RADAR

Manual de Regras, Procedimentos e Controles Internos

Junho de 2022

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 portfólio para fundos locais de investimento em ações ("Fundos Locais"), de carteiras administradas ("Carteiras Administradas") e veículos de investimento estrangeiros ("Veículos Estrangeiros") (cada um dos referidos veículos de investimento, um "Fundo Gerido", em conjunto, os "Fundos Geridos"). Para guiar seus sócios, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento de suas atividades ("Colaboradores"), a equipe de compliance da Gestora desenvolveu o presente manual ("Manual").

Neste sentido, este Manual, elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, a Resolução CVM nº 21, de 25 de fevereiro de 2021 ("RCVM 21"), demais orientações da Comissão de Valores Mobiliários ("CVM"), no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA de ART"), no Código ANBIMA de Ética ("Código ANBIMA de Ética"), e no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), tem por objetivo estabelecer 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 Geridos. 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, que fica sob a responsabilidade do Sr. Leonardo Tavares Pereira, ("Diretor de Compliance, Risco e PLD").

O presente Manual visa, ainda, evidenciar as regras aplicáveis ao exercício da atividade de gestão de carteiras de fundos de investimento, sobretudo, com vistas a: (i) coibir situações que caracterizem conflito entre os interesses próprios e dos Fundos Geridos pela Radar; (ii) garantir a confidencialidade de informações a que a Radar tenha acesso no exercício de suas atividades; (iii) garantir a condução e continuidade dos negócios da Radar em conformidade com as boas práticas de mercado; (iv) promover práticas de prevenção à lavagem de dinheiro e no combate a atividades ilícitas; (v) estabelecer algumas restrições com relação à negociação de valores mobiliários; e (vi) expor os métodos e procedimentos adotados pela Radar para o treinamento de seus Colaboradores.

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

II. Aspectos gerais

A Gestora mantém uma política de compliance ("Política") abrangente e integrada que é alicerçada num sistema interno de controle de práticas de negócio ("Sistema") apoiado por normas adequadas, recursos humanos e infraestrutura técnico/tecnológica, e governança alinhada com os objetivos da empresa.

Por meio de mecanismos de controle interno adequados, 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, em suas diversas dimensões; e
(iii) Aos padrões de conduta ética e profissional.

II. 1. Elementos do Sistema

O sistema de compliance da Gestora inclui os seguintes elementos:

(i) Políticas e procedimentos criados com o objetivo de resguardar a integridade da Radar;
(ii) Manual de Controles Internos, Código de Ética e demais políticas adotadas pela empresa;
(iii) Recursos adequados para desenvolver, manter e melhorar as atividades da função de compliance; e
(iv) Um programa de treinamento adequado.

II.2. Governança do Sistema de Compliance

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

- Estrutura: a governança do sistema de compliance da Gestora é baseada nos seguintes órgãos principais:

(a) Área de Compliance, sob a responsabilidade de Leonardo Tavares Pereira, responsável pela área nos termos da regulamentação em vigor ("Diretor de Compliance, Risco e PLD");
(b) Comitê de Risco, composto pelos membros sêniores do Comitê de Investimento e pelo Diretor de Compliance, Risco e PLD;
(c) Comitê de Compliance, composto pelo Diretor de Compliance, Risco e PLD e pelo diretor Mario Cunha Campos ("Diretor de Gestão"), este apenas para fins de reporte e Pedro Batista de Lima Filho, (cada um dos referidos, um "Diretor", em conjunto, os "Diretores"); e
(d) Conselho de Administração ("CA"), composto pelos dois Diretores e um representante indicado pela 3G Capital.

- Competências:

(a) **Diretor de Compliance, Risco e PLD**: O Diretor de Compliance, Risco e PLD estará incumbido de:

(i) Implementar o programa de Compliance da Gestora, planejando a execução e cumprindo as metas definidas pelo Comitê de Compliance;
(ii) Redigir 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) Produzir relatórios de risco e levá-los para análise do comitê de Risco;
(v) Auxiliar o Comitê de Compliance e o CA em qualquer questão atinente a sua área; e
(vi) Analisar e decidir sobre conflitos de interesse em geral.

(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.

(c) **Comitê de Risco**: O Comitê de Risco é o órgão da Gestora incumbido de:

(i) Dar parâmetros gerais, orientar e aprovar o programa de gestão de risco da Gestora;
(ii) Estabelecer objetivos e métricas para a gestão de risco; e
(iii) Avaliar resultados da gestão de risco, solicitar modificações e correções, e aprovar os limites para as métricas de risco dos fundos e da Gestora.

- <u>Autoridade e Poderes</u>:

(a) **Diretor de Compliance, Risco e PLD**: para realizar sua missão institucional, o Diretor de Compliance, Risco e PLD terá poderes para, entre outros:

(i) Planejar, definir e implementar o programa de compliance da Gestora;
(ii) Analisar possíveis violações à política de compliance da Gestora ou às leis e regulações aplicáveis à Gestora e a suas atividades;
(iii) Determinar auditorias, requisição de documentos, tomada de contas, averiguações, investigações, medidas corretivas e punições;
(iv) Realizar o cálculo e monitoramento diário das métricas de risco.

(b) **Comitê de Compliance**: Para realizar sua missão institucional, o Comitê de Compliance terá poderes para, entre outros:

(i) Aprovar manuais internos de compliance, Código de Ética e outras normas e regulamentos referentes à política de compliance da Gestora;
(ii) Recomendar, propor e adotar orientações e políticas novas, e determinar a modificação, substituição ou a extinção das existentes; e

(iii) Avocar quaisquer matérias envolvendo o programa de compliance, violações a regras e regulamentos (prevenção, aplicação e medidas corretivas)

(c) **Comitê de Risco**:

(i) Aprovar manuais internos de risco e outras normas e regulamentos referentes à política de risco da Gestora;

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

(iii) Planejar, definir, implementar e monitorar a política de Gestão de Risco da Gestora; e

(iv) Analisar parâmetros e definir limites para as métricas de risco dos Fundos Geridos

- Independência: a Área de Compliance, o Comitê de Compliance e o Comitê de Risco 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, o Comitê de Compliance e o Comitê de Risco submetem-se diretamente apenas ao Conselho de Administracão ("CA").

- Reuniões:

(a) Área de Compliance: o responsável pela Área de Compliance poderá se reunir com o CA ordinariamente, uma vez por ano, para apresentar o relatório anual de compliance, e extraordinariamente, quando houver necessidade.

(b) O 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

(c) O Comitê de Risco se reunirá semanalmente, antes da reunião do Comitê de Investimento, para analisar relatórios de risco e discutir novas metodologias e métricas de risco, quando houver necessidade. O Comitê de Risco também poderá ser convocado extraordinariamente, em caso de necessidade ou oportunidade, tais como momentos de incerteza do mercado, eventos que tenham potencial para gerar o desenquadramento da carteira do fundo, solicitações de resgate em volume superior aos definidos como padrão pelas metodologias de gestão do risco de liquidez, além de outras situações que impactem o risco de liquidez.

- Decisões:

(a) **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.

(b) **Comitê de Risco**: preferencialmente, as decisões do Comitê de Risco deverão ser tomadas por consenso entre os membros. Caso o consenso não seja possível, as decisões serão tomadas por maioria, cabendo aos Diretores o direito de veto. Em relação à política de risco, ainda, o CA tem poderes de orientação geral e pode a qualquer tempo avocar para si matérias de competência do Comitê de Risco. Do mesmo modo, o CA tem poderes de veto sobre as decisões do Comitê de Risco, e modificações substanciais na política deverão ter seu assentimento.

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. 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 moldura legal e regulatória, nacional e internacional (“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.

Responsabilização e Penalidades

III.I 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 normas legais (leis ou regulamentos);
(ii) Agir em desacordo com o Manual ou quaisquer outras normas de compliance;
(iii) Agir de forma antiética ou de qualquer forma que prejudique a reputação da Gestora;

(iv) Solicitar a outras pessoas Violação; ou
(v) Retaliar Colaborador ou quem tenha reportado uma preocupação com infração.

III.II. 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.III 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.IV. 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.V. Dever de Reportar

Os Colaboradores entendem e aceitam que têm o dever ativo de prontamente reportar suspeitas ou indícios 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 3 (três) 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; e
(xi) Relacionamento entre a Radar e a 3G Capital.

Quando de seu ingresso na Radar e, posteriormente, em até 30 (trinta) dias corridos após o término de cada semestre 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 Geridos ou das operações realizadas pela Radar. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração 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 dos Fundos Geridos 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 Gerido ou do projeto 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; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

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 de um membro do Conselho, sendo tal ato passível de penalidades e sanções tais quais as descritas no artigo XI. do Código de Ética.

Ademais, as regras de 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 pelo Colaborador 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, 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 crachás eletrônicos. Somente os Colaboradores possuem crachás que permitem a entrada automática e, na hipótese de o Colaborador esquecer o seu crachá eletrônico, 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, 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.

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

O processamento é centralizado, e a rede local roda sobre uma plataforma de máquinas virtuais existentes no servidor central. Cada Colaborador possui um computador com todas as informações de usuário local redirecionada para os servidores. A estrutura de acesso remoto conta com um servidor virtual dedicado com dupla autenticação habilitada.

A Gestora utiliza a solução de virtualização VMWARE, garantindo redundância da própria infraestrutura e melhor tempo de recuperação de desastres (RTA). Estrutura de servidores com 2 hosts físicos e 6 virtuais com sistemas operacionais Windows. Servidores contam com uma estrutura de contingência em Boston (EUA) permitindo a recuperação dos serviços em caso de desastre. Está prevista a revisão desta estrutura com previsão de implantação no primeiro semestre de 2019.

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. Todas as estações de trabalho 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. Além disso, é realizada uma cópia noturna de todas as máquinas virtuais, cópia esta que é armazenada localmente e copiada para o co-location de Boston.

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 deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:
a) Malware (vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;
d) Phishing scam;

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

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Gestora definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um 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 dispensará especial atenção ao monitoramento constante dos riscos envolvendo a segurança cibernética da Radar, a fim de proteger Informações Confidenciais e os recursos tecnológicos da Gestora. Para tanto, a área de TI procederá com testes e medidas de precaução relativas à segurança cibernética, conforme detalhado em seção específica da presente política.

II. ***Ações de prevenção e proteção***

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a Gestora adota, conforme já detalhado nas regras internas de Segurança da Informação.

A Gestora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de *login* e alteração de senhas são auditáveis e rastreáveis. A Gestora deve criar logs e trilhas de auditoria sempre que os sistemas permitam. Tais verificações serão registradas e arquivadas pela empresa de T.I contratada por, no mínimo, 5 (cinco) anos.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela Segurança Cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A Gestora conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais. A Gestora deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares

e/ou aplicações não autorizadas.

Conforme abordado anteriormente, 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 como Informações Confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de Compliance, Risco e PLD.

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.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar HD externo ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

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 servidores e computadores da Gestora, bem como avisar prontamente o Diretor de Compliance, Risco e PLD.

Não obstante o disposto no parágrafo anterior, todos os anexos dos e-mails recebidos pelos Colaboradores da Gestora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente, bem como são criptografadas.

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

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 Gestora adota também *backup* das informações e dos diversos ativos da instituição, conforme detalhado na política de segurança da informação, constante deste Manual.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas 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 o previsto na RCVM 21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da Gestora e devem ser observadas integralmente.

III. *Mecanismos de Supervisão e Testes Periódicos*

O Diretor de Compliance, Risco e PLD deve se assegurar de que os mecanismos de controle descritos acima, dentre outros são anualmente testados pela equipe responsável, sem prejuízo dos testes de restauração para validação do processo de recuperação de dados, que são feitos mensalmente.

A gestora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A Gestora mantém inventários atualizados de *hardware* e *software*, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da Gestora deve diligenciar para manter os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A área responsável deve também monitorar diariamente as rotinas de *backup*, executando testes regulares de restauração dos dados.

Deve-se, ademais, realizar testes de invasão externa, *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados na forma definida no item anterior devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

Por fim, o Diretor de Compliance, Risco e PLD deverá verificar, aleatoriamente, (i) os e-mails repassados pelos Colaboradores, (ii) o modo adotado pelos Colaboradores para utilização dos ativos, sistemas, servidores e rede de informações da Gestora, incluindo a verificação de sites visitados, e

(iii) do histórico de acessos às áreas restritas da Gestora.

IV. *Plano de resposta*

A Área de Gestão de Riscos e de Compliance deve, conjuntamente com os profissionais de *cybersecurity* e Segurança da Informação, elaborar um plano formal de resposta a ataques virtuais. A Gestora deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deverá levar em conta os cenários de ameaças previstos no *risk assessment*. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

Considerando que cada evento de ataque virtual é dotado de características peculiares, o plano de resposta será desenvolvido pela área de TI de forma personalizada para resolver o problema factual enfrentado. Desta forma, o referido plano deverá ser formalizado por e-mail, e enviado ao Diretor de Compliance, Risco e PLD para ciência e eventuais tomada de eventuais procedimentos cabíveis.

V. Reciclagem e Revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da Gestora sobre a matéria, deverá ser revisto e atualizado semestralmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A Gestora deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

Os Colaboradores deverão participar de treinamentos que abordem o tema da segurança cibernética, os quais serão aplicados pelo responsável pela presente política, em periodicidade não superior a 12 (doze) meses.

Política de Certificação ANBIMA

A Gestora aderiu e está sujeita às disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código de Certificação"), 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 o Código de Certificação, que a Certificação de Gestores ANBIMA ("CGA") e a Certificação de Gestores ANBIMA para Fundos Estruturados ("CGE") são as certificações pertinentes 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 e CGE, a depender do investimento gerido, 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 e a CGE é aplicável aos profissionais que atuam em fundo de investimento em participações, fundo de investimento em direitos creditórios não padronizados, fundo de índice, fundo de investimento em direitos creditórios, fundo de investimento em cotas de fundos de investimento em direitos creditórios e/ou fundo de investimento imobiliário..

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 ou CGE na Gestora e a certificação não esteja vencida, a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGA e CGE 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 ou CGE 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 ou CGE, 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 no Código ANBIMA de Certificação.

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 no Código ANBIMA de Certificação.

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 ou CGE, conforme aplicável (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 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, 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 IV** 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 encarregado 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. Somente os Colaboradores possuem crachás que permitem a entrada automática e, na hipótese de o Colaborador esquecer o seu crachá eletrônico, 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, 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) desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

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. <u>Definição</u>

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.

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

PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS

ATIVIDADES DA RADAR GESTORA DE RECURSOS LTDA.

1. Instrução CVM Nº 555/14

2. Resolução CVM Nº 21/21

3. Resolução CVM Nº 50/21

4. Ofício-Circular/CVM/SIN/Nº 05/2014

5. Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros

6. Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada

7. Código ANBIMA de Administração de Recursos de Terceiros

8. Lei 9.613/98, conforme alterada

Data Base: Junho/2022

ANEXO IV
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: