compromisso de comunicar ao Diretor de Compliance, Risco e PLD da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

[local], [data].

_____

[**COLABORADOR**]

ANEXO II

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, doravante denominado Colaborador, e **SOD CAPITAL LTDA.** ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios FUNDOS, incluindo:

a) *Know-how,* técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora, conforme aplicável;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela GESTORA, conforme aplicável;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores,

assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do art. 482 da CLT.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de

avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Tenho ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD") e me comprometo a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas na Gestora em conformidade com o estabelecido pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.1. Estou ciente, ainda, de meu compromisso de comunicar ao Encarregado[1], conforme definido pela Gestora, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.2. Na qualidade de pessoa física titular de Dados Pessoais ("Titular de Dados Pessoais"), estou ciente de que a Gestora, na qualidade de "Controladora" para fins de atendimento às disposições da LGPD, tome decisões relativas ao Tratamento de meus Dados Pessoais[2], incluindo operações como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração ("Tratamento") durante todo o período em que eles forem pertinentes, observados os princípios e as garantias ora estabelecidas pela referida lei.

6.2.1. Ainda, na qualidade de Titular de Dados Pessoais, estou ciente de que, a qualquer tempo, mediante requisição à Controladora, tenho o direito de (i) confirmar a existência de Tratamento e acessar meus Dados Pessoais; (ii) corrigir dados incompletos, inexatos

[1] "Encarregado" é a pessoa indicada pela Gestora para atuar como canal de comunicação entre os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados.
[2] Para os fins do presente Termo de Compromisso são considerados Dados Pessoais toda informação relacionada a uma pessoa física que a torne diretamente identificada ou identificável.

ou desatualizados; (iii) solicitar a anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD; (iv) solicitar a portabilidade de meus Dados Pessoais a outro fornecedor de serviço, desde que tal solicitação não inviabilize a prestação de serviços da Gestora; (v) solicitar a eliminação dos Dados Pessoais tratados com o meu consentimento, exceto na hipótese de tal Tratamento ser exigido para fins de atendimento de obrigações legais por parte da Gestora; (vi) solicitar informações sobre o compartilhamento dos meus dados pela Controladora e sobre a possibilidade de não fornecer o consentimento e as consequências dessa negativa; e (vii) me opor ao Tratamento de meus Dados Pessoais em caso de descumprimento da LGPD.

6.2.2. Ademais, reconheço que a Gestora, na qualidade de Controladora, poderá compartilhar os Dados Pessoais com outros agentes de Tratamento de dados, tais como escritórios de contabilidade, agências de turismo, planos de saúde e instituições financeiras, caso seja necessário, observados os princípios e as garantias estabelecidas pela referida LGPD.

6.2.3. Estou ciente de que a Gestora, na qualidade de Controladora, poderá manter armazenados os Dados Pessoais necessários após o término da relação contratual, por prazo determinado em lei, para fins de cumprimento de obrigações legais e/ou regulatórias, bem como para exercer seus direitos em processos administrativos e/ou judiciais.

6.3. Comprometo-me, enfim, a observar em tudo às instruções fornecidas pela Gestora, na qualidade de Controladora, acerca do Tratamento que deverá ser concedido aos Dados Pessoais aos quais tiver acesso em razão de minhas atividades, bem como a sempre agir de acordo com as disposições da LGPD e das normas internas da Gestora quanto à privacidade e proteção de Dados Pessoais.

7. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

8. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[local], [data].

_____

[COLABORADOR]

_____

SOD CAPITAL LTDA.

Testemunhas:

1._____
Nome:
CPF/ME:

2._____
Nome:
CPF/ME:

ANEXO III

PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DA SOD CAPITAL GESTÃO DE RECURSOS LTDA.

1. Resolução CVM n.º 21/21.
2. Resolução CVM n.º 35/21
3. Instrução CVM Nº 617/19.
4. Instrução CVM Nº 555/14.
5. Resolução CVM Nº 30/21.
6. Instrução CVM Nº 472/08.
7. Instrução CVM Nº 578/16.
8. Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.
9. Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada.
10. Lei 9.613/98, conforme alterada.

Data Base: Agosto /2024[3]

[3] **Atenção:** Todo Colaborador deve checar a vigência e eventuais alterações dos normativos contidos neste Anexo previamente à sua utilização.

ANEXO IV

TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____ ("Colaborador"), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **SOD CAPITAL LTDA.** ("GESTORA"), nesta data, dos documentos contidos no *pen drive* da marca [•], número de série [•] ("Documentos"), bem como sua futura utilização pela Gestora, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no pen drive da marca [•], número de série [•], que ficará com a Gestora e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

[•], [•] de [•] de [•].

_____

[COLABORADOR]

Apêndice

Lista dos Arquivos Gravados nos *Pen Drives*

ANEXO V
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/ME sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **SOD CAPITAL GESTÃO DE RECURSOS LTDA.** ("GESTORA") por prazo indeterminado:

[ ] até que me certifique pela CGA, no caso da atividade de gestão de recursos de terceiros com alçada/poder discricionário de investimento;

[ ] ou até que o Conselho de Certificação, nos termos do Código de Certificação, me conceda a isenção de obtenção da CGA;

[ ] tendo em vista que não sou mais Colaborador da Gestora;

São Paulo, [•] de [•] de [•].

_____
[COLABORADOR]

_____
SOD CAPITAL LTDA.

Testemunhas:

1._____
Nome:
CPF/ME:

2._____
Nome:
CPF/ME: