RADAR

Manual de Regras, Procedimentos e Controles Internos

Junho de 2025

SUMÁRIO

Manual de Compliance

I. Introdução

A **RADAR GESTORA DE RECURSOS LTDA.** ("Radar" ou "Gestora") é uma sociedade que se dedica à prestação de serviços de gestão de fundos locais constituídos como fundos de investimentos financeiros cujas classes são tipificadas como "Ações" ("Fundos Locais") e veículos de investimento estrangeiros ("Veículos Estrangeiros") (cada um dos referidos veículos de investimento, um "Fundo", em conjunto, os "Fundos").

Neste sentido, este Manual de Regras, Procedimentos e Controles Internos ("Manual") tem por objetivo descrever brevemente as principais 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 Radar tanto na sua atuação interna quanto na comunicação com os diversos públicos.

A Radar acredita que, com a definição de critérios objetivos a serem seguidos, bem como orientações necessárias para pautar a conduta de seus Colaboradores, torna-se mais fácil e eficiente o exercício das atividades da Radar e de seus Colaboradores no melhor interesse dos Fundos. Assim, todos devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Radar, bem como do completo conteúdo deste Manual.

Em caso de dúvidas ou necessidade de aconselhamento, o Colaborador deve buscar auxílio junto à área de compliance da Radar ("Área de Compliance"), que fica sob a responsabilidade do Diretor de Compliance, Risco e PLD, conforme definido no Formulário de Referência da Gestora disponível em seu website.

A fim de cumprir o seu objetivo, este Manual será revisado anualmente, ou sempre que se fizer necessário, pelo Diretor de Compliance, Risco e PLD e circulado aos Colaboradores.

II. Base Legal aplicável à Gestora

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. São as principais normas aplicáveis às atividades da Gestora:

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21");
(ii) Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM nº 50");
(iii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM nº 175") e seus Anexos Normativos;
(iv) Ofício-Circular/CVM/SIN/Nº 05/2014;
(v) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais

("ANBIMA") de Ética ("Código ANBIMA de Ética");

(vi) Código Anbima de Autorregulação para Administração e Gestão de Recursos de Terceiros ("Código de AGRT");

(vii) Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros ("Regras e Procedimentos ANBIMA do Código de AGRT"), especialmente seu Anexo Complementar III;

(viii) Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, de 11 de julho de 2022, conforme alterada ("Normas de Anticorrupção");

(ix) Lei nº 9.613, de 03 de março de 1998, conforme alterada; e

(x) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora.

1.3. Interpretação e Aplicação do Manual

Para fins de interpretação dos dispositivos previstos deste Manual, exceto se expressamente disposto de forma contrária: (a) os termos utilizados deste Manual terão o significado atribuído na Resolução CVM nº 175; (b) as referências a Fundos abrangem as classes e subclasses, se houver; (c) as referências a regulamento abrangem os anexos e apêndices, se houver, observado o disposto na Resolução CVM nº 175.

II. Aspectos gerais

A Gestora mantém um programa interno de compliance ("Programa de Compliance") apoiado por normas adequadas, recursos humanos e infraestrutura técnico/tecnológica, e governança alinhada com os objetivos da empresa.

Por meio do Programa de Compliance, a Gestora garante o permanente atendimento às normas e regulamentações vigentes:

(i) Em relação aos produtos de investimento oferecidos e serviços prestados;
(ii) À própria atividade de gestão de recursos de terceiros, em suas diversas dimensões; e
(iii) Aos padrões de conduta ética e profissional.

II. 1. Elementos do Sistema

O Programa de Compliance da Gestora inclui os seguintes elementos:

(i) Manual de Controles Internos, Código de Ética e demais políticas adotadas pela Radar criados com o objetivo de resguardar a integridade desta;
(ii) Código de Ética e Conduta;
(iii) Política de Investimentos Pessoais;
(iv) Recursos adequados para desenvolver, manter e melhorar as atividades relacionadas ao compliance; e
(v) Um programa de treinamento de Colaboradores adequado.

II.2. Governança do Programa de Compliance

Os seguintes elementos formam a governança do Programa de Compliance da Gestora:

- Estrutura: a governança do Programa de Compliance da Gestora é baseada nos seguintes órgãos principais:

(a) Área de Compliance, sob a responsabilidade de Diretor de Compliance, Risco e PLD;

(b) Comitê de Compliance, composto pelo Diretor de Compliance, Risco e PLD e pelo Diretor de Gestão, conforme definido no Formulário de Referência da Gestora, este apenas para fins de reporte e Pedro Batista de Lima Filho, (cada um dos referidos, um "Diretor", em conjunto, os "Diretores"); e

- Competências:

(a) **Área de Compliance e Diretor de Compliance, Risco e PLD**: A Área de Compliance, sob responsabilidade final do Diretor de Compliance, Risco e PLD estará incumbida de:

(i) Implementar o Programa de Compliance da Gestora, planejando a execução e cumprindo as metas definidas pelo Comitê de Compliance;

(ii) Redigir e revisar os manuais, procedimentos e regras de compliance;

(iii) Interpretar e aplicar as regras de compliance sobre os casos fáticos, inclusive conduzindo ações disciplinares e determinando punições;

(iv) Auxiliar o Comitê de Compliance em qualquer questão atinente a sua área;

(v) 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 pelo Comitê de Compliance, caso entenda necessário;

(vi) Analisar possíveis violações às políticas da Gestora ou às leis e regulações aplicáveis à Gestora e a suas atividades;

(vii) Atender prontamente todos os Colaboradores;

(viii) Identificar possíveis condutas contrárias a este Manual;

(ix) 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;

(x) Encaminhar aos órgãos de administração da Gestora, até o último dia útil do mês de abril de cada ano, relatório anual de compliance 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 de Gestão ou, quando for o caso, pelo Diretor de Compliance, Risco e PLD 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;

(xi) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual e das outras políticas internas da Gestora;

(xii) 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;

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

(xiv) Determinar auditorias, requisição de documentos, tomada de contas, averiguações, investigações, medidas corretivas e punições;

(xv) Solicitar sempre que necessário, para a análise de suas questões, o apoio de auditoria externa ou outros assessores profissionais; e

(xvi) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio da realização de treinamento inicial e treinamento periódico de reciclagem, podendo profissionais especializados serem contratados para conduzirem os treinamentos.

(b) **Comitê de Compliance**: O Comitê de Compliance é o órgão da Gestora incumbido de:

(i) Dar parâmetros gerais, orientar e aprovar o Programa de compliance da Gestora;

(ii) Estabelecer objetivos e metas para a Área de Compliance;

(iii) Analisar e deliberar acerca de potenciais situações de conflito de interesses;

(iii) Avaliar resultados e performance da Área de Compliance, solicitar modificações e correções, e aprovar o relatório de compliance.

(iv) Aprovar manuais internos de controles internos, Código de Ética e outras normas e regulamentos referentes à política de compliance da Gestora;

(v) Recomendar, propor e adotar orientações e políticas novas, e determinar a modificação, substituição ou a extinção das existentes; e

(vi) Avocar quaisquer matérias envolvendo o Programa de Compliance, violações a regras e regulamentos (prevenção, aplicação e medidas corretivas).

- Independência: a Área de Compliance e o Comitê de Compliance são independentes das outras áreas da Gestora, e poderão exercer seus poderes em relação a qualquer Colaborador.

- Organograma: em vista de sua independência, a Área de Compliance e o Comitê de Compliance tem plena autonomia para discutir e decidir sobre as matérias relacionadas à compliance.

- Reuniões:

(a) **Área de Compliance**: o responsável pela Área de Compliance poderá se reunir com o a Diretoria da Gestora, uma vez por ano, para apresentar o relatório anual de compliance, e

extraordinariamente, quando houver necessidade.

(b) **Comitê de Compliance**: reunir-se-á semestralmente, de forma ordinária, e extraordinariamente, quando houver necessidade. Sempre que necessário, o Diretor de Compliance, Risco e PLD poderá solicitar que o Comitê de Compliance se reúna extraordinariamente para solucionar casos complexos, analisar questões disciplinares e determinar orientações gerais ou específicas nos casos de conflitos de interesse

- Decisões:

Comitê de Compliance: Em matéria de compliance, as decisões do Comitê de Compliance deverão ser tomadas por consenso entre os membros. Nos casos disciplinares e naqueles referentes a investigações de conduta de Colaboradores da Gestora, o Comitê de Compliance poderá decidir por maioria simples. Em relação a medidas corretivas e medidas emergenciais, o Diretor de Compliance, Risco e PLD poderá decidir monocraticamente, sujeito à ratificação do Comitê de Compliance, quando necessário.

Todas as decisões relacionadas ao presente Manual, tomadas pelo Diretor de Compliance, Risco e PLD e pelos demais diretores mencionados neste Manual, ou pelos comitês instituídos pela Gestora, conforme o caso, devem ser formalizadas em ata ou e-mail e todos os materiais que documentam tais decisões serão mantidos arquivados por um período mínimo de 5 (cinco) anos e disponibilizados para consulta, caso sejam solicitados, por exemplo, por órgãos reguladores.

II.3. 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, este utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

A Equipe de Compliance e Risco:

(a) Poderá acessar, quando julgar oportuno e necessário, todo conteúdo que está na rede, inclusive arquivos pessoais salvos em cada computador. Da mesma forma, mensagens de correio eletrônico de Colaboradores poderão ser monitoradas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que são ferramentas de trabalho disponibilizadas pela Gestora;
(b) Escolherá aleatoriamente uma amostragem significativa dos Colaboradores e realizará um monitoramento, anualmente, 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;
(c) Verificará, 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; e

(d) Analisará os controles previstos neste Manual, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles que eventualmente sejam considerados deficientes, monitorando as respectivas correções, sendo que as análises e eventuais correções, se for o caso, deverão ser objeto do relatório anual de compliance.

O Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas nos monitoramentos descritos acima 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.

II.4. Políticas e Procedimentos de Compliance Escritos

A Gestora desenvolveu e adotou um conjunto de políticas de compliance escritas que se encontram neste Manual. As Políticas orientam e são aplicáveis a operações, atividades, processos de todos os Colaboradores. Os objetivos dessas políticas são:

(i) Estabelecer claramente orientações e procedimentos para adequar as condutas da Gestora à legislação, regulamentação e autorregulamentação nacional ("Regras");
(ii) Prevenir, disciplinar e reprimir violações às Regras;
(iii) Prevenir e disciplinar conflitos de interesses;
(iv) Promover a adesão da Gestora aos padrões mais elevados de conduta de gestão de ativos, adequando as práticas e processos internos às boas práticas da indústria.

III. Responsabilização e Penalidades

III.1 Violações

A violação das normas da Gestora por negligência, imprudência e/ou omissão ("Violação"), são passíveis de punição. A Gestora entende por violação:

(i) Agir em desacordo com as leis, regulamentações e autorregulamentações aplicáveis às atividades da Gestora;
(ii) Agir em desacordo com o Manual ou quaisquer outras políticas e normas de compliance da Gestora;
(iii) Agir de forma antiética ou de qualquer forma que prejudique a reputação da Gestora;
(iv) Solicitar que outras pessoas pratiquem ato que se caracterize como Violação; ou
(v) Retaliar Colaborador ou quem tenha reportado uma preocupação com Violação.

III.2. Esclarecimentos

Se constatada alguma irregularidade praticada pelo Colaborador ou desvio de conduta em desacordo com os padrões estabelecidos, o Colaborador será chamado a prestar esclarecimentos. A Área de Compliance poderá arquivar o processo, adverti-lo, firmar Termo de Compromisso, ou, ainda, instaurar Inquérito Administrativo Interno.

III.3. Termo de Compromisso

As seguintes regras aplicam-se ao Termo de Compromisso:

- Utilização: quando se constatar que o ato praticado pelo Colaborador tem alguma gravidade, mas apesar de apontar conduta insatisfatória, não indicar incompatibilidade para o desempenho das funções, a Área de Compliance pode optar por firmar um Termo de Compromisso.
- Objeto: por meio do Termo de Compromisso, o Colaborador reconhece a infração causada pela conduta e reconhece igualmente a necessidade de ajuste às normas.
- Prazo: tendo em vista que a finalidade de tal instrumento é a recuperação funcional do envolvido, haverá um prazo estabelecido para a verificação do ajuste de sua conduta, que não poderá superar 60 dias.
- Acompanhamento: o superior imediato é responsável pelo acompanhamento e por zelar pelas condições necessárias para o cumprimento integral do Termo de Compromisso.

III.4. Inquérito Administrativo

As seguintes regras aplicam-se ao Inquérito Administrativo:

- Utilização: a instauração de Inquérito Administrativo Interno ocorrerá quando: (i) a infração incorrida pelo Colaborador for grave, (ii) quando for passível de enquadramento no artigo 482 da CLT (Consolidação das Leis do Trabalho) que trata das hipóteses de dispensa do Colaborador por justa causa ou (iii) possam causar prejuízo à Gestora. São assegurados neste procedimento ampla defesa e direito ao contraditório.
- Responsabilização: após a conclusão do inquérito administrativo, ponderada a gravidade da ocorrência, o Colaborador pode ser responsabilizado e sujeitar-se a ações disciplinares; sendo que a Área de Compliance tem autoridade para definir sua aplicação, conforme determinação legal, às seguintes sanções:
  (i) Responsabilização pecuniária;
  (ii) Advertência escrita ou verbal;
  (iii) Censura;
  (iv) Suspensão até 30 dias;
  (v) Demissão.

- Responsabilização Pecuniária: a responsabilização pecuniária levará em conta o vencimento padrão do Colaborador. Quando envolver mais de um Colaborador, deve-se apurar o

percentual de responsabilidade de cada um dos envolvidos, que será igual ao grau de participação, limitado ao valor sob julgamento.

III.5. Dever de Reportar

Os Colaboradores entendem e aceitam que têm o dever ativo de prontamente reportar suspeitas ou indícios de Violações. Nenhum Colaborador deverá ser penalizado por reportar suspeitas ou supostas violações.

Política de Confidencialidade

I. Objetivo

As regras e princípios estabelecidos nesse documento tem por objetivo orientar os Colaboradores da Radar no que diz respeito ao acesso, uso e tratamento de informações confidenciais por parte dos mesmos. Esta Política deve ser lida em conjunto com o Código de Ética e a Política de Investimentos Pessoais.

II. Informações confidenciais

Os Colaboradores deverão se atentar, ainda, ao uso de informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Radar ("Informações Confidenciais"), as quais devem ser utilizadas apenas para desempenhar as atribuições na Radar e sempre em benefício dos interesses dos Fundos Geridos. Além das definições trazidas pelo Anexo II ao presente Manual, são exemplos de informações confidenciais:

(i) Modelos de *valuation* de empresas, assim como as premissas nele utilizadas;
(ii) Planilhas eletrônicas que façam parte do processo de investimento, monitoramento do portfólio ou que digam respeito ao universo de investimento contemplado pela Radar;
(iii) Estratégias de investimento;
(iv) Metodologias de gerenciamento de risco, entendendo-se aqui os riscos tanto de mercado quanto de liquidez dos ativos;
(iv) Investidores e potencias investidores;
(v) Posições em ativos, mesmo aquelas encerradas em até 6 (seis) meses;
(vi) Sistemas de controle proprietários;
(vii) Informações referentes à contabilidade da Radar, como receitas, despesas e lucro
(viii) Relacionamento da Radar com corretoras e com os demais membros da comunidade de investimentos.

Quando de seu ingresso na Radar e, posteriormente, em até 30 (trinta) dias corridos após o término de cada ano civil, os Colaboradores deverão assinar o Termo de Compromisso e o Termo de Confidencialidade reforçando seu cumprimento no que se refere às regras constantes nessa Política.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Radar, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos Fundos ou das operações realizadas pela Radar. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à area de Compliance da Radar, para que sejam tomadas as medidas cabíveis.

A Radar exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a

respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Radar, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações confidenciais dos Fundos ou de suas operações deverá ser mantido nas dependências da Radar, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do Colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do Fundo ou da atividade a que se refere tal arquivo eletrônico.

Para fins de manutenção das Informações Confidenciais, a Radar recomenda que seus Colaboradores (i) bloqueiem o computador quando o mesmo não estiver sendo utilizado; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro *("clean desk policy");* (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos.

No momento em que for encerrado o vínculo do Colaborador com a Radar, o mesmo receberá um pen drive com todos os seus arquivos pessoais. Cabe ressaltar que é expressamente proibida a gravação de arquivos sem a autorização do Diretor de Compliance, sendo tal ato passível de penalidades e sanções tais quais as descritas no Manual de Compliance.

Ademais, as regras de Proteção de Dados Pessoais, Segurança da Informação e Segurança Cibernética devem ser observadas para fins de manutenção das Informações Confidenciais.

III. Informações Privilegiadas

Ainda no que tange aos potenciais conflitos, o Colaborador também deve se atentar ao uso de Informações Privilegiadas, obtidas por ele no exercício de sua função, conforme definido neste capítulo.

Considera-se informação privilegiada ("Informação Privilegiada") aquela relacionada a qualquer emissor de valores mobiliários negociados no mercado brasileiro (como companhias abertas e fundos de investimento) que preencha, cumulativamente, as seguintes condições:

- Seja confidencial, assim entendida a informação que não tenha sido ainda divulgada ao mercado de maneira oficial, pelo emissor ou pelo terceiro detentor da informação relacionada ao emissor; e
- Seja relevante, assim entendida a informação capaz de afetar a decisão dos investidores de negociar com valores mobiliários do emissor, inclusive no que diz respeito ao exercício de direitos políticos.

É vedada a compra ou venda de títulos e valores mobiliários, com base na utilização de Informação Privilegiada, visando à obtenção de benefício próprio ou de terceiros (incluindo a Radar, os Fundos Geridos e seus Colaboradores).

É vedada também a divulgação a terceiros de Informação Privilegiada que possa ser utilizada vantajosamente na compra ou venda de títulos e valores mobiliários *("tipping"),* sob pena de apuração das práticas irregularmente tomadas, assim como a aplicação das sanções administrativas e judiciais eventualmente cabíveis.

IV. Dever de Informação ao Diretor de Compliance, Risco e PLD

No exercício de suas atividades, a Radar e seus Colaboradores pode eventualmente ter acesso à Informações Privilegiadas e/ou Confidenciais, sob regime legal ou contratual de confidencialidade, por força de relações que mantêm com o emissor. Muitas vezes tais informações não são relevantes, e por vezes estão à disposição de outros agentes. Sem prejuízo disto, são exemplos de situações nas quais o Diretor de Compliance, Risco e PLD deverá ser obrigatoriamente informado:

(i) Sempre que uma nova Informação Privilegiada potencialmente relevante chegar ao conhecimento dos Colaboradores;
(ii) Celebração de contrato que estabeleça um fluxo de Informações Privilegiadas potencialmente relevantes sobre emissor de valores mobiliários; e
(iii) Existência de situações de relação comercial, profissional ou de confiança, entre a Radar e uma companhia aberta, da qual resulte fluxo de informações potencialmente relevantes;

A informação acima deverá ser enviada eletronicamente, com indicação de confidencialidade do conteúdo da mensagem, e deve conter todas as informações julgadas relevantes pelo Colaborador, sem prejuízo de outras informações ou confirmações que possam vir a ser solicitadas pelo Diretor de Compliance, Risco e PLD. Caso o Diretor de Compliance, Risco e PLD entenda que existe a necessidade, os valores mobiliários do emissor podem ser classificados como em Restrição Total, conforme definido na Política de Investimentos Pessoais da Gestora.

Todo Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Radar, gerar conflitos ou, ainda, caracterizar-se como contrárias ao previsto neste Manual, deverá informar seu superior imediato ou diretamente ao Diretor de Compliance, Risco e PLD, para que sejam tomadas as providências cabíveis.

Política de Segurança da Informação

I. Objetivo

As medidas de segurança da informação contidas nesse documento têm por finalidade minimizar as ameaças aos negócios da Radar advindas do uso inadequado dos sistemas de informação.

II. Disposições Gerais

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Radar.

O acesso ao escritório e a sala de operações da Radar é totalmente informatizado e controlado por controle de acesso por biometria. Somente os Colaboradores possuem cadastro biométrico que permitem a entrada automática e, em caso de falha na leitura biométrica, cada colaborador possui uma senha para acesso ao escritório. O acesso de terceiros à Radar somente é permitido na recepção e nas salas de reunião, enquanto na sala de operações este acesso está condicionado ao acompanhamento de pelo menos um Colaborador. O acesso de pessoas estranhas à mesa de operações ou às outras dependências da empresa, inclusive à sala dos servidores, somente será possível quando acompanhado dos responsáveis pelas respectivas áreas.

A Radar mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores e monitorará o acesso dos Colaboradores a tais pastas e arquivos com base na senha e *login* disponibilizados. O acesso às pastas e arquivos eletrônicos é controlado de acordo com cada função dos Colaboradores, e somente algumas instâncias de visualização são livres para todos os Colaboradores.

A Gestora conta com o auxílio de empresa especializada de T.I, a qual auxiliará o Diretor de Compliance, Risco e PLD na verificação, por amostragem, em periodicidade mínima anual, do processo de acesso escalonado implementado.

III. Regras

Somente com autorização será permitido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Radar e circulem em ambientes externos a Radar com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como Informações Confidenciais.

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 Radar. 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.

Os Colaboradores devem garantir que suas mesas estejam sempre organizadas e livres de quaisquer documentos ou anotações que contenham informações confidenciais.

Qualquer impressão de documentos deve ser imediatamente retirada na impressora, pois podem conter informações restritas e confidenciais mesmo no ambiente interno da Radar.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado 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-drive, HD externo ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Radar.

Todas as informações que possibilitem a identificação de um cliente da Radar devem permanecer em arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se for para o atendimento dos interesses da Radar ou do próprio cliente. Tal restrição não se aplica na eventualidade de cumprimento de ordem de autoridade judicial ou administrativa determinando a disponibilização de informações sobre eventual cliente da Radar, cujo atendimento deverá ser previamente comunicado à Área de Compliance, a quem caberá tomar as providências necessárias.

É proibida a conexão de equipamentos na rede da Radar que não estejam previamente autorizados pela área de informática e pela Área de Compliance.

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

IV. Uso dos Ativos, Internet e E-mail

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

Tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Radar poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores.

Para o serviço de e-mail a Radar utiliza a plataforma Office365 e conta com as contingências oferecidas pela Microsoft. Essa plataforma é amplamente utilizada pelo mercado e conta com diversos dispositivos para garantir a integridade e disponibilidade dos serviços. Além das contingências na nuvem, as estações de trabalho de cada profissional mantêm cópias dos e-mails dos usuários e permitem acesso aos dados mesmo sem o acesso a plataforma Office365.

A Gestora conta com o auxílio de empresa especializada de T.I, a qual auxiliará o Diretor de Compliance, Risco e PLD na verificação, por amostragem, em periodicidade mínima anual, do processo de verificação de e-mails dos Colaboradores.

V. Infraestrutura

Infraestrutura utilizando a solução de virtualização da Microsoft, garantindo redundância da própria infraestrutura e melhor tempo de recuperação de desastres (RTA). Cada Colaborador possui um computador com todas as informações de usuário local redirecionada para os servidores. Acessos remotos aos servidores por VPN IPSEC/SSL, com certificado SSl e MFA Microsoft com possibilidade de auditoria de acessos.

A Radar possui uma estrutura de servidores redundantes no serviço Azure da Microsoft. Os serviços AD, DNS, FILE SERVER estão entre os replicados em tempo real para os servidores redundantes e são acionados automaticamente em caso de falha nos servidores primários. Os demais serviços possuem backup diretamente para a plataforma em nuvem da Microsoft com possibilidade de recuperação manual diretamente no Azure em caso de falha na estrutura local.

Sistema de Firewall redundante (UTM) com múltiplas camadas de segurança como IDS, IPS, Web Filtering, ATP, Anti-Malware e Anti-Spam; Acessos remotos aos servidores por VPN IPSEC/SSL e possibilidade de auditoria de acessos.

A Radar possui uma estrutura de links de Internet corporativos redundantes com balanceamento de tráfego. Distribuição de links por múltiplas operadoras e “últimas milhas” distintas.

A Radar possui uma estrutura de nobreaks (UPS) nos equipamentos do CPD com gerenciamento remoto e monitoramento ambiental. Estações de trabalho que não contam com notebooks possuem nobreaks individuais.

A Radar possui Central telefônica digital IP (PABX) e linhas de telefone digitais (E1) com redundâncias de linhas de telefonia analógicas.

VI. Back-up

Para garantir a manutenção dos dados, existem as seguintes rotinas de *backup*. A primeira realiza o versionamento dos arquivos de aproximadamente 30 (trinta) dias nos próprios servidores, sendo executado duas vezes ao dia. A segunda rotina é feita na plataforma Microsoft Azure (nuvem) onde os *backups* são realizados diariamente e armazenados em datacenters redundantes. Os *backups* são realizados de segunda a sexta e armazenados por 4 (quatro) semanas. Uma versão mensal com a posição da última sexta-feira de cada mês é armazenada pelos últimos 12 (doze) meses. Na última sexta do mês de dezembro é armazenada uma versão de *backup* anual que é mantida por 5 (cinco) anos. As informações contidas no *backup* estão criptografadas por chave de 256 (duzentos e

cinquenta e seis) bits e acessíveis somente por acessos restritos por senha de segurança. As rotinas de *backup* são validadas diariamente pelo mantenedor de TI. Testes de restauração para validação do processo de recuperação de dados são feitos mensalmente.

VII. Testes de Segurança

Os testes oficiais de segurança são realizados todos os anos. Em tais testes, usuários acessam o ambiente de trabalho remotamente enquanto o ambiente de co-location está ativo. Testes não-oficiais são realizados de forma mais frequente, durante a janela de operação regular da rede.

VIII. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas neste Manual ("Informações" ou "Informação"), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de Compliance, Risco e PLD deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de Compliance, Risco e PLD, primeiramente, identificará se a Informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de Compliance, Risco e PLD procederá da seguinte forma:

A. No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

B. No caso de vazamento de Informações relativas aos cotistas:

Neste caso, o Diretor de Compliance, Risco e PLD procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de Compliance, Risco e PLD ficará à inteira disposição para auxiliar na solução da questão.

Política de Segurança Cibernética

I. Identificação e avaliação de Riscos (risk assessment)

A Gestora avaliou e identificou continuamente os principais riscos cibernéticos aos quais está exposta. De acordo com o Guia ANBIMA de Segurança Cibernética, os tipos de ataques mais recorrentes promovidos por agentes mal-intencionados incluem:
a) Malware (vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;
d) Phishing scam;
e) Vishing (phishing por chamadas de voz);
f) Smishing (phishing via mensagens SMS);
g) Acesso indevido por pessoas autorizadas (insiders);
h) Ataques de DDoS e uso de botnets;
i) Invasões por ameaças persistentes avançadas (APT – Advanced Persistent Threats).

Com o objetivo de mitigar esses e outros riscos potenciais, a Gestora mapeou e classificou todos os ativos críticos da organização, considerados essenciais para a continuidade de suas operações. Foram estabelecidos critérios para a classificação da informação e processos contínuos de avaliação de vulnerabilidades desses ativos.

A Gestora levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

Considerando a evolução incessante dos riscos cibernéticos, a área de TI manterá vigilância permanente sobre os riscos relacionados à segurança da informação, com o objetivo de proteger as Informações Confidenciais e os recursos tecnológicos da Gestora. Para isso, serão realizados testes periódicos, implementadas medidas preventivas e adotadas práticas específicas de cibersegurança, conforme detalhado em seção própria desta Política

II. 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 pela Gestora, se apresenta da seguinte maneira:
• Público - todo o conteúdo de todos os documentos é visualizado por qualquer colaborador da Gestora, clientes, fornecedores e parceiros.
• Interno - todo o conteúdo de todos os documentos é visualizado somente por colaboradores 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/Interno	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.

III. Ações de prevenção e proteção

A Gestora adota um conjunto de medidas técnicas e administrativas com o objetivo de prevenir incidentes e proteger seus ativos de informação. Entre essas medidas, destacam-se:

a. Segregação de Acessos e Gestão de Privilégios

A segregação de acessos a sistemas e dados é um dos principais pilares da política de Segurança da Informação da Gestora. O acesso a sistemas, redes e dispositivos é concedido apenas quando estritamente necessário à função desempenhada, com base no princípio do menor privilégio.
As permissões são atribuídas conforme critérios definidos, levando em conta a relevância do ativo acessado e as responsabilidades de cada colaborador. Eventos como login e alteração de senha são auditáveis e rastreáveis, sendo gerados logs sempre que os sistemas permitirem. Esses registros são armazenados pela empresa de T.I. contratada por, no mínimo, 5 (cinco) anos.

b. Segurança de Autenticação e Senhas

São aplicadas regras mínimas de complexidade e renovação de senhas, com exigência de criptografia e parametrização conforme boas práticas globais. O compartilhamento de senhas e credenciais de acesso é expressamente proibida, e o colaborador poderá ser responsabilizado por uso indevido decorrente da negligência com essas informações.

c. Acesso Remoto e Configuração Segura de Sistemas

O acesso remoto a arquivos, sistemas locais ou em nuvem é controlado e permitido apenas mediante

critérios definidos pelo responsável por Segurança Cibernética. Sistemas e equipamentos novos somente entram em produção após passarem por testes em ambiente de homologação ou prova de conceito, com configurações seguras aplicadas.

A Gestora mantém soluções de proteção como antivírus, anti-malware e firewalls pessoais instalados em estações de trabalho e servidores, além de aplicar restrições de acesso a websites e bloqueio da execução de softwares ou aplicativos não autorizados.

d. Uso e Compartilhamento de Informações Confidenciais

Nos casos em que o uso de cópias se fizer necessário para o desempenho das funções do colaborador, este será diretamente responsável pela integridade, confidencialidade e guarda adequada dos documentos.

Dispositivos de armazenamento externo, como HDs ou pen drives, só devem ser utilizados com autorização expressa e para fins estritamente profissionais.

e. Uso de Ativos de TI

Os recursos tecnológicos da Gestora — incluindo computadores, telefones, e-mails, sistemas e internet — devem ser utilizados prioritariamente para fins profissionais. O uso pessoal deve ser eventual, moderado e nunca comprometer a segurança da informação.

f. Segurança de E-mails

Embora o recebimento de e-mails muitas vezes fuja ao controle do colaborador, espera-se discernimento para evitar ou excluir mensagens com características suspeitas. Caso receba e-mails com arquivos ou links suspeitos, o colaborador deverá excluí-los imediatamente e notificar o Diretor de Compliance, Risco e PLD.

Todos os anexos de e-mails recebidos são submetidos à verificação automática pelos servidores da Gestora, que bloqueiam preventivamente arquivos maliciosos identificados.

g. Backup e Retenção de Informações

A Gestora realiza backup periódico dos dados e ativos críticos, conforme definido na Política de Segurança da Informação. Toda informação — inclusive aquelas confidenciais, privilegiadas ou sujeitas a investigações — deve ser armazenada em local seguro, para fins de auditorias, conformidade regulatória ou investigações internas, conforme disposto na RCVM 21.

h. Diligência e Responsabilidade

Cabe a cada colaborador zelar pela segurança das informações sob sua responsabilidade. Isso inclui

o controle físico e digital dos equipamentos utilizados, bem como a observância de medidas de diligência prévia, fundamentais para a proteção dos ativos da Gestora.

IV. Monitoramento, Validação e Revisão Contínua de Controles

O Diretor de Compliance, Risco e PLD é responsável por assegurar que os mecanismos de controle de segurança da informação, descritos nesta política e em normas complementares, sejam anualmente testados pela equipe técnica responsável, visando verificar sua eficácia, consistência e atualidade.

Paralelamente, os testes de restauração de dados — parte fundamental do processo de recuperação em caso de incidentes — são realizados mensalmente, de modo a validar a integridade e a disponibilidade dos backups.

A Gestora mantém mecanismos sistemáticos de monitoramento e validação das medidas de proteção implementadas, garantindo seu funcionamento adequado e a constante mitigação de riscos cibernéticos. Dentre essas medidas, destacam-se:

a. Inventário e Controle de Ativos

A Gestora possui inventários permanentemente atualizados de hardware, software e dispositivos conectados, os quais são auditados periodicamente com o objetivo de identificar eventuais elementos não autorizados ou anômalos na infraestrutura tecnológica.

b. Gestão de Atualizações e Correções

A área técnica responsável deve garantir a instalação tempestiva de atualizações de segurança em sistemas operacionais, softwares de aplicação, firmwares e dispositivos de rede, observando as janelas de manutenção e os protocolos internos de homologação. Patches críticos devem ser aplicados com prioridade, conforme avaliação de impacto e risco.

c. Backup e Testes de Restauração

As rotinas de backup são monitoradas diariamente, e os testes de restauração são realizados regularmente, com registros documentados, garantindo a capacidade de recuperação dos dados em caso de perda, ataque cibernético ou falha sistêmica.

d. Testes de Segurança e Análises de Vulnerabilidade

A Gestora realiza, periodicamente ou sempre que houver alterações relevantes na infraestrutura, as seguintes ações de verificação técnica:

• Testes de intrusão (penetration testing) conduzidos por profissionais qualificados;

• Simulações de ataques de phishing para avaliação da conscientização dos usuários;
• Varreduras de vulnerabilidades em sistemas, servidores, endpoints e aplicações web;
• Avaliações de conformidade com as políticas internas e os requisitos regulatórios aplicáveis.

e. Auditoria de Logs e Atividades

Os logs de eventos, acessos e alterações em sistemas críticos são analisados regularmente pela equipe de segurança da informação. Isso permite a identificação proativa de tentativas de violação, comportamento anômalo de usuários e acessos indevidos, sejam eles de origem interna ou externa.

Esses registros são armazenados de forma segura e íntegra, por período não inferior a 5 (cinco) anos, em conformidade com as obrigações regulatórias e as boas práticas de governança de dados.

f. Verificações Aleatórias e Fiscalização Interna

O Diretor de Compliance, Risco e PLD deve realizar verificações aleatórias e não anunciadas, que poderão incluir:
1. Análise de e-mails encaminhados ou respondidos por Colaboradores, quando houver indício de uso indevido;
2. Avaliação do uso de ativos tecnológicos da Gestora (como computadores, rede, sistemas e dispositivos móveis), incluindo a análise de sites acessados e uso de aplicações não autorizadas;
3. Revisão dos registros de acesso a ambientes restritos, como áreas com dados sensíveis, servidores ou arquivos confidenciais.

Essas ações visam garantir o uso adequado dos recursos corporativos, a proteção de informações confidenciais e o alinhamento com as diretrizes de segurança estabelecidas pela Gestora.

g. Revisão Contínua de Controles

Todos os controles, políticas e práticas devem ser revistos periodicamente, à luz da evolução dos riscos cibernéticos, novas regulamentações e mudanças tecnológicas. Sempre que identificadas fragilidades ou oportunidades de melhoria, planos de ação corretiva devem ser elaborados e executados com prazo e responsáveis definidos.

V. Plano de Resposta a Incidentes de Segurança Cibernética

A Área de Gestão de Riscos e de Compliance, em conjunto com os profissionais de Cibersegurança e Segurança da Informação, é responsável pela elaboração, implementação e manutenção de um Plano Formal de Resposta a Incidentes de Segurança Cibernética.

Este plano tem por objetivo minimizar os impactos de incidentes cibernéticos, garantir a continuidade dos negócios, preservar a integridade e a confidencialidade das informações e assegurar o cumprimento das obrigações legais e regulatórias aplicáveis.

a. Estruturação do Plano

b.

O Plano de Resposta deverá conter, no mínimo, os seguintes elementos:

1. Definição de papéis e responsabilidades:

- Estabelecimento claro das atribuições de cada área envolvida (TI, Compliance, Jurídico, Comunicação, entre outras).
- Identificação e mapeamento dos colaboradores-chave que devem ser acionados em caso de incidente.
- Inclusão de contatos externos relevantes, como fornecedores de segurança, especialistas forenses, provedores de nuvem e autoridades reguladoras.

2. Cenários e ameaças previstas:

O plano deverá considerar os principais vetores de ataque identificados na Avaliação de Riscos (Risk Assessment) da Gestora, incluindo, mas não se limitando a:

- Ransomware;
- Phishing direcionado (spear phishing);
- Invasões externas (APT);
- Vazamento de dados;
- Comprometimento de credenciais;
- Indisponibilidade de sistemas (DDoS).

3. Classificação dos incidentes por severidade:

- Estabelecimento de critérios objetivos para classificação dos incidentes, com base em impacto e urgência (ex: Crítico, Alto, Médio, Baixo).
- Tratamento diferenciado conforme o grau de severidade, incluindo níveis de escalonamento interno.

4. Procedimentos de contenção, erradicação e recuperação:

- Etapas a serem seguidas para conter a ameaça, eliminar a causa raiz e restabelecer os serviços afetados com segurança.
- Procedimentos para ativação de ambientes de contingência, acessos alternativos ou recuperação em nuvem, quando necessário.
- Plano para retorno às instalações originais, após estabilização da situação, de forma segura e controlada.

5. Notificação e comunicação:

- Diretrizes para comunicação interna e externa em caso de incidente, incluindo:

- Notificação às partes afetadas;
- Comunicação à ANBIMA, CVM, Banco Central e outras autoridades, quando aplicável;
- Interface com o Encarregado de Proteção de Dados (DPO) para avaliação de impactos relacionados à LGPD.

- Modelos de mensagens de crise e canais de comunicação alternativos.

6. Preservação de evidências e investigação:

Medidas para preservar logs, registros e elementos técnicos que possam subsidiar:

- Investigações internas e externas;
- Análises forenses;
- Ações administrativas, cíveis ou criminais.

7. Documentação e formalização:

- O plano de resposta deverá ser formalizado e documentado, com versão controlada.
- Cada incidente deverá gerar um registro individual (relatório de incidente) contendo: data, hora, descrição, impacto, ações tomadas, responsáveis e lições aprendidas.
- Sempre que o plano for atualizado ou acionado, deverá ser comunicado formalmente por e-mail ao Diretor de Compliance, Risco e PLD, que avaliará a necessidade de medidas complementares, inclusive comissões de apuração.

8. Atualização e Testes do Plano

O Plano de Resposta a Incidentes deverá ser revisado ao menos anualmente, ou sempre que ocorrer:

- Alteração relevante na estrutura tecnológica;
- Incidente de segurança com lições aprendidas;
- Mudança nas obrigações regulatórias.

Devem ser realizados testes periódicos de simulação (exercícios de mesa e testes técnicos), com documentação dos resultados e plano de melhorias.

VI. Reciclagem, Revisão e Conscientização

O Programa de Segurança Cibernética da Gestora, que engloba os procedimentos técnicos, controles administrativos, o Plano Formal de Resposta a Incidentes, bem como todas as políticas internas correlatas, deverá ser revisado e atualizado semestralmente, ou sempre que houver:

- Alterações relevantes na infraestrutura tecnológica ou nos sistemas utilizados;
- Identificação de novas ameaças ou vulnerabilidades significativas;
- Mudanças regulatórias ou normativas aplicáveis;
- Ocorrência de incidentes de segurança relevantes.

a. Revisão Contínua e Atualização Técnica

As áreas envolvidas diretamente com qualquer aspecto do programa de segurança — incluindo TI, Compliance, Riscos, Jurídico e demais times técnicos — devem se manter atualizadas quanto às melhores práticas do mercado, participando de fóruns, treinamentos e, quando necessário, consultando fornecedores especializados para reavaliação ou aprimoramento das medidas vigentes.

Deverão ser mantidos registros documentais das revisões realizadas no programa, com indicação de responsáveis, datas, escopo alterado e justificativas.

b. Divulgação Interna e Cultura de Segurança

A Gestora deve promover a ampla divulgação interna do Programa de Segurança Cibernética, por meio de:

- Comunicados institucionais;
- Materiais explicativos;
- Atualizações em intranet corporativa ou canais de comunicação interna.

Deve-se fomentar uma cultura organizacional orientada à segurança da informação, conscientizando os Colaboradores sobre os riscos cibernéticos mais comuns (ex: phishing, engenharia social, uso indevido de sistemas) e boas práticas de prevenção.

c. Treinamentos e Capacitação Contínua

Todos os Colaboradores deverão participar, obrigatoriamente, de programas de capacitação em segurança cibernética, com periodicidade mínima anual, e sempre que:

- Houver o ingresso de novos profissionais;
- Ocorrerem atualizações relevantes nas políticas de segurança;
- For identificado baixo índice de conformidade ou vulnerabilidades humanas em testes simulados (ex: campanhas de phishing).

Esses treinamentos serão coordenados pela área responsável por esta política, podendo contar com o apoio de consultorias externas especializadas, e deverão abordar, no mínimo:

- Conceitos básicos de cibersegurança;
- Práticas seguras no uso de dispositivos, e-mails e senhas;
- Reconhecimento e resposta a ameaças comuns;
- Responsabilidades individuais sobre a proteção da informação;
- Procedimentos a adotar em caso de incidentes.

A participação será registrada formalmente e poderá compor indicadores de conformidade, sendo considerada parte das obrigações contratuais dos Colaboradores com a instituição.

Política de Certificação ANBIMA

A Gestora aderiu e está sujeita às disposições das Regras e Procedimentos de Certificação ANBIMA, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

I. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros, a Gestora identificou, segundo as Regras e Procedimentos de Certificação ANBIMA, que a Certificação de Gestores ANBIMA ("CGA") é a certificação pertinente às suas atividades, aplicáveis aos profissionais com alçada/poder discricionário de investimento.

Nesse sentido, somente o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA, uma vez que a CGA é a certificação aplicável aos profissionais que atuam em carteiras administradas, fundo de renda fixa, fundo de ações, fundo multimercado, fundo cambial e/ou fundos de índice.

Em complemento, a Gestora destaca que as certificações são de cunho pessoal e intransferíveis, bem como seguirão os seguintes prazos, os quais serão monitorados pelo Diretor de Compliance, Risco e PLD, sendo certo que caso o Colaborador esteja exercendo a atividade elegível de CGA na Gestora 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 e a sua atuação na atividade elegível. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível da CGA na Gestora, a validade da respectiva certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível da CGA, conforme o caso.

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 nas Regras e Procedimentos de Certificação ANBIMA .

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

Antes da contratação ou admissão 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.

O Diretor de Gestão deverá esclarecer ao Diretor de Compliance, Risco e PLD se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de

investimento e com quais produtos cada um dos Colaboradores irá atuar.

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 os 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**, 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.

III. 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 nas Regras e Procedimentos de Certificação ANBIMA.

Ainda, o Diretor de Compliance, Risco e PLD deverá contatar o Diretor de Gestão **prontamente** sempre que houver algum tipo de alteração nos cargos / funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos e/ou com quais produtos cada destes Colaboradores atuarem, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento.

Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho 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 Gestão, 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 Gestão ou do Comitê de Investimentos por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente, o Diretor de Compliance, Risco e PLD poderá 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 das Regras e Procedimentos de Certificação ANBIMA, 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, reforçando que (a) 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 Gestão e/ou ao Comitê de Investimentos; e (iii) treinamento direcionado aos Colaboradores da área de Compliance, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

IV. Processo de afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais haja certificação exigível, nos termos previstos neste Manual, serão imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem ou até que o Conselho de Certificação conceda a isenção de obtenção da certificação aplicável, devendo para tanto assinar a documentação prevista no **Anexo III** a este Manual, comprovando o seu afastamento da Gestora

Política de Treinamento Contínuo

I. Objetivo

Esta política tem o intuito de promover o constante aperfeiçoamento dos profissionais da Radar e a melhoria constante das funções dos Colaboradores. Dessa forma, a Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, especialmente aqueles que tenham acesso à 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.

II. Disposições Gerais

Cursos de atualização ou certificados que sejam relacionados às atividades desenvolvidas são incentivados e poderão ser integral ou parcialmente patrocinados pela Radar, especialmente quando voltadas para estudos nas áreas de Finanças e Estratégia.

Poderão ser ministradas a todos os Colaboradores da Radar palestras internas, a fim de dar ciência sobre i) as políticas adotadas pela Radar; ii) a regulamentação vigente e aplicável aos negócios da Radar e, ainda, iii) eventuais problemas ocorridos, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela Radar.

Todo o treinamento interno proposto pela Radar, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais da Radar, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

A Área de Compliance ficará encarregada de aplicar o treinamento, o qual será realizado a cada 12 (doze) meses, e obrigatório a todos os Colaboradores. Quando do ingresso de um novo Colaborador, a Área de Compliance aplicará o devido treinamento de forma individual para o novo Colaborador.

O treinamento acima descrito será realizado conjuntamente com o treinamento sobre as regras de prevenção à lavagem de dinheiro, conforme a Política de Prevenção à Lavagem de Dinheiro e Combate ao Terrorismo e Cadastro da Gestora.

Sem prejuízo do treinamento anual, sempre que houver uma mudança legislativa que impacte diretamente na rotina de trabalho dos Colaboradores, o departamento de compliance aplicará um treinamento a fim de orientar sobre mudança legislativa.

Política de Segregação de Atividades

I. Introdução

Inicialmente, cumpre esclarecer que a Gestora atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito.

II. Segregação de atividades e funções

O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de Gestor, Analistas, Compliance, Risco e Administrativo. Perfis de acesso físico e eletrônico, e o controle são realizados com base nessas divisões, conforme já detalhado neste Manual.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade ("*as-needed basis*") nos comitês da Gestora, sendo que os participantes se responsabilizam pelo sigilo das informações.

III. Segregação física

O acesso ao escritório e a sala de operações da Radar é totalmente informatizado e controlado por crachás eletrônicos e biometria. Somente os Colaboradores possuem crachás e biometria cadastrada que permitem a entrada automática. O acesso de terceiros à Radar somente é permitido na recepção e nas salas de reunião, e apenas enquanto acompanhados de pelo menos um Colaborador. O acesso de pessoas estranhas à mesa de operações ou às outras dependências da empresa, inclusive a sala dos servidores, somente será possível quando acompanhado dos responsáveis pelas respectivas áreas.

IV. Segregação eletrônica

A Radar mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores e monitorará o acesso dos Colaboradores a tais pastas e arquivos com base na senha e *login* disponibilizados. O acesso às pastas e arquivos eletrônicos é controlado de acordo com cada função dos Colaboradores, e somente algumas instâncias de visualização são livres para todos os Colaboradores.

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) fechar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso destas.

Política de Anticorrupção

I. Introdução

A Gestora está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção").

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção 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 criminal dos indivíduos envolvidos.

II. Abrangência das Normas de Anticorrupção

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 às 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.

a. Definição

Nos termos das Normas de 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.

b. Normas de Conduta

É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização prévia do Diretor de Compliance, Risco e PLD.

Os Colaboradores deverão se atentar, ainda, 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 suborno seja recusada pelo agente público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

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

c. Proibição de Doações Eleitorais

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

d. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências (“Audiências”) com agentes públicos, sejam elas internas ou externas, a Gestora buscará ser representada por, ao menos, 2 (dois) Colaboradores ou conforme orientação do Diretor de Compliance, Risco e PLD, 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 os apresentar ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

Vigência e Atualização

Esta 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
Junho de 2025	3ª e Atual	Diretor de Compliance, Risco e PLD

ANEXO I

TERMO DE COMPROMISSO AO MANUAL DE CONDUTA DA RADAR GESTORA DE RECURSOS LTDA.

Eu, [=], doravante denominado simplesmente "Declarante", na qualidade de Colaborador da **RADAR GESTORA DE RECURSOS LTDA.** ("Radar"), neste ato, conforme definido no Manual DE Regras, Procedimentos e Controles Internos ("Manual"), venho, por meio deste Termo de Adesão:

(i) Declarar ter recebido 1 (uma) cópia do Manual, as quais são de mesmo conteúdo e forma, sendo certo que uma das cópias rubricadas por mim, Declarante, é entregue neste ato à Radar para arquivo;

(ii) Declarar que li e compreendi por completo o Manual e todos os termos nele contidos;

(ii) Declarar que aceitei e aderi, neste ato, às disposições constantes do Manual, obrigando-me a observá-lo integralmente, sem qualquer ressalva e que, em caso de dúvida, consultarei o responsável pela Área de Compliance da Radar previamente à tomada de qualquer atitude;

(iv) Declarar que assumi expressamente responsabilidade pessoal pelo cumprimento das regras constantes do referido Manual, inclusive no que diz respeito à confidencialidade abaixo descrita, obrigando-me a pautar minhas ações e exercício de atividades referentes à Radar sempre em conformidade com tais regras, sujeitando-me, ainda, às penalidades cabíveis de acordo com o disposto no referido Manual.

O dever de confidencialidade previsto neste Manual subsistirá por toda a relação, societária ou empregatícia, com a Radar, e subsistirá pelo período de 2 (dois) anos após o desligamento, se vier a ocorrer.

Assim, eu, na condição de Declarante, firmo o presente Termo de Adesão em 2 (duas) vias de igual teor e forma.

[Local], [=] de [=] de 20[=]

_____

[=]

ANEXO II
TERMO DE CONFIDENCIALIDADE

Através deste instrumento, [=], inscrito no CPF sob o nº [=], doravante denominado "Colaborador", e **RADAR GESTORA DE RECURSOS LTDA** ("Gestora"), resolvem, 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 ("Informações Confidenciais"), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, 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, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos.
b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Gestora, bem como 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.

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 privilegiadas, "Insider Trading", Divulgação Privilegiada 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 e sem remédio jurídico para a Gestora e terceiros, 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 artigo 482 da Consolidação das Leis de Trabalho, ou desligamento ou exclusão por justa causa, conforme a função do Colaborador à época do fato, obrigando-lhe a indenizar a Gestora e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.

3.2 O Colaborador expressamente autoriza a Gestora a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos, observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízos do direito do Gestora de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

3.3 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

3.4 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:

a) 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;
b) 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;
c) 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 (“Informação Protegida”), 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.
d) Nos termos da Lei 9.279/95, é proibida a divulgação, exploração ou utilização sem autorização, de Informação Protegida a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato, 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 a qual 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. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 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 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Local], [=] de [=] de 20[=]

_____

[=]

ANEXO III
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de tomada de decisão de investimento ou da equipe de gestão de recursos de terceiros, conforme o caso, da **RADAR GESTORA DE RECURSOS LTDA.**, inscrita no CNPJ sob o nº 17.776.271/0001-36 ("GESTORA") por prazo indeterminado:

[ ] até que me certifique pela CGA e CGE;

[ ] ou até que o Conselho de Certificação me conceda a isenção de obtenção da CGA e CGE;

[ ] até que me certifique pela CGA;

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGA;

[ ] até que me certifique pela CGE; ou

[ ] até que o Conselho de Certificação me conceda a isenção de obtenção da CGE.;

Rio de Janeiro, [---] de [---] de [---].

_____
[COLABORADOR]

_____
RADAR GESTORA DE RECURSOS LTDA

Testemunhas:

1._____
Nome:
CPF:

2._____
Nome:
CPF: